EXTENSIONS IN THE THEORY OF LUCAS AND LEHMER PSEUDOPRIMES

By

ANDREW DAVID LOVELESS

A dissertation submitted in partial fulfillment of
the requirements for the degree of

DOCTOR OF PHILOSOPHY

WASHINGTON STATE UNIVERSITY
Department of Mathematics

AUGUST 2005

To the Faculty of Washington State University:

The members of the Committee appointed to examine the dissertation of ANDREW DAVID LOVELESS find it satisfactory and recommend that it be accepted.

Chair

ACKNOWLEDGEMENTS

The completion of this dissertation is due in large part to my advisor William Webb. He always is ready for discussion even when I drop in unexpected. I deeply thank him for all the direction and advice he has given me over the last several years. In addition, I owe a special thanks to my other committee members, Matt Hudelson and Duane DeTemple. I have greatly enjoyed my weekly combinatorial geometry seminar meetings with these three faculty members. Many of my mathematical interests stem from Prof. Hudelson. His combinatorics class was one of my favorites. He always has interesting problems to talk about and I will miss having neighboring offices. Prof. DeTemple has introduced to me to many interesting problems and proof techniques. He has a great talent of exposition and I thank him for his help in my work.

Certainly, many of my achievements can be attributed to the outstanding faculty and staff at Washington State University. Specifically, thank you to Prof. Wollkind, Prof. Kent, Prof. McDonald, Prof. Tsatsomeros, Prof. Watkins, Prof. Schumaker, Prof. Khapalov and Prof. Kucera. You all have been supportive and helpful in my studies and I have learned a lot about mathematics and the teaching of mathematics from each of you. I also would like to thank Prof. Ariyawansa, Prof. Manoranjan, and Prof. Genz for their help in ensuring that I received financial help by way of scholarships over the last three years.

My quest towards a Ph.D. would never have begun without the pressing of the amazing professors at the University of Puget Sound. A special thanks to Prof. Ron VanEnkevort for planting the seed of graduate school in my mind; He was my best teacher. Also, thank you to Prof. Robert Beezer, Prof. Bryan Smith, and Prof. Carolyn Smith for their advice and support.

In addition, I would like to thank my office mates Indika Radjapaske and Christian Ketelson for many helpful discussions. I have been lucky to be surrounded by such good friends.

A quiet mathematician seems quite a misfit in a social family composed of workers in business, construction, teaching, advertising, broadcasting and farming. Yet, I am blessed with overwhelming support from my family. For instilling in me the importance of education, and paying for it, thank you to my parents. To Matt, Brad, Cecelia, Tara, Kurt, Katie, Jennifer, Kristina, Samantha, Pryce, Carson, Victoria, Ethan, Zachary, and Alexandra, I feel lucky to be a part of your lives and I love you all. To Marilyn and Karl, thank you for welcoming me into your wonderful family and for your constant support.

I am lucky to have the unwavering support of my wife, Joelle. Without her, I would never have had the confidence or ambition to pursue this endeavor. She has made me a better mathematician and a better man. I am truly blessed. Thank you.

EXTENSIONS IN THE THEORY OF LUCAS AND LEHMER PSEUDOPRIMES

Abstract

by Andrew David Loveless, Ph.D.
Washington State University
August 2005

Chair: William A. Webb

We begin by briefly explaining the applications and history of primality testing. Chapter 1 surveys the number theory topics that are essential to the study with motivation where possible. After summarizing the current literature in Chapter 2, the remainder of the dissertation extends known research and investigates new ideas in probabilistic primality testing based on Lucas and Lehmer sequences by both theoretical and numerical means.

First, we define Lehmer sequences and give four congruence relations for these sequences which are satisfied by all primes. For given parameters, each congruence gives a probabilistic primality test in which all primes pass the test, but some composites, called pseudoprimes, also pass. For an odd composite integer n with the discriminant of the sequence fixed, we give the number of parameters that yield n as a pseudoprime for Congruence 1 of Chapter 3. Using this formula, we deduce a bound on the number of parameters that yield n as a pseudoprimes. With further results in Chapter 6, we

are able to give a count and bound on all parameter sets for all discriminants. In Chapter 4, we explore ways to systematically reduce the number of pseudoprimes exhibited by Congruences 1 and 2 of Chapter 3.

Primality testing based on congruence relations with modulus n^2 instead of n are investigated in Chapter 5. We motivate this change and give several such relations. Extensive numerical tables are given for the number of pseudoprimes up to $x = 10^k$ for various congruences and methods in Chapters 3, 4, and 5.

By analyzing the characteristic roots of Lehmer sequences in Chapter 6, we are able to give several relationships between parameters sets for congruence relations of previous chapters. We use these relationships to help explain the effectiveness, or ineffectiveness, of specific congruences and methods.

In the final chapter, we consider Lucas and Lehmer sequences where the parameters are taken in the general setting of commutative rings with identity. Much of the theory and results also hold in this setting. We also look at the special case of quotient rings.

Table of Contents

To Joelle.

Introduction

A prime number is a positive integer greater than 1 whose only divisors are 1 and itself. The structure of the sequence of prime numbers that arise from this definition have fascinated mathematicians for centuries. Several innocent looking questions about these numbers remain unanswered even after centuries of inquiry by generations of mathematicians. The famous mathematician Leonard Euler once wrote:

Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate.

With this said, we do know a few facts about the sequence of primes and a great many of them are due to Euler himself. Some of the major results illustrate how primes are foundational to all of mathematics while other theorems are concerned with special types of primes and the growth of the sequence of primes. We investigate the following question.

QUESTION: Given a large integer, n, can we describe algorithms to quickly determine if n is prime? In addition, can we articulate the effectiveness of such algorithms?

We do not give a rigorous mathematical answers to these questions, but for all practical purposes we hope you become convinced that the answers are yes. Let us further clarify these questions. In practice, the "large integer" is roughly 100 digits or more and it is appropriate to think of numbers of this size as we proceed. The algorithms we describe would also work "quickly" on integers with thousands of digits. By "quickly determine", we mean that the algorithm could be implemented on a computer and would finish checking an integer, n, in $\mathrm{O}(\log(n))$ steps. We consider multiplication as one step for simplicity, some authors consider bit operations instead. When we use the terms $\mathrm{O}(\log(n))$ operations, we will be thinking of the number of multiplications. For 100 digit numbers, we want the algorithm to finish checking in fractions of a second on a desktop computer.

We are not the first to investigate this question. Several good algorithms are known. This work extends known results and explores different approaches to the problem. In Chapter 2, we give an overview of known methods. Before continuing, we discuss why this question warrants investigation.

The ability to find large primes efficiently is important in the subject of cryptography and has become an interesting topic in its own right. Many cryptographic schemes and protocols begin by finding large primes. For instance, the celebrated RSA cryptosystem is based on finding two large primes, p and q, and then using the integer $n = pq$ to develop a secure form of communication over the internet.

In addition to the practical importance of prime recognition, the characteristics of primes are fundamental to the whole of mathematics and for this reason alone deserve to be studied from every angle and approach. In 1801, in the book Disquisitiones Arithmeticae, the great mathematician Carl Friedrich Gauss wrote:

The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic... . The dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.

There are two types of methods for determining if a large integer is prime, deterministic primality testing and probabilistic primality testing. In this work, we only discuss probabilistic primality tests. When the term primality test is used alone, we are implying that the test is probabilistic.

A deterministic primality test gives a rigorous proof that a given integer n is prime. In other words, these algorithms verify, with certainty, that a number is prime. Sometimes we say that such a test gives a certificate of primality for an integer n.

In August 2002, three computer scientists, Manindra Agrawal, Neeraj Kayal and Nitin Saxena gave a polynomial time algorithm for proving primality [4]. This was a major breakthrough and was based on relatively simple ideas. However, these tests still take too long for cryptographic purposes. The best known algorithms for primality proving, to date, have running time $\mathrm{O}(\log(n)^6)$ [25]. Cryptographic algorithms, such as the RSA cryptosystem, require faster methods. For this reason, probabilistic primality tests are used.

Probabilistic primality tests (sometimes called compositeness tests) function in the following way. Any prime number will pass the test. However, there is the possibility that some composite numbers will give false positives. These 'liars' are called pseudoprimes. The goal in the theory of probable primality testing is to find an efficient test which exhibits few pseudoprimes.

Probable primality testing theory is an interesting game. Any theorem that reads, *If n is a prime, then 'conclusion'*, can be used as a primality test. The test is the 'conclusion'. If the conclusion is false for n, then we know for certain that n is composite. If the conclusion is true for n, then we know nothing for certain, so we say n is a probable prime. As we will see, certain theorems work better than others and some give very high confidence in their results.

The first attempts at probabilistic primality tests were based on variants of Fermat's little theorem. If n and a are relatively prime integers and $a^{n-1} \equiv 1 \ (mod\ n)$, then we say that n is a probable prime to the base a. Pseudoprimes for this test have been studied extensively. In the current study, we investigate a class of primality tests which are based on Lucas sequences.

The fundamental concepts necessary to the study of these tests will be presented in Chapter 1. In Chapter 2, we survey the classical primality tests focusing on variant's of Fermat's Theorem and the use of Lucas sequences. The remaining chapters focus on new research.

Chapter 3 thoroughly discusses an extension of the theory of Lucas sequences which was introduced by D.H. Lehmer [33]. These sequences, now known as Lehmer sequences, can be used in primality testing in much the same way as Lucas sequences. We explain how Lehmer sequence tests are as efficient as Lucas sequence tests and have a broader range of parameter choices. We also prove a fundamental result about the number of 'bad' parameters, *i.e.* parameters which lead to a pseudoprime. We end the chapter with extensive numerical data which indicates the tests and methods that give the highest confidence.

The Lehmer sequences of Chapter 3 give a broader range of choices for primality testing and make the theory more robust. However, the number of pseudoprimes they exhibit is not a great improvement on the standard Lucas sequence. In Chapter 4, we explore two ways to systematically reduce the number of pseudoprimes exhibited by the tests in Chapter 3. The first strengthening technique is known in special cases, but we develop it into a general theory. The second is not found in the literature. This technique will lead to a primality test which experimentally is as good as any known. It has roughly the same efficiency as current methods in use and it is accurate for many different methods of choosing parameters.

Chapters 3 and 4 only consider congruence properties modulo a prime. Chapter

5 is devoted to exploring generalization of Lucas/Lehmer tests modulo prime powers. We discuss reasons for and against making such a generalization. We give several congruences and combined congruences and provide tables of data for comparison. The majority of the tests in this section are very effective, but they are theoretically difficult to investigate.

In Chapter 6, we restate several of the congruence theorems from previous chapters in terms of their characteristic roots. This is an important theoretical method and it allows for ease in comparison between the various tests. Using these techniques we will prove various results concerning the connections between various parameters sets. These theorems will give at least partial explanations for why some tests are better than others.

In the final chapter, we state the properties of Lucas and Lehmer primality testing in the general setting of commutative rings with unity. The downside is that all of the computations must be done in the ring, which generally takes more time. If the ring is chosen to be a finite field, then the computation can be done in a relatively efficient way and the test are very accurate. Primality tests in finite fields have been studied before, but no one has investigated Lucas sequences where each parameter is chosen from an arbitrary ring.

Chapter 1

Essential Number Theory Topics

The topics and theorems of number theory that are relevant to the study of primality testing and pseudoprimes are discussed here. We introduce foundational tools in the theory of congruences and motivate their use in primality testing. The focus is on presenting the ideas. We leave proofs for the new material in later chapters. The majority of the proofs omitted can be found in elementary texts on number theory. For more detail expositions on these topics see [7], [14], [27], [49], [56].

1.1 Euler and Carmichael Functions

A vast array of integer functions are central to the study of number theory. Here, we discuss two such functions which are important tools in the study of primality testing. These functions, the Euler ϕ-function and the Carmichael λ-function, are often used in generalizing theorems which concern primes.

The Euler ϕ-function can be defined strictly in terms of the prime divisors of an integer, but it also has a combinatorial interpretation. For a positive integer $n > 1$, the value $\phi(n)$ is defined as the number of positive integers less than n that are relatively prime to n. Several proofs in elementary number theory make use of the properties of relatively prime integers. The Euler ϕ-function is a useful notational convenience in such instances.

For a given integer n, the value $\phi(n)$ can be computed in terms of the prime factorization of n. Most introductory number theory texts include a full derivation of the following formulas.

Theorem 1.1.1. *The Euler ϕ-function satisfies the following properties*

1. *If m and n are positive integers with $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

2. *If p is a prime and α is a positive integer, then $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*

3. *Thus, if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, then $\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i} - p_i^{\alpha_i-1}$.*

The Carmichael λ-function is less well-known and does not have a similar combinatorial interpretation. However, it allows for more articulate generalizations of certain theorems than the Euler ϕ-function. Although the functions are defined slightly differently for powers of two, the most significant difference is in their definition for products of primes. Note that one involves a product and the other involves the least common multiple (LCM).

Definition 1.1.1. The Carmichael λ-function is defined for all positive integers as follows:

1. If p is an odd prime and α is a positive integer, then $\lambda(p^\alpha) = \phi(p^\alpha)$.
2. If α is a positive integer, then

$$\lambda(2^\alpha) = \phi(2^\alpha), \text{ if } \alpha = 0, 1, 2, \quad \text{and} \quad \lambda(2^\alpha) = \frac{1}{2}\phi(2^\alpha), \text{ if } \alpha > 2.$$

3. If $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, then $\lambda(n) = \text{LCM}(\lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k}))$.

Both the Euler ϕ-function and the Carmichael λ-function have been used in the study of primality tests. We use these functions in the following sections.

1.2 Congruences

Throughout this manuscript, we will be interested in many different types of congruence relations. Primality tests are based on the existence of congruences which always hold for primes and never, or rarely, hold for composites. One of the most well-known of these is Wilson's Theorem.

Theorem 1.2.1. *Wilson's Theorem.*

The positive integer p is a prime number if and only if $(p-1)! \equiv -1$ (mod p).

This theorem completely characterizes primes, but it is not useful in practice without an efficient way to compute $(n-1)!$ modulo n for large integers n. There are other congruences which characterize, or are conjectured to characterize, primes, yet they all suffer from the same problem when it comes to implementing them in practice. The best deterministic algorithms, that is an algorithm implementing a characterization of primes, requires $\mathrm{O}(\mathrm{Log}(n)^6)$ steps as mentioned in the introduction. The ultimate goal would be to find a test that completely characterizes primes and is more efficient to use.

The trick with primality testing is to build a congruence which can be tested quickly and is somehow based on a characterization of primes. We tend to lose the prime characterization in the process, but we create a practical test which works "most" of the time. Clarifying what is meant by "most" occupies a major portion of the rest of this work. The following characterization of primes is often more useful in the creation of primality tests in this way.

Theorem 1.2.2. *The positive integer p is prime if and only if*

$$\left(\begin{array}{c} p \\ k \end{array} \right) \equiv 0 \ (mod\ p), \ \textit{for all } k \textit{ such that } 1 \leq k \leq p-1.$$

This theorem is one of the main tools used in proving congruences for primality tests. In Chapter 5, we will look at a similar characterization modulo p^2. Once again, this theorem cannot be tested directly, since there is no known way to efficiently compute these binomial coefficients modulo n. However, we will see ways that sums of binomial coefficients can be tested. We make use of these ideas in the next section.

1.3 Fermat's Little Theorem

Many of the foundational concepts in primality testing stem from the following theorem. The congruences given in this theorem can be proven from the characterization of primes using binomial coefficients in Theorem 1.2.2 and we include the proof as an example of how primality tests are created.

Theorem 1.3.1. *Fermat's Little Theorem.*

If p is prime and a is a positive integer, then $a^p \equiv a$ $(mod\ p)$. If, in addition, $p \nmid a$, then $a^{p-1} \equiv 1$ $(mod\ p)$.

Proof. Use induction on a. If $a = 1$, then $1^p \equiv 1$ $(mod\ p)$. If the statement is true for a, then

$$(a+1)^p = \sum_{k=0}^{p} \left(\begin{array}{c} p \\ k \end{array} \right) a^k \equiv a + 1\ (mod\ p).$$

Thus, the statement is true for all values of a. The second congruences follows immediately from the first under the conditions $p \nmid a$. □

Note that the last congruence in the proof follows directly from Theorem 1.2.2. This connection will occur again later.

When we discuss the effectiveness of this primality test, we are interested in composite integers which satisfy the congruence in Fermat's Little Theorem. Thus, it is natural to ask about generalizations of this theorem concerning composite integer. For composite integers, we have the following related theorems.

Theorem 1.3.2. *Euler's Theorem.*

If n and a are positive integers with $(n, a) = 1$, then $a^{\phi(n)} \equiv 1$ (mod n).

Euler's Theorem is well-known, but lesser known is Carmichael's Theorem. It should be noted that Carmichael's Theorem is more general than Euler theorem. Indeed, for a given integer n, we have $\lambda(n)|\phi(n)$. See [14], for proof of this result.

Theorem 1.3.3. *Carmichael's Theorem.*

If n and a are positive integers with $(n, a) = 1$, then $a^{\lambda(n)} \equiv 1$ (mod n).

We discuss these congruences and generalizations of them in Chapter 2.

1.4 Quadratic Residues

We often want to know when an integer is a square modulo a prime p. If $p > 2$ does not divide a, and if there exists an integer b such that $a \equiv b^2$ (*mod* p), then a is called a quadratic residue modulo p; otherwise, it is a quadratic nonresidue modulo p.

The following notation is standard when discussing quadratic residues.

Definition 1.4.1. Let p be an odd prime and a an integer. The Legendre symbol, $(a|p)$, is defined as follows:

$$\left(\frac{a}{p}\right) = (a|p) = \begin{cases} +1 & \text{, if a is a quadratic residue modulo p} \\ -1 & \text{, if a is a quadratic nonresidue modulo p} \\ 0 & \text{, if p divides a} \end{cases}$$

Here we summarize some of the key properties of the Legendre symbol.

Theorem 1.4.1. *Let p and q be odd primes.*

1. *If $a \equiv b$ (mod p), then $(a|p) = (b|p)$.*

2. *For integers a and b, $(ab|p) = (a|p)(b|p)$.*

3. *$(a|p) \equiv a^{(p-1)/2}$ (mod p).*

4. *(Quadratic Reciprocity) $(q|p) = (-1)^{(p-1)(q-1)/4}(p|q)$.*

For composite integers, it is not as easy to characterize the squares. However, there is a useful generalization of the Legendre symbol that is used frequently in primality testing. The Jacobi Symbol, $(a|b)$, is an extension of the Legendre symbol, which is defined for any odd integer $b > 1$ as follows.

Definition 1.4.2. Let a be an integer and let b be an odd positive integer with $b > 1$ where $b = \prod_{i=1}^{k} p_i^{\alpha_i}$ is the prime factorization of b. The Jacobi symbol, $(a|b)$, is defined as follows:

$$\left(\frac{a}{b}\right) = (a|b) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i}.$$

When b is a prime the Jacobi symbol and Legendre symbol are the same. Unlike the Legendre symbol, the Jacobi symbol does not characterize the squares. However, they do share many properties as described below.

Theorem 1.4.2. *Let $b > 1$ be a positive odd integer.*

1. *If $a \equiv a'$ (mod b), then $(a|b) = (a'|b)$.*

2. *For integers a and a', $(aa'|p) = (a|b)(a'|b)$.*

3. *For an odd integer $b' > 1$, $(a|bb') = (a|b)(a|b')$.*

4. *(Quadratic Reciprocity) For a and b relatively prime positive odd integers, $(a|b) = (-1)^{(a-1)(b-1)/4}(b|a)$.*

It is important to note that the Jacobi symbol can be computed quickly in practice, even for large integers. Probabilistic primality tests often call for the computation of Jacobi symbols. When this is the case, we assume that the computation time is negligible.

1.5 Lucas Sequences

Given integers P and Q, the Lucas sequences, $U_k(P,Q)$ and $V_k(P,Q)$, are defined by the following recurrence relations with initial conditions:

$$U_k(P,Q) = PU_{k-1}(P,Q) - QU_{k-2}(P,Q), \quad U_0(P,Q) = 0, U_1(P,Q) = 1$$

$$V_k(P,Q) = PV_{k-1}(P,Q) - QV_{k-2}(P,Q), \quad V_0(P,Q) = 2, V_1(P,Q) = P.$$

Associated with the Lucas sequence is the characteristic polynomial $x^2 - Px + Q$. Let $D = P^2 - 4Q$ denote the discriminant of this polynomial. We denote the characteristic roots by $\alpha = \frac{P+\sqrt{D}}{2}$ and $\beta = \frac{P-\sqrt{D}}{2}$. Consequently, we have the following properties.

Theorem 1.5.1. *The values P, Q, D, α, and β described above satisfy*

1. $\alpha + \beta = P$.

2. $\alpha\beta = Q$.

3. $\alpha - \beta = \sqrt{D}$.

4. *(Binet Formulas)* $U_k(P,Q) = \frac{\alpha^k - \beta^k}{\alpha - \beta}$ *and* $V_k(P,Q) = \alpha^k + \beta^k$ *for* $k \geq 0$.

The special sequence $U_k(1,-1)$ is called the Fibonacci sequence. This sequence was first investigated by the thirteenth-century mathematician Leonardo da Pisa as a model for population growth of rabbits. Various other mathematicians studied special cases of Lucas sequences throughout the centuries. However, the general theory of Lucas sequences was not developed until 1878. In this year, Eduard Lucas published a long exposition [31] in Volume I of the *American Journal of Mathematics* on the various properties of Lucas sequences along with their connections with trigonometry, continued fractions, and primality tests. Since this time, Lucas sequences have become a topic of great interest in number theory.

Many facts are known about these sequences. We mention only a few here. Specifically, we touch on the subject of Lucas sequence identities. Lucas sequences are highly interconnected and satisfy many identities (enough to fill entire books). For our study, it is only necessary to have a few of these identities at our disposal, see [49] for a more extensive list. The next two theorems highlight the identities which we use the most.

For simplicity, we write $U_k = U_k(P,Q)$ and $V_k = V_k(P,Q)$.

Theorem 1.5.2. *If U_m and V_m represent the Lucas sequences as defined above, then*

1. $2U_{k+j} = U_kV_j + V_kU_j$ *for* $k, j \geq 0$.

2. $2V_{k+j} = V_kV_j + DU_kU_j$ *for* $k, j \geq 0$.

3. $2QU_{k-j} = U_kV_j - V_kU_j$ *for* $k, j \geq 0$ *and* $k \geq j$.

4. $2QV_{k-j} = V_kV_j - DU_kU_j$ *for* $k, j \geq 0$ *and* $k \geq j$.

5. $V_{2k} = V_k^2 - 2Q^k$ *for* $k \geq 0$.

We often take $j = \pm 1$ as a special case of Theorem 1.5.3. For this reason, we give the following corollary.

Corollary 1.5.3. *If $\epsilon = \pm 1$, then*

1. $2Q^{(1+\epsilon)/2}U_{k-\epsilon} = U_kP - \epsilon V_k$ *for* $k \geq 1$.

2. $2Q^{(1+\epsilon)/2}V_{k-\epsilon} = V_kP - \epsilon DU_k$ *for* $k \geq 1$.

The next theorem is a major tool in the creation of congruences which hold for primes. We shall make extensive use of it, so we include a proof.

Theorem 1.5.4. *If n is a positive integer, then*

$$2^{n-1}U_n = \sum_{i \text{ odd}} \binom{n}{i} P^{n-i}D^{(i-1)/2} \text{ and } 2^{n-1}V_n = \sum_{i \text{ even}} \binom{n}{i} P^{n-i}D^{i/2}.$$

Proof. Using the definition of the characteristic roots, the Binet formula gives $U_n = \frac{\alpha^n-\beta^n}{\alpha-\beta} = \frac{(P+\sqrt{R})^n-(P-\sqrt{R})^n}{2^n\sqrt{D}}$. Applying the binomial theorem and collecting terms, we obtain

$$2^n U_n = \frac{1}{\sqrt{D}} \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) P^{n-i} \left((\sqrt{D})^i - (-\sqrt{D})^i \right)$$

Note $(\sqrt{D})^i - (-\sqrt{D})^i$ equals 0 when i is even. Hence, we obtain the first formula by canceling one factor of $\sqrt{D}$ and dividing by 2. The second formula is proved the same way, starting from $V_n = \alpha^n + \beta^n$. □

Lucas sequence have found their way into primality testing due to their divisibility properties. In Chapter 2, we discuss specific congruence properties of Lucas sequences which always hold for primes and rarely hold for composites. When exploring divisibility of Lucas sequence, we often use the rank of appearance.

Definition 1.5.1. For a positive integer n and integer parameters P and Q, the *rank of appearance* of n is the least positive integer k such that $n|U_k(P, Q)$. We denote this value by $\omega(n; P, Q)$.

The rank of appearance is useful in proving theoretical results about divisibility because of the following, see [49] for a proof.

Theorem 1.5.5. *If* $U_k(P, Q) \equiv 0$ $(mod\ n)$*, then* $\omega(n; P, Q)|k$*.*

From Carmichael's Theorem, we have $a^k - 1 \equiv 0$ $(mod\ n)$ when $k = \lambda(n)$. The value $\lambda(n)$ may not be the smallest such value, but it is the best we can prove in general. For Lucas Sequences, we have results analogous to Euler's and Carmichael's Theorems concerning divisibility of U_k. First, we need to define the Φ and Λ functions for the Lucas sequence.

Definition 1.5.2. For a positive integer $n = \prod_{i=1}^{k} p_i^{a_i}$ and a positive integer D with $(D, n) = 1$, define the Euler-Lucas Φ-function by

$$\Phi_D(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - (D|p_i))$$

and the Carmichael-Lucas Λ-function by

$$\Lambda_D(n) = \text{LCM}\{p_1^{a_1-1}(p_1 - (D|p_1)), ..., p_k^{a_k-1}(p_k - (D|p_k))\}.$$

With these definitions, we have the Euler-Lucas and Carmichael-Lucas Theorems. A complete development and proof of these theorems can be found in [49].

Theorem 1.5.6. *Euler-Lucas and Carmichael-Lucas Theorems.*

If n is a positive integer and $U_k = U_k(P, Q)$ has discriminant D with $(D, n) = 1$, then

$$U_{\Lambda_D(n)} \equiv 0 \ (mod\ n) \ \textit{and}$$

$$U_{\Phi_D(n)} \equiv 0 \ (mod\ n).$$

The previous two theorems combined give the following corollary.

Corollary 1.5.7. *If n is a positive integer, then $\omega(n; P, Q)|\Lambda_D(n)$ and, consequently, $\omega(n; P, Q)|\Phi_D(n)$.*

Note for prime values we have $\omega(p^a; P, Q)|p^{a-1}(p - (D|p))$.

1.6 Computational Considerations

In the previous sections, we have described tools for primality testing which either used (1) exponentiation of integers or (2) values of Lucas sequences. If these operations could not be done efficiently, then they would be useless in practice. However, there are efficient, $O(\log(n))$ operation, algorithms for computing (1) and (2).

The standard exponential method for integers is well-known and is accurately called the method of successive squaring. For Lucas sequences, we use a similar idea. In fact, by making use of the following theorem, we can use the same algorithm where multiplication of integers is replace by multiplication of matrices.

Theorem 1.6.1. *If P and Q are the parameters for the Lucas sequences U_k and V_k, then* $\begin{bmatrix} U_{n+1} \\ U_n \end{bmatrix} = \begin{bmatrix} P & -Q \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ *and* $\begin{bmatrix} V_{n+1} \\ V_n \end{bmatrix} = \begin{bmatrix} P & -Q \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} P \\ 2 \end{bmatrix}$.

Although there are faster implementations for calculating values of the Lucas sequences, fast exponentiation by successive squaring of a matrix is an efficient method which is easy to implement on most mathematical software packages.

Exponentiation of integers and calculation of values of Lucas sequences are both $O(\log(n))$ operations. However, using optimal methods, calculation of values of Lucas sequences takes about twice as much time as integer exponentiation.

1.7 Commutative Rings

Much of the theory concerning Lucas sequences is also true when P and Q are chosen out of a commutative ring with identity. In Chapter 7, we investigate this idea in general. We assume the reader has a basic knowledge of the definition of rings. Here we recall some of the concepts in ring theory that are central to our study. As is standard, we define the following notations.

Definition 1.7.1. If $\mathbb{R}$ is a commutative ring with identity, $\mu \in \mathbb{R}$ and k is a non-negative integer, then

- $k\mu = \underbrace{\mu + \mu + \cdots + \mu}_{k \text{ times}}$
- $\mu^k = \underbrace{\mu \cdot \mu \cdots \mu}_{k \text{ times}}.$

For the study of Lucas sequences in primality testing, the essential property satisfied by commutative rings with identity is the binomial theorem given below.

Theorem 1.7.1. *If $\mathbb{R}$ is a commutative ring with identity, $\mu, \nu \in \mathbb{R}$ and n is a positive integer, then*

$$(\mu + \nu)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) \mu^k \nu^{n-k}.$$

We also discuss finite fields as an important class of commutative rings with identity. For a prime p, the set $\{0, 1, 2, \ldots, p-1\}$ with arithmetic modulo p is the finite field denoted by $\mathbb{F}_p$. This is the simplest type of finite field and is often used without even the mention of the word field. The finite fields which we use in Chapter 7 have p^k elements for p a prime and k a positive integer. The remainder of this section discusses the creation and representation of finite fields with p^k elements. If the prime p is replaced by an arbitrary positive integer n in the following development, then we are back in the setting of a commutative ring with identity.

Definition 1.7.2. Given a positive integer n, let $f(x)$ be a polynomial in the ring $\mathbb{Z}_n[x]$ of degree $k > 0$. We define the following quotient ring notation $\mathbb{Z}_n[x]/(f(x))$ to represent

$$\{a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} |\ a_0, a_1, \ldots, a_{k-1} \in \mathbb{Z}_n \text{ where } k \text{ is the degree of } f(x)\}$$

where arithmetic is modulo $f(x)$ and n. If n is a prime and $f(x)$ is irreducible, then $\mathbb{Z}_n[x]/(f(x)) = \mathbb{F}_n[x]/(f(x))$ is a field with n^k elements.

Quotient rings in general are not commonly discussed in the literature since they fail to possess many of the useful properties of fields. Nonetheless, the definition for the quotient ring here is valid. In [19], a brief discussion of this fact can be found in the section concerning ideals and factor rings.

Most major computer algebra systems contain packages to implement the arithmetic of the finite quotient rings described above. For ease of implementation, we have found it convenient to use the following representation of the finite ring $\mathbb{Z}_n[x]/(f(x))$. If we write $f(x) = x^d + f_{d-1}x^{d-1} + \cdots + f_1 x + f_0$, then it is useful to consider the companion matrix

$$X = \begin{bmatrix} 0 & 0 & \cdots & 0 & -f_0 \\ 1 & 0 & \cdots & 0 & -f_1 \\ 0 & 1 & \cdots & 0 & -f_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -f_{d-1} \end{bmatrix}.$$

Note that $f(x)$ is the characteristic polynomial of X. Thus, by the Cayley-Hamilton Theorem, $f(X) = 0$, *i.e.* $X^d = -f_{d-1}X^{d-1} - \cdots - f_1X - f_0I$.

Using this matrix, we can do arithmetic in the finite ring using matrices modulo n. We summarize this fact in the following theorem.

Theorem 1.7.2. *The mapping* $a_0+a_1x+\cdots+a_{n-1}x^{n-1} \mapsto a_0I+a_1X+\cdots+a_{n-1}X^{n-1}$ *is a ring isomorphism from* $\mathbb{Z}_n[x]/(f(x))$ *onto* $\{a_0I+a_1X+\cdots+a_{n-1}X^{n-1} | \, a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_n\}$*, where the matrix arithmetic is modulo* n.

While implementing finite rings using matrices may not be the fastest technique, it allows for quick and easy programming. When running many primality tests with varied methodologies this is a desirable trait. In addition, the matrix viewpoint of finite rings eliminates the need for reduction modulo a polynomial.

Chapter 2

Classical Probable Primality Tests

Over the last several decades, the ability to find large primes quickly has become an essential part of several cryptographic algorithms. As a result, many methods have been proposed to solve this problem. Some methods are more than a century hold, but have been re-energized by the need in cryptography and the speed of computers. The majority of primality tests in use stem from Fermat's Little Theorem. Here we give an overview of these tests, how they work, and the current literature on this topic. Then we will discuss classical tests based on Lucas sequences. In later chapters, we will extend the theory of testing based on Lucas sequences.

2.1 Fermat Tests

We stated and proved Fermat's Little Theorem in Theorem 1.3.1, but we restate it below for convenience.

Theorem 2.1.1. *Fermat's Little Theorem.*

If n is a prime and a is a positive integer with $(a, n) = 1$, then $a^{n-1} \equiv 1$ $(mod\ n)$.

The converse of Fermat's Little Theorem is false. For example, $n = 341 = 11 \cdot 31$ is a composite and $2^{340} \equiv 1$ $(mod\ 341)$. In fact, 341 is the first composite integer to satisfy this congruence (the next two are 561 and 645). Certainly without the aid of a computer, we may have conjectured that the converse was true long before we computed all the integers out to 341. However, the converse is not true and the numbers occur far too frequently to be disregarded.

A *pseudoprime* to the base a (or psp(a)) is a composite integer n such that $a^{n-1} \equiv 1$ $(mod\ n)$. In older publications, the term pseudoprimes is often synonymous with the psp(2). We use the term broadly. The term pseudoprime in general will refer to a composite integer which satisfies a given set of congruences with respect to specific parameters. Here psp(a) refers to a composite integer satisfying Fermat's Little Theorem congruence with respect to a.

With any primality test it is useful to get some sort of count on the number of parameters that yield a specific composite integer as a pseudoprime. For the primality test based on Fermat's Little Theorem, we have the following. (For a proof see [13])

Theorem 2.1.2. *If $n = \prod_{i=0}^{k} p_i^{\alpha_i}$ is the prime factorization of the positive integer, n, then the number of distinct bases a $(mod\ n)$ for which n is a psp(a) is*

$$\prod_{i=0}^{k} (n - 1, p_i - 1).$$

A logical idea would be to use more than one base, that is run the test with $a = 2, 3, 5,$ etc. Such attempts are foiled by the existence of positive integers n which are pseudoprimes to every base satisfying $(a, n) = 1$. These pseudoprimes are called Carmichael numbers and have been studied in detail, see [5], [44]. In fact, Carmichael numbers have been completely characterized by their prime factorization [29].

Theorem 2.1.3. *The positive integer n is a Carmichael number if and only if n is a composite, square-free positive integer satisfying $p - 1 | n - 1$ for every prime divisor p of n.*

In 1994, Alford, Granville, and Pomerance [5] proved that there are infinitely many Carmichael numbers. This was a long standing question that was conjectured in 1910 by Carmichael. Given $k \geq 3$, it is still an open question as to whether there are infinitely many Carmichael numbers having exactly k prime factors. It is not even known if there exist infinitely many Carmichael numbers which are the product of exactly three prime factors [49]. Several methods for constructing Carmichael numbers are known, but, for many, it is not known if they can be infinitely extended. See [44] for a relatively recent discussion on the construction of Carmichael numbers.

Slight modifications of the Fermat based test can eliminate the possibility of Carmichael numbers. The two standard fixes are the Euler Probable Prime and the Strong Probable Prime Tests. The Euler Probable Prime test uses the Euler criterion given here.

Theorem 2.1.4. *Euler Criterion.*

If n is a prime and a is a positive integer such that $(n, a) = 1$, then

$$a^{(n-1)/2} \equiv (a|n)\ (mod\ n).$$

If n is a composite integer and $(n, a) = 1$ such that $a^{(n-1)/2} \equiv (a|n)\ (mod\ n)$, then we say n is an Euler pseudoprime with respect to a, epsp(a). The Strong Probable Prime test uses the following theorem.

Theorem 2.1.5. *Strong Criterion.*

Let n be a prime and write $n - 1 = 2^s d$ where $2 \nmid d$. Let a be a positive integer such that $n \nmid a$. Then one of the following congruences holds

$$a^d \equiv 1\ (mod\ n)\ or$$

$$a^{2^r d} \equiv -1\ (mod\ n),\ for\ some\ r, 0 \leq r \leq s.$$

If n is a composite integer and $(n, a) = 1$ such that the Strong Criterion is satisfied, then we say n is a strong pseudoprime with respect to a, spsp(a). For a composite integer n, it is known (often called the Rabin-Monier theorem) that the number of bases a for which n is a spsp(a) and $0 < a < n$ with $(a, n) = 1$ is less than $\phi(n)/4$. Thus, for a composite integer n at most one quarter of the bases give n as a strong pseudoprime. It is also known that this is a tight bound. That is, there exist composite integers n that have exactly $\phi(n)/4$ bases giving n as a strong pseudoprime.

It is not difficult to show that if n is a strong pseudoprime to the base a, then it is an Euler pseudoprime to the base a. Thus, the strong test is in fact the best of the above three, as the name suggests. Most probable prime tests implemented on computers today are simply implementations of the strong probable prime test where the test is run several times with different bases.

The most commonly implemented primality test is known as the Miller-Rabin primality test. This test was developed and investigated in [34], [35], and [48]. Here we give a brief description of this test. Given an integer n to test, an integer b_1 is chosen with $0 < b_1 < n$. If n satisfies the conclusions of Theorem 2.1.5 with respect to b_1, then another integer base $b_2 \neq b_1$ is chosen. We continue using the Strong Probable Prime Test for several bases, either randomly chosen or from a predetermined set of bases. If the integer n passes the test for several bases, then we have high confidence that n is a prime. Many implementations simply use the bases 2, 3, 5, 7, and 11. Some use more prime bases.

The following theorem gives a theoretic count on the number of bases that are necessary to give a deterministic test based on the Generalized Riemann Hypothesis (GRH). We do not introduce the GRH here. N. Koblitz [29] gives a longer introduction to this subject.

Theorem 2.1.6. *If the GRH is true, and if n is a composite odd integer, then n fails the Miller-Rabin test for at least one base b less than $2log^2(n)$.*

The Miller-Rabin test is widely accepted as an effective form of primality testing. However, the theory still has many loose ends. In [6], [9], [10], and [28] methods are given for constructing composite integers that are strong pseudoprimes for many bases. Generally it is possible to construct composite integers which pass the Miller-Rabin for any given fixed set of bases [6]. In particular, [9] gives a composite which is a strong pseudoprimes for all forty-six prime bases up to 200.

Another aspect of research has been the analytical investigation of the distribution of pseudoprimes. Define $\theta_a(x)$ to be the number of pseudoprimes to the base a not exceeding x. Note that we are not discussing strong pseudoprimes. C. Pomerance [45], [46], improving on the results of [32] and [17], proved the following bounds

$$\exp\{(\log x)^{15/37}\} \leq \theta_a(x) \leq x \cdot \exp\{-\log x \log \log \log x/\log \log x\}.$$

Similar bounds are known for Euler pseudoprimes and Strong pseudoprimes.

As the literature shows, Fermat based testing is effective, but has several theoretical flaws. The introduction of Lucas sequences in primality testing seems to open up more directions in primality testing research. In addition, numerical evidence seems to suggest that Lucas sequence based testing is more effective in identifying composites. For the remainder of this text we view primality testing through the eyes of Lucas sequences.

2.2 Lucas Sequence Tests

Edouard Lucas was the first to suggest using the recurrence sequences which now bear his name to test integers for primality [31]. He was interested in deterministic tests that worked for specific classes of integers. However, probable primality tests based on Lucas sequences was not a major research area until the late 1970's.

In 1980, Baillie and Wagstaff gave a thorough treatment of the use of Lucas sequences in primality testing [13]. They specifically examined the following four congruences.

Theorem 2.2.1. *Lucas Criteria.*

Let n be an odd prime and P and Q be integers. If $(n, Q) = 1$, then

1. $U_{n-(D|n)}(P, Q) \equiv 0$ *(mod n).*
2. $V_{n-(D|n)}(P, Q) \equiv 2Q^{(1-(D|n))/2}$ *(mod n).*
3. $U_n(P, Q) \equiv (D|n)$ *(mod n).*
4. $V_n(P, Q) \equiv P$ *(mod n).*

A composite integer n which satisfies congruence i in the theorem above is called a Lucas pseudoprime with respect to the parameters P and Q and congruence i (or $\text{lpsp}_i(P, Q)$) for $i = 1, 2, 3$, or 4. Most results about Lucas pseudoprimes refer to Congruence 1 which seems to be more approachable theoretically. For this reason, we define $\mathrm{lpsp}(P,Q) = \mathrm{lpsp}_1(P,Q)$. However, numerical evidence seems to suggest that the other congruences are much better at detecting composite numbers in practice. We will summarize the results known about $\mathrm{lpsp}(P,Q)$.

Lucas pseudoprimes were studied and tabulated by Pomerance, Selfridge and Wagstaff [46], as well as Baillie and Wagstaff [13]. Various methods for choosing parameters have been investigated. Theoretically, few explanations are known for the reason that one method of choosing parameters is better than another, but extensive numerical data suggests that certain methods allow very few pseudoprimes.

Given a composite integer n, there is some useful information known about the number of parameters that give n as a pseudoprime. For a fixed D value, the number of parameter pairs (P,Q) which lead to a pseudoprime for a given composite n is characterized by the following formula which is similar to Theorem 2.1.2. See [13] for a proof.

Theorem 2.2.2. *Let D be a fixed positive integer and let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ be an odd positive integer with $(D,n) = 1$. Then the number of distinct values of P modulo n, for which there is a Q such that $P^2 - 4Q \equiv D \ (mod\ n)$ and $U_{n-(D|n)}(P,Q) \equiv 0 \ (mod\ n)$ is*

$$\prod_{i=1}^{k} [(n - (D|n), p_i - (D|p_i)) - 1].$$

It should be noted that if we also require $(2DPQ, n) = 1$, then we can prove that the formula becomes $\prod_{i=1}^{k} [(n - (D|n), p_i - (D|p_i)) - 2]$. In practical implementations, if the chosen parameters are not relatively prime to n, then we would immediately discover that n is composite and there would be no need to test. Thus, this seems to be a more appropriate count. To my knowledge, this fact is not noted in the literature.

An odd integer n is a Carmichael-Lucas number associated with D if it is a lpsp(P, Q) for all integers P and Q such that $(P, Q) = 1$, $P^2 - 4Q = D$, and $(n, QD) = 1$. The concept of Carmichael-Lucas numbers are studied, in [58], as an analog to the Carmichael numbers of the standard Fermat Test. As with Carmichael numbers, these numbers possess specific prime factorizations.

Theorem 2.2.3. *If n is a Carmichael-Lucas number associated with D, then $(p - (D|p))|(n - (D|n))$ for every prime divisor p of n.*

The questions of the existence of an infinite number of Carmichael-Lucas numbers with respect to a fixed D is still an open question. It should be noted that if n is a Carmichael-Lucas number with respect to $D = 1$, then it is a Carmichael number. Thus, any result in this direction would be a generalization of the result concerning Carmichael numbers in [5] (which in itself took 84 years to prove).

As with the Fermat based tests, the Lucas sequence congruences of Theorem 2.2.1 have been improved to create Euler Lucas and Strong Lucas Tests. We summarize these tests here.

Theorem 2.2.4. *Euler Lucas Criterion.*

Let P and Q be given and $D = P^2 - 4Q$. If n is an odd prime and $(n, QD) = 1$, then

$$U_{(n-(D|n))/2} \equiv 0 \ (mod\ n) \ when\ (Q|n) = 1 \ and$$

$$V_{(n-(D|n))/2} \equiv 0 \ (mod\ n) \ when\ (Q|n) = -1.$$

If n is a composite integer with integers P and Q satisfying the conditions of the Euler Lucas Criterion, then we say n is an Euler Lucas pseudoprime with respect to (P, Q), elpsp(P, Q). The Strong Lucas Probable Prime test uses the following theorem.

Theorem 2.2.5. *Strong Lucas Criterion.*

If n is an odd prime with $(n, QD) = 1$ and $n - (D|n) = 2^s d$ with d odd, then

$$U_d \equiv 0 \ (mod\ n) \ or$$

$$V_{2^r d} \equiv 0 \ (mod\ n) \ for\ some\ r, 0 \leq r < s.$$

As with Fermat based tests, if n is a Strong Lucas pseudoprime, then it is also an Euler Lucas pseudoprime. If n is a composite integer with integers P and Q satisfying the conditions of the Strong Lucas Criterion, then we say n is an Strong Lucas pseudoprime with respect to (P, Q), slpsp(P, Q). For a fixed composite integer n and an integer D with $(D, n) = 1$, F. Arnault [8] proved that the number of bases (P, Q) for which $0 \leq P, Q < n$, $P^2 - 4Q \equiv D$ $(mod\ n)$, $(Q, n) = 1$ and n is a slpsp(P, Q) is less than $\frac{4}{15}n$ except if n is the product of twin primes. He also proved that the number of parameters is less than $n/2$ in any case. This is actual not as good a bound as the case of the Fermat based probable prime test. However, numerical evidence suggests that Lucas sequence based tests are better. This is the first of many instances where the results proved in theory seem to be inadequate compared to the results seen in experimentation.

Towards this end, we believe that the generalizations given in later chapters will allow for the proving of better bounds. In particular, we take the first step towards such bounds in Chapter 3. We actually prove a bound on the parameters of $\phi(n)/2$ for a congruence analogous to Congruence 1. Thus, we get a better bound before we have even used any sort of strong primality testing.

Concerning the distribution of Lucas pseudoprimes, much less is known. Define $\vartheta_{P,Q}(x)$ to be the number of lpsp(P, Q)'s not exceeding x. Note that we are only discussing Congruence 1. Baillie and Wagstaff [13] and Erdös, Kiss and Sárközy [18] give the following upper and lower bounds, respectively. For x sufficiently large, there exist positive constants c_1 and c_2 such that

$$\exp\{(\log x)^{c_1}\} \leq \vartheta_{P,Q}(x) \leq x \cdot \exp\{-c_2(\log x \log\log x)^{1/2}\}.$$

Very little has been proved about the Congruences 2, 3, and 4 of the Lucas Criteria. In this work, we give these congruences more attention. Numerically we show that generalizations of these congruences are quite good at identifying composites.

It should be noted that several individuals have investigated the idea of using a Strong Lucas based test and then using a Strong Fermat based test. For appropriate choices in parameters, there are no known examples of pseudoprimes that satisfy both of these tests. However, proving that no such number exist has been difficult. We hope that the extensions made in this work will aid in the exploration of these open questions.

2.3 Other Probabilistic Primality Tests

In subsequent chapters, we investigate and extend primality tests based on Lucas sequences. By studying such tests, we will be exposed to the types of problems often encountered in the theory of pseudoprimes. Here we give a brief overview of other extensions in primality testing which we will not be discussing.

Lucas sequences are second order linear recurrence sequences with specific initial conditions. It seems natural to ask if recurrence sequences of higher order may be effective in primality testing. The articles [1], [2], [11] and [30] study tests based on specific third order recurrence sequences. These sequences are a generalization of the so-called Perrin sequence. It is known that certain values of this sequence satisfy special congruences relations modulo a prime. Although these tests are not computationally as efficient, experimental evidence suggests they provide extremely reliable tests. However, it has been shown that their exists an infinite number of pseudoprimes with respect to the Perrin sequence [24]. Similar primality tests for more general higher order recurrence sequences have been investigated by Gurak [26].

All the tests described so far involve computations with integers. The restriction to computation with integers is not necessary and the subject of cryptography, and specifically primality testing, has benefited from computations using finite fields and rational points on elliptic curves.

J. Grantham [22], [23] makes extensive use of finite fields to give a general testing method called Frobenius Primality Test. Computations in finite fields can be more cumbersome, but Grantham offers effective tests which are provably stronger than many of the known primality testing algorithms. His parameters are polynomials in a finite field (a finite ring if n is a composite). In particular, he proves that one such test will allow a composite integer n to pass for less than 1/7710 of the possible polynomial parameters of a given type. We will be using finite fields in a different way in Chapter 7. The key disadvantage in any such method is the computation. It seems desirable to confine the computations to integers when possible.

Rational points on elliptic curves are most well-known for their use as tools in primality proving and integer factoring. Many of the fastest deterministic algorithms for both these questions involve elliptic curves. Probabilistic primality testing on elliptic curves is a relatively new topic with a growing wealth of research. Using elliptic curves to give probabilistic primality tests and the distribution of pseudoprimes for such tests is discussed in [20], [21].

Chapter 3

Lehmer Pseudoprimes

D.H. Lehmer [33] investigated the properties of Lucas sequences with the parameter $P = \sqrt{R}$ for some integer R. We explore these Lehmer sequences as tools in primality testing. For an odd composite integer n, we give a formula for the number of parameters giving n as a pseudoprime and an upper bound on this formula. We prove results on connections between different congruences for these sequences, and give extensive numerical data concerning the number of pseudoprimes for various methods of choosing parameters. We note that Lehmer sequences allow for a broader range of parameter choices and a stronger underlying theory than standard Lucas sequences without any increase in computational time.

3.1 Introduction

As noted in previous chapters, some of the most effective probable prime tests are based on congruence relations for second order linear recurrence sequences, also called Lucas sequences. For convenience we recall the definition of Lucas sequences of the first kind as defined in Chapter 2:

$$U_0 = 0, U_1 = 1 \text{ and } U_k = PU_{k-1} - QU_{k-2} \text{ for } k \geq 2,$$

where P and Q are integer parameters. Lucas sequences of the second kind, V_k, satisfy the same recurrence but have initial values $V_0 = 2$ and $V_1 = P$. The discriminant is $D = P^2 - 4Q$.

In [33], Lehmer studied extended Lucas sequences where the integer parameter P is replaced by the parameter $\sqrt{R}$, for an integer R. The discriminant for such sequences will be denoted by $D = R - 4Q$. Lehmer proved that these extended sequences, or Lehmer sequences, possess properties similar to the ordinary sequences with respect to rank of appearance. In addition, Lehmer sequences satisfy all of the same identities as given in Section 1.5 for Lucas sequences.

Thus, formally we define $U_k = U_k(\sqrt{R}, Q)$ and $V_k = V_k(\sqrt{R}, D)$ where $R, Q \in \mathbb{Z}$, by:

$$U_0 = 0, U_1 = 1, U_k = \sqrt{R}U_{k-1} - QU_{k-2} \text{ for } k \geq 2$$

$$V_0 = 2, V_1 = \sqrt{R}, V_k = \sqrt{R}V_{k-1} - QV_{k-2} \text{ for } k \geq 2.$$

These sequences satisfy the Binet formulas:

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} \text{ and } V_k = \alpha^k + \beta^k$$

where $\alpha, \beta = (\sqrt{R} \pm \sqrt{D})/2$.

In particular, we shall often choose R to be a non-square, so $U_k \in \mathbb{Z}$ if and only if $2 \nmid k$, $(k > 0)$, and $V_k \in \mathbb{Z}$ if and only if $2|k$.

We view the symbol $\sqrt{R}$ in the following way. We never evaluate $\sqrt{R}$, it formally represents an object that is equal to R when it is squared. In addition, we define $a\sqrt{R} + b \equiv c\sqrt{R} + d$ $(mod\ n)$ if $a \equiv c$ $(mod\ n)$ and $b \equiv d$ $(mod\ n)$.

The key advantages of Lehmer sequences are two-fold. First, the Binet formulas, $(\sqrt{R} \pm \sqrt{D})/2$, have symmetry in R and D, which allows for ease in comparison of various congruences. Secondly, since $D = R - 4Q$ the values for R, D, and Q can be chosen in any congruence class modulo 4. In the case $D = P^2 - 4Q$, we must have $D \equiv 0$ or 1 $(mod\ 4)$. Thus, we get a wider variety in parameter choices and a sequence which is easier to analyze theoretically. We further clarify these advantages as the chapter proceeds.

First we will derive congruence relations for these sequences similar to those of Theorem 2.2.1, which concerned standard Lucas sequences. In fact, by making the substitution $R = P^2$, our result is a direct generalization of Theorem 2.2.1. Using the Binet formulas, if n is an odd prime, one can obtain relations for U_{n-1}, V_{n-1}, U_n, V_n, U_{n+1}, etc.

Perhaps the easiest way to generate any such formula is to compute U_n and V_n and then use the well known identities given in Theorem 1.5.2. We use this technique to prove the following congruence relations which are central to much of this study.

Theorem 3.1.1. *Lehmer Criteria.*

If n is an odd prime and $(RQ, n) = 1$, then

1. $U_{n-(RD|n)}(\sqrt{R}, Q) \equiv 0 \ (mod\ n)$.

2. $V_{n-(RD|n)}(\sqrt{R}, Q) \equiv 2(R|n)Q^{(1-(RD|n))/2} \ (mod\ n)$.

3. $U_n(\sqrt{R}, Q) \equiv (D|n) \ (mod\ n)$.

4. $V_n(\sqrt{R}, Q) \equiv (R|n)\sqrt{R} \ (mod\ n)$.

Proof. For any integer k, from Theorem 1.5.4, we have the following identities:

$$2^{k-1}U_k = \sum_{i\ odd} \begin{pmatrix} k \\ i \end{pmatrix} R^{(k-i)/2} D^{(i-1)/2}$$

$$2^{k-1}V_k = \sum_{i\ even} \begin{pmatrix} n \\ i \end{pmatrix} R^{(k-i)/2} D^{i/2}.$$

Using the characterization of primes via binomial coefficients (Theorem 1.2.1), we replace k by n in the above sums and eliminate terms congruent to zero modulo n. This yields Congruences 3 and 4 of the theorem.

$$U_n \equiv 2^{n-1}U_n \equiv D^{(n-1)/2} \equiv (D|n) \ (mod\ n)$$

$$V_n \equiv 2^{n-1}V_n \equiv R^{n/2} \equiv R^{(n-1)/2}\sqrt{R} \equiv (R|n)\sqrt{R} \ (mod\ n).$$

Recalling the identities of Theorem 1.5.2

$$2U_{n+1} = V_1U_n + U_1V_n, \quad 2V_{n+1} = V_1V_n + DU_1U_n$$

$$2QU_{n-1} = V_1U_n - U_1V_n, \quad 2QV_{n-1} = V_1V_n - DU_1U_n$$

and combining them with congruences 3 and 4 we obtain

$$2U_{n+1} \equiv [(D|n) + (R|n)]\sqrt{R}, \quad 2V_{n+1} \equiv [(D|n) + (R|n)]R - 4(D|n)Q \ (mod\ n)$$

$$2QU_{n-1} \equiv [(D|n) - (R|n)]\sqrt{R}, \quad 2QV_{n-1} \equiv [(D|n) - (R|n)]R + 4(D|n)Q \ (mod\ n).$$

By examining the separate cases it is not difficult to see that

$$U_{n-(RD|n)} \equiv 0 \ (mod\ n) \text{ and}$$

$$V_{n-(RD|n)} \equiv 2(R|n)Q^{(1-(RD|n))/2} \ (mod\ n).$$

□

A composite integer n which satisfies congruence i in the theorem above is called a Lehmer pseudoprime with respect to the parameters R and Q and congruence i (or lehpsp$_i(R,Q)$) for $i = 1, 2, 3,$ or 4. Before using these congruences in primality testing, it is useful in practice to discuss how the terms of this sequence can be efficiently computed. Even though not all of the terms are integers, we can use auxiliary integer sequences to compute the terms of U_k and V_k.

Definition 3.1.1. Define the auxiliary sequences W_k, X_k, Y_k, and Z_k as follows: $W_k = U_{2k}/\sqrt{R}$, $X_k = U_{2k+1}$, $Y_k = V_{2k}$, and $Z_k = V_{2k+1}/\sqrt{R}$.

Given the definitions above we have the following properties:

- $W_k = (R-2Q)W_{k-1} - Q^2W_{k-2}, \quad W_0 = 0, W_1 = 1.$

- $X_k = (R-2Q)X_{k-1} - Q^2X_{k-2}, \quad X_0 = 1, X_1 = R-Q.$

- $Y_k = (R-2Q)Y_{k-1} - Q^2Y_{k-2}, \quad Y_0 = 2, Y_1 = R-2Q.$

- $Z_k = (R-2Q)Z_{k-1} - Q^2Z_{k-2}, \quad Z_0 = 1, Z_1 = R-3Q.$

Using successive squaring of matrices as discussed in Section 1.6, sequences of this type can be computed in $\mathrm{O}(\log(n))$ operations. To test the congruences in the Lehmer criteria we use the following corollary.

Corollary 3.1.2. *Let W_k, Y_k, X_k, and Z_k be defined as above. If n is an odd prime and $(RQ, n) = 1$, then*

1. $W_{(n-(RD|n))/2} \equiv 0$ *(mod n).*

2. $X_{(n-(RD|n))/2} \equiv 2(R|n)Q^{(1-(RD|n))/2}$ *(mod n).*

3. $Y_{(n-1)/2} \equiv (D|n)$ *(mod n).*

4. $Z_{(n-1)/2} \equiv (R|n)\sqrt{R}$ *(mod n).*

As with any of the primality tests so far it is important to note that the relations above are not sufficient conditions for n being prime.

Various results are known about Lehmer pseudoprimes and can be found in [51], [52], [53], [54], and [59]. In [54], Rotkiewicz and Wasén investigate composite numbers satisfying a related congruence $V_{\frac{1}{2}(n-(RD|n))} \equiv 0 \ (mod\ n)$. In [51] and [52], Rotkiewicz studied Euler Lehmer Pseudoprimes and Strong Lehmer Pseudoprimes which we will discuss in Chapter 4. These studies focus mainly on the number of pseudoprimes in a designated arithmetic progression. In essence, the major results on Lehmer pseudoprimes all are concerned with proving that there are infinitely many Lehmer pseudoprimes and Strong Lehmer pseudoprimes under various conditions. These results are only concerned with Congruence 1 of the Lehmer Criteria. In fact, we have yet to find any literature that discusses Congruences 2, 3, and 4 of the Lehmer Criteria.

In this chapter, we add to the theory by:

(1) Counting the parameters that yield a pseudoprime for Congruence 1 and bounding this count.

(2) Articulating connections between the various congruences.

(3) Providing extensive numerical data illustrating the effectiveness of Lehmer sequences in primality testing.

We make the case that using Lehmer sequences over standard Lucas sequences allows for a more robust set of probable primality tests.

3.2 A Formula for the Number of Parameters Yielding a Pseudoprime

If n is composite, the effectiveness of a test detecting this fact depends on the number of parameters for which the congruence holds versus the number for which it fails.

Suppose $n = \prod_i p_i^{a_i}$ is odd, and D is chosen such that $(D, n) = 1$. After Theorem 2.2.2, we stated that the number of distinct values of P $(mod\ n)$ for which $(P, n) = 1$ and $U_{n-(D|n)}(P, Q) \equiv 0$ $(mod\ n)$ is $\prod_i [(n - (D|n), p_i - (D|p_i))) - 2]$. The situation for $U_{n-(RD|n)}(\sqrt{R}, Q)$ is more complicated because of the dependence on the value of $(RD|n)$, not just $(D|n)$.

We will denote the rank of $U_k(A, B)$ modulo m, that is the lease positive k such that $m|U_k$, by $\omega(m; A, B)$.

Lemma 3.2.1. *If p is an odd prime, $(R(R - Q), p) = 1$, and $0 < c < p$, then*

$$\omega(p^a; \sqrt{R}, Q) = \omega(p^a; cR, c^2QR).$$

Proof. Let $\alpha_1, \beta_1 = \frac{1}{2}(\sqrt{R} \pm \sqrt{R - 4Q})$ so that $U_k(\sqrt{R}, Q) = (\alpha_1^k - \beta_1^k)/(\alpha_1 - \beta_1)$. Then $U_k(cR, c^2QR) = (\alpha_2^k - \beta_2^k)/(\alpha_2 - \beta_2)$ where $\alpha_2, \beta_2 = \frac{1}{2}(cR \pm \sqrt{c^2R + 4c^2QR}) = c\sqrt{R}\alpha_1, c\sqrt{R}\beta_1$.

Then $p^a|U_k(\sqrt{R}, Q)$ if and only if $p^a|(\alpha_1^k - \beta_1^k)$ if and only if $p^a|(\alpha_2^k - \beta_2^k)$ if and only if $p^a|U_k(cR, c^2QR)$. □

Note that the discriminants of the two sequences in Lemmas 3.2.1 are $D_1 = R-4Q$

and $D_2 = c^2R^2 - 4c^2QR = c^2RD_1$. So $(D_2|p) = (c^2RD_1|p) = (R|p)(D_1|p)$.

Lemma 3.2.2. *If p is an odd prime, a is a positive integer and D is fixed such that $(D, p) = 1$, then for $0 < R < p^a$, $(R - D, p) = 1$ and $0 < c < p^a$, $(p, cR) = 1$, the sequences $U_k(cR, c^2QR)$ represent uniquely, modulo p^a, every sequence $U_k(A, B)$ where $(AB(A^2 - 4B), p) = 1$.*

Proof. Given such integers A and B, we need to show that there exists a unique solution for c $(mod\ p^a)$ of the congruence system below.

$$cR \equiv A\ (mod\ p^a)$$

$$c^2QR \equiv B\ (mod\ p^a)$$

Taking the second congruence and dividing by the first gives $cQ \equiv B/A\ (mod\ p^a)$. Hence, $A - cD \equiv cR - cD \equiv 4cQ \equiv 4B/A\ (mod\ p^a)$ and so

$$c \equiv \frac{A^2 - 4B}{AD}\ (mod\ p^a) \text{ and}$$

$$R \equiv \frac{A}{c} \equiv \frac{A^2D}{A^2 - 4B}\ (mod\ p^a).$$

□

For a fixed D value we will now count the number of distinct values of R modulo p such that $\omega(p; \sqrt{R}, Q) = d$. The cases $(R|p) = +1$ and $(R|p) = -1$ are essentially the same, so suppose $(R|p) = +1$. Let k be the number of such R. The one to $p-1$ correspondence between $U(\sqrt{R}, Q)$ and $U(cR, c^2RQ)$, $1 \leq c \leq p-1$, in Lemma

3.2.2, produces $k(p-1)$ sequences which constitute all $U(A,B)$ with rank d and all discriminants $D_2 = A^2 - 4B$ such that $(D_2|p) = (D|p) = +1$. There are $(p-1)/2$ such D_2.

By Theorem 2 of [58], there are $\phi(d)$ such sequences $U(A,B)$ with a given D_2, and so $\phi(d)(p-1)/2$ sequences in all. Hence, $k(p-1) = \phi(d)(p-1)/2$ or $k = \phi(d)/2$, independent of D.

Thus, we have proved

Lemma 3.2.3. *If p is an odd prime, $\epsilon = \pm 1$, and D is fixed with $(D,p) = 1$, then the number of distinct R values modulo p such that $\omega(p; \sqrt{R}, Q) = d$, where $d|p - (RD|p)$ with $d > 2$, and $(R|p) = \epsilon$ is $\phi(d)/2$.*

Now we have the tools to prove our main result concerning the number of parameters yielding a pseudoprime for a particular positive odd composite integer. Note Q is uniquely determined by R and D.

Theorem 3.2.4. *Parameter Count for lehpsp$_1$(R,Q).*
If $n = \prod_{i=1}^{k} p_i^{a_i}$ is odd and D is fixed with $(D,n) = 1$, then the number of distinct R and Q values modulo n satisfying $R - 4Q \equiv D$ (mod n) for which $U_{n-(RD|n)}(\sqrt{R}, Q) \equiv 0$ (mod n) and

1. *$(R|n) = +1$ is $\sum \prod_{i=1}^{k} \left[\frac{1}{2}(n - (D|n), p_i - x_i(D|p_i)) - 1\right]$.*

   The sum is over all $(x_1, \ldots, x_k) \in \{-1, +1\}^k$ such that $\prod_{i=1}^{k} x_i^{a_i} = +1$.

2. $(R|n) = -1$ *is* $\sum \prod_{i=1}^{k} \left[\frac{1}{2}(n + (D|n), p_i - x_i(D|p_i))) - 1\right]$.

The sum is over all $(x_1, \ldots, x_k) \in \{-1, +1\}^k$ *such that* $\prod_{i=1}^{k} x_i^{a_i} = -1$.

3. Both cases together with the definition $h(x) = \prod_{i=1}^{k} x_i^{a_i}$ *give*

$$\sum_{x \in \{-1,+1\}^k} \prod_{i=1}^{k} \left[\frac{1}{2}(n - h(x)(D|n), p_i - x_i(D|p_i)) - 1\right].$$

Proof. We will treat the case $(R|n) = +1$. The case $(R|n) = -1$ is essentially identical. Since $(R|n) = \prod_{i=1}^{k}(R|p_i)^{a_i} = +1$ consider a specific choice of $(x_1, \ldots, x_k) \in \{-1, +1\}^k$ such that $\prod_{i=1}^{k} x_i^{a_i} = +1$ and $(R|p_i) = x_i$.

Note that $U_{n-(RD|n)}(\sqrt{R}, Q) \equiv U_{n-(D|n)}(\sqrt{R}, Q) \equiv 0 \ (mod\ n)$ if and only if $U_{n-(D|n)}(\sqrt{R}, Q) \equiv 0 \ (mod\ p_i^{a_i})$ for $0 < i \leq k$ if and only if $d = \omega(p_i^{a_i}; \sqrt{R}, Q)$ divides $n - h(x)(D|n) = n - (D|n)$. By Theorems 1.6 and 1.9 of [33], $d = p_i^b \omega(p_i; \sqrt{R}, Q)$ for some $b \geq 0$, which in turn divides $p_i^b(p_i - (RD|p_i)) = p_i^b(p_i - x_i(D|p_i))$.

Now $(n - (D|n), p_i) = 1$ so d divides $(n - (D|n), p_i - x_i(D|p_i))$.

Let $\delta_i = (n - (D|n), p_i - x_i(D|p_i))$. Since $U_n(\sqrt{R}, Q)$ cannot have period 1 or 2 when $(RD, n) = 1$, summing over all such $d > 2$ yields

$$\sum_{\substack{d|\delta_i \\ d>2}} \phi(d)/2 = \frac{1}{2}(n - (D|n), p_i - x_i(D|p_i)) - 1.$$

To count the number of R values for which $U_{n-(D|n)}(\sqrt{R}, Q) \equiv 0 \ (mod\ n)$ with a specific choice of $(x_1, \ldots, x_k)$, by the Chinese Remainder Theorem, we take the product of the above formula over these x_i. Finally, summing over all the possible $(x_1, \ldots, x_k)$ such that $\prod_{i=1}^{k} x_i^{a_i} = +1$, we get the desired result. □

Of the four gcd quantities $(n \pm 1, p \pm 1)$ three are divisible by 2, one is divisible by 2^a for $a \geq 2$ and one is divisible by 3^b for some $b \geq 1$. There may or may not be divisibility by primes greater than 3.

For ordinary Lucas sequences, from Theorem 2.2.2, we see that the number of parameters P producing a pseudoprime depends on only one of these four values for each $p|n$. We do not know whether it will be the largest of these values or not. However, the estimate in Theorem 3.2.4 uses all four of these numbers. The number of parameters involves more of an average of these gcd's. This fact will allow for a better bound on the number of 'bad' parameters.

As mentioned earlier, one benefit of using Lehmer sequences is greater freedom in choosing parameters. Now, R and D can be chosen arbitrarily in any residue class modulo 4. Also, we can choose $(R|n)$ and $(D|n)$ to have any desired ± 1 values. Examining the number of pseudoprimes for various choices of both the parameters and the four congruence relations from Theorem 3.1.1 yields interesting information about how to create very good prime testing methods. Note that these tests can be applied using the auxiliary integer sequences mentioned above and so the computational complexity is essentially the same as previous Lucas testing methods.

Although it is the easiest to analyze, the Congruence 1 used in the preceding theorem is not, in practice, as strong at detecting composite numbers as the other three congruences in Theorem 3.1.1. In the final section of this chapter, we will numerically compare the various congruences and illustrate this fact. But first, we get a bound for the number of 'bad' parameters for a composite integer n and we explore the relationships between the four congruences.

3.3 A Bound on the Number of Parameters Yielding a Pseudoprime

We now use the formulas from the preceding section to get a rough bound on the number of parameters yielding a pseudoprime for a fixed D value. Thus, running the test several times with different parameter sets will give a high probability of success since it would be unlikely to choose a 'bad' parameter several times in a row.

Definition 3.3.1. For an odd composite integer, n, and a fixed integer D with $(D, n) = 1$, we define $\Psi_D(n)$ to be the number of distinct R and Q values modulo n satisfying $R - 4Q \equiv D \ (mod\ n)$ such that $U_{n-(RD|n)}(\sqrt{R}, Q) \equiv 0 \ (mod\ n)$ and $(R, n) = 1$.

If the prime factors of n are known, then $\Psi_D(n)$ is precisely formula 3 of Theorem 3.2.4. In primality testing we are rarely in possession of the prime factors of the integer n we are testing. Here we give a bound on $\Psi_D(n)$ in terms of n, but first we need a lemma concerning gcd values.

Lemma 3.3.1. *If n is an odd integer, k is a positive integer and $\epsilon = \pm 1$, then*

$$(n-1, k-\epsilon) + (n+1, k-\epsilon) \leq 2 + k - \epsilon$$

Proof. The only common factor of $n-1$ and $n+1$ is 2. Thus, $(n-1, k-\epsilon)(n+1, k-\epsilon) \leq 2(k-\epsilon)$ and so $(n+1, k-\epsilon) \leq \frac{2(k-\epsilon)}{(n-1,k-\epsilon)}$. Consider the function $f(x) = x + \frac{2(k-\epsilon)}{x}$ with domain $[2, k-\epsilon]$. Taking two derivatives on $f(x)$ easily shows that it is concave up. Therefore, the maximum is either at $x = 2$ or $x = k - \epsilon$. Both give the same maximum value of $f(x)$ as $2 + k - \epsilon$. □

Now we have the tools to prove the following bound.

Theorem 3.3.2. *Parameter Bound on lehpsp$_1$(R,Q).*

If n is an odd composite integer that is not a perfect square, then

$$\Psi_D(n) < \frac{\phi(n)}{2}.$$

Proof. Write $n = p_1^{2a_1+1} \dots p_r^{2a_r+1} p_{r+1}^{2a_{r+1}} \dots p_k^{2a_k}$. We simplify the formula from Theorem 3.2.4 by factoring out the terms involving p_1.

Note that $(n \pm (D|n), p_i - x_i(D|p_i)) - 2 \leq p_i - 1$.

$$\Psi_D(n) = \frac{1}{2^k} \sum_{x \in \{-1,+1\}^k} \prod_{i=1}^{k} [(n - h(x)(D|n), p_i - x_i(D|p_i)) - 2]$$

$$= \frac{1}{2^k} \sum_{x \in \{-1,+1\}^k} [(n-h(x)(D|n), p_1 - x_1(D|p_1)) - 2] \prod_{i=2}^{k} [(n - h(x)(D|n), p_i - x_i(D|p_i)) - 2]$$

$$< \frac{1}{2^k} \sum_{x \in \{-1,+1\}^k} [(n - h(x)(D|n), p_1 - x_1(D|p_1)) - 2] \prod_{i=2}^{k} (p_i - 1)$$

$$= \frac{1}{2^k} \prod_{i=2}^{k} (p_i - 1) \sum_{x \in \{-1,+1\}^k} [(n - h(x)(D|n), p_1 - x_1(D|p_1)) - 2].$$

Let $\epsilon = \pm 1$ and $\delta = \pm 1$ and notice that the terms in the sum break into the four cases $h(x)(D|n) = \epsilon$ and $x_1(D|p_1) = \delta$. It is easily verified that a fixed choice of ϵ and δ corresponds to exactly 2^{k-2} elements $x \in \{-1, +1\}^k$. Breaking up the sum into the four cases and using Lemma 3.3.1 yields the following upper bound for $\Psi_D(n)$:

$$\frac{1}{2^k}\left[\prod_{i=2}^{k}(p_i-1)\right] 2^{k-2}[(n+1,p_1-1)+(n-1,p_1-1)+(n+1,p_1+1)+(n-1,p_1+1)-8]$$

$$\leq \frac{1}{4}\left[\prod_{i=2}^{k}(p_i-1)\right](2p_1-4) < \frac{\phi(n)}{2}.$$

□

If n is a perfect square, then note that the parameter bound in Theorem 3.2.4 only depends on the prime factors of n and not on the square of such factors. Thus, in this case we actually get a much better bound than $\frac{\phi(n)}{2}$. Therefore, Theorem 3.3.2 actually gives a bound for the worst case.

Hence, for a fixed D value and an odd composite integer, n, the congruence $U_{n-(RD|n)}(\sqrt{R}, Q) \equiv 0 \ (mod\ n)$ is satisfied by at most half of the choices for R. This is a very rough bound, but it shows that one application of this test is accurate at least fifty percent of the time. Applying the test with k different random values of R, the chance that n passes the test each time is $1/2^k$. In Chapter 2, we noted that [8] proves that the number of Strong Lehmer pseudoprimes is less than $n/2$ in general. Using Lehmer sequences, Theorem 3.3.2 shows that this bound can be attained without appealing to strong versions of the congruences.

It should be re-iterated that numerically this congruence appears to be the worst of the four in accuracy of identifying composites. In the following section we compare the relationships between the four congruences given in Theorem 3.1.1.

3.4 Relations Among The Tests

Here we explore the four congruences of Theorem 3.1.1 more deeply to give some information about their relation to each other. We have previously defined the notation $\mathrm{lehpsp}_i(R, Q)$, but in the following section we are more interested in the parameters R and D due to their symmetry in the Binet formulas. Since $Q = \frac{R-D}{4}$, the parameters R and D uniquely determine Q. Thus, defining the sequence in terms of R and D is equivalent. We extend the previously defined notation to include all the parameters simply to allow for ease in comparison of these parameters.

Definition 3.4.1. For an odd composite integer, n, we say n is a Lehmer pseudoprime for congruence i with parameters R, D, and Q, or simply n is a $\mathrm{lehpsp}_i(R, Q, D)$, if n satisfies congruence i of Theorem 3.1.1 for $i = 1$, 2, 3, or 4 and $Q = \frac{R-D}{4}$.

Note $\mathrm{lehpsp}_i(R, Q, D) = \mathrm{lehpsp}_i(R, Q) = \mathrm{lehpsp}_i(R, \frac{R-D}{4})$, depending on whether we know R and Q, or R and D. In addition, we will use the notation $U_k\sqrt{R}, Q, D$ when we are interested in explicitly expressing the parameter D as well. In each of these instances, the notation is only defined for parameters satisfying $D = R - 4Q$.

We investigate the relationships of the congruences by examining the characteristic roots of the Lehmer sequences. The characteristic roots of the Lehmer sequences have a nice symmetry in the quantities R and D. This symmetry makes connections between congruences more transparent than in the case of standard Lucas sequences. We further exploit these properties in Chapter 6.

Theorem 3.4.1. *Parameter Reciprocity of Congruences 1 and 2.*
If n is an odd composite integer, then

i. n is a lehpsp$_1(R, Q, D)$ if and only if n is a lehpsp$_1(D, -Q, R)$.

ii. n is a lehpsp$_2(R, Q, D)$ if and only if n is a lehpsp$_2(D, -Q, R)$.

Proof. We prove the first statement only, the second is proved in a similar way. Let $\alpha, \beta = \frac{\sqrt{R}\pm\sqrt{D}}{2}$ be the characteristic roots of $U_k(\sqrt{R}, Q, D)$. If $\widehat{\alpha}$ and $\widehat{\beta}$ are the characteristic roots of $U_k(\sqrt{D}, -Q, R)$, then $\widehat{\alpha} = \alpha$ and $\widehat{\beta} = -\beta$.

Since $U_k(\sqrt{R}, Q, D) = \frac{\alpha^k - \beta^k}{\sqrt{D}}$, we have n is a lehpsp$_1(R, Q, D)$ if and only if $\alpha^{n-(RD|n)} \equiv \beta^{n-(RD|n)}$ $(mod\ n)$ if and only if $\widehat{\alpha}^{n-(DR|n)} \equiv \widehat{\beta}^{n-(DR|n)}$ $(mod\ n)$ if and only if n is a lehpsp$_1(D, -Q, R)$. □

Notice that the statements in the theorem above are only equivalent because $n - (RD|n)$ is even. In Congruences 3 and 4 the power of the characteristic roots is odd giving a different scenario. The following theorem illustrates that Congruences 3 and 4 are interconnected.

Theorem 3.4.2. *Parameter Bi-Reciprocity Between Congruences 3 and 4.*

If n is an odd composite integer, then n is a lehpsp$_3(R, Q, D)$ if and only if n is a lehpsp$_4(D, -Q, R)$.

Proof. Let $\alpha, \beta = \frac{\sqrt{R}\pm\sqrt{D}}{2}$ be the characteristic roots of $U_k(\sqrt{R}, Q, D)$. If $\widehat{\alpha}$ and $\widehat{\beta}$ are the characteristic roots of $V_k(\sqrt{D}, -Q, R)$, then $\widehat{\alpha} = \alpha$ and $\widehat{\beta} = -\beta$. Thus, we have n is a lehpsp$_3(R, Q, D)$ if and only if $\frac{\alpha^n-\beta^n}{\sqrt{D}} \equiv (D|n)$ $(mod\ n)$ if and only if $\widehat{\alpha}^n + \widehat{\beta}^n \equiv (D|n)\sqrt{D}$ $(mod\ n)$ if and only if n is a lehpsp$_4(D, -Q, R)$. □

If R and D are valid parameters, then D and R are valid parameters. For a given odd composite integer n, we can use Theorem 3.4.2 to conclude that there will be the same number of parameters that will give n as a lehpsp$_3$ and a lehpsp$_4$. Roughly speaking, Congruences 3 and 4 are equally good tests.

Theorem 3.4.1 does not let us make similar connections about Congruences 1 and 2. These congruences appear not to be related. The data will suggest that Congruence 2 is often the best while Congruence 1 is the worst. We can give at least a partial explanation of why Congruence 1 seems to be the least effective test.

Theorem 3.4.3. *Families of Parameters for Congruence 1.*

If n is a lehpsp$_1(R, Q, D)$, then

i. n is a lehpsp$_1(cR, cQ, cD)$ for all c with $(n, c) = 1$.

ii. n is a lehpsp$_1(cD, -cQ, cR)$ for all c with $(n, c) = 1$.

In addition, these families of parameters are different if $D \not\equiv -R$ (mod n).

Proof. Let $\alpha_c, \beta_c = \frac{\sqrt{cR} \pm \sqrt{cD}}{2} = \sqrt{c}\alpha_1, \sqrt{c}\beta_1$. Then $\alpha_1^{n-(RD|n)} \equiv \beta_1^{n-(RD|n)}$ $(mod\ n)$ if and only if $(\sqrt{c}\alpha_1)^{n-(RD|n)} \equiv (\sqrt{c}\beta_1)^{n-(RD|n)}$ $(mod\ n)$ if and only if $\alpha_c^{n-(c^2RD|n)} \equiv \beta_c^{n-(c^2RD|n)}$ $(mod\ n)$. The second claim follows from Theorem 3.4.1.

The family of parameters (cR, cQ, cD) and $(cD, -cQ, cR)$ with $(c, n) = 1$ are equivalent if and only if there exists a particular c_1 and c_2 with $(c_1c_2, n) = 1$ and (1) $c_1R \equiv c_2D$ $(mod\ n)$, (2) $c_1Q \equiv -c_2Q$ $(mod\ n)$, and (3) $c_1D \equiv c_2R$ $(mod\ n)$. Since $(Q, n) = 1$, (2) gives $c_2 \equiv -c_1$ $(mod\ n)$. Substituting this relationship into (1) and (3), we obtain $c_1R \equiv -c_1D$ $(mod\ n)$ and $c_1D \equiv -c_1R$ $(mod\ n)$. Since $(c_1, n) = 1$, either of these give the desired result. □

Thus, if we have one 'bad' set of parameters for a composite integer n and $D \not\equiv -R$ $(mod\ n)$, then we also have $2\phi(n)$ 'bad' sets of parameters. Even if $D \equiv -R$ $(mod\ n)$, then we also have $\phi(n)$ 'bad' sets of parameters. So we should avoid these parameters if we run the test more than once. In particular, if one parameter yields a pseudoprime using Congruence 1, then the above family of parameters also yields the pseudoprime using Congruence 1. It appears difficult to prove similar results for the other congruences. This at least gives a partial explanation for why Congruence 1 is the worst in practice. It is useful to keep this in mind as we numerically compare these congruences in the next section.

3.5 Numerical Results

For ordinary Lucas sequences the effectiveness of a probable prime test depends on which congruence is used, and how the parameters P, Q, and D are chosen. An experimentally effective way used by Baillie and Wagstaff [13] is to choose D from a sequence such as $\{5, 9, 13, 17, \ldots\}$ or $\{5, -7, 9, -11, 13, \ldots\}$ such that $(D|n) = -1$, then pick an appropriate value of P and let $Q = (P^2 - D)/4$. Note that D must be congruent to 0 or 1 (mod 4), usually $D \equiv 1 \ (mod\ 4)$. One benefit of using Lehmer sequences is that we can easily provide similar methods which choose the parameter $D \equiv 2$ or $3 \ (mod\ 4)$ as well.

The following tables give the number of pseudoprimes exhibited by each congruence for certain methods. The methods are described below:

METHOD A (1 mod 4) – Let D be the first element in the sequence 5, 9, 13, 17, 21, ..., such that $(D|n)$ has the desired value. Using the same sequence, let R be the next value such that $(R|n)$ has the desired value. We will either start by checking R beginning with $R = D + 4$ or $R = D + 8$. Note $Q = (R - D)/4$.

METHOD B (2 mod 4) – Use the sequence 2, 6, 10, 14, 18, ...

METHOD C (3 mod 4) – Use the sequence 3, 7, 11, 15, 19, ...

METHOD D (4 mod 4) – Use the sequence 4, 8, 12, 16, 20, ...

When using any of these methods, if a Jacobi symbol ever is evaluated to be zero, then we have a divisor of n and we immediately stop the tests and return that n is composite.

In all the following tables: M = Method, C = Congruence, and we designate whether we have $R \geq D+4$ or $R \geq D+8$. In addition, we explore the various choices for $(D|n)$ and $(R|n)$. All tables give the number of pseudoprimes up to $x = 10^k$, that is, the number of composite integers which satisfy the congruence for given method.

These tables have anomalies that leave unanswered questions, but we can make some general observations about the effectiveness of each method. Specifically, it is interesting to observe the differences that occur between $R \geq D+4$ and $R \geq D+8$, along with the effect of changing the values of $(D|n)$ and $(R|n)$. Note that the table on the right has been tabulated further than the one on the left.

Table 3.5.1: The number of pseudoprimes up to $x = 10^k$ for the four methods and four congruences of this chapter with $(D|n) = (R|n) = -1$.

M	C	10^3	10^4	10^5	10^6	10^7
A	1	2	13	56	174	530
	2	0	4	16	34	87
	3	0	2	12	30	89
	4	0	2	9	20	55
B	1	3	15	52	164	546
	2	1	2	6	25	78
	3	1	2	7	34	88
	4	1	3	5	19	58
C	1	1	12	45	153	504
	2	0	4	11	38	87
	3	0	4	15	50	104
	4	0	2	7	28	65
D	1	2	16	60	177	568
	2	0	3	8	22	73
	3	1	3	11	29	71
	4	0	2	8	21	61

(a) $R \geq D+4$

M	C	10^3	10^4	10^5	10^6	10^7	10^8
A	1	3	12	54	174	524	1452
	2	0	0	2	7	13	24
	3	0	0	1	4	12	22
	4	0	2	3	6	12	21
B	1	1	14	47	168	539	1486
	2	0	0	1	2	20	67
	3	3	4	9	15	45	108
	4	0	0	2	4	20	66
C	1	0	8	36	140	499	1359
	2	0	1	2	3	10	33
	3	0	0	1	3	12	33
	4	0	0	2	4	11	33
D	1	3	16	59	191	562	1559
	2	0	1	3	9	21	49
	3	2	3	6	10	22	49
	4	0	1	5	10	22	51

(b) $R \geq D+8$

Except for Congruence 1, Table 3.5.1(b) has far fewer pseudoprimes. Since $D = R-4Q$, by forcing $R \geq D+8$ we are eliminated the case when $Q = \pm 1$. As Baillie and Wagstaff [13] noticed for Lucas pseudoprimes, the cases $Q = \pm 1$ tend to give more pseudoprimes. Secondly, note that Congruences 2, 3, and 4 are drastically better than Congruence 1, and recall that Theorem 3.2.4 concerned Congruence 1. This is a fundamental difficulty in the theory of probable primality testing. It is often easier to prove theorems about weaker tests, while the numerical calculations show drastically better results than those which are proven.

Now we will create similar tables, but with $(D|n) = -1$ and $(R|n) = +1$.

Table 3.5.2: The number of pseudoprimes up to $x = 10^k$ for the four methods and four congruences of this chapter with $(D|n) = -1$ and $(R|n) = +1$.

M	C	10^3	10^4	10^5	10^6	10^7
A	1	3	15	71	228	693
	2	3	12	52	168	502
	3	3	7	39	124	373
	4	3	10	46	164	485
B	1	4	18	59	201	611
	2	3	12	40	122	483
	3	3	7	24	84	282
	4	3	7	26	96	326
C	1	1	12	42	185	569
	2	0	5	25	100	313
	3	0	5	20	75	232
	4	0	6	27	98	299
D	1	6	28	94	282	829
	2	4	20	84	260	740
	3	4	17	70	190	512
	4	4	19	81	248	714

(a) $R \geq D+4$

M	C	10^3	10^4	10^5	10^6	10^7	10^8
A	1	3	19	63	208	644	1840
	2	0	0	0	1	1	1
	3	0	0	0	1	3	3
	4	0	0	0	2	6	29
B	1	2	12	62	216	618	1688
	2	0	0	0	0	0	1
	3	3	7	18	44	93	215
	4	0	1	2	4	6	21
C	1	2	15	64	205	625	1666
	2	0	0	0	1	1	3
	3	0	0	0	0	0	0
	4	0	1	2	5	5	19
D	1	6	25	72	233	726	2001
	2	1	1	1	3	3	4
	3	1	1	2	4	7	18
	4	0	1	2	3	9	21

(b) $R \geq D+8$

As the rest of the data will confirm, the cases when $(RD|n) = -1$ are much better in practice. To illustrate this idea, look at the numbers of pseudoprimes for Congruences 2, 3, and 4 in Table 3.5.1(b) and compare these results to Congruences 2, 3, and 4 in Table 3.5.2(b). It is one of many anomalies that Table 3.5.2(a) is actually worse than Table 3.5.1(a). However, after reviewing all the tables it should be noted that $(RD|n) = -1$ seems to consistently be the best choice, especially when $R \geq D + 8$.

Now we will create the tables with $(D|n) = +1$ and $(R|n) = \pm 1$. As we have seen above the case when $R \geq D + 8$ tends to be better. For this reason the following tables only consider this case.

Table 3.5.3: The number of pseudoprimes up to $x = 10^k$ for the four methods and four congruences of this chapter with $(D|n) = +1$, $(R|n) = -1$, and $R \geq D + 8$.

M	C	10^3	10^4	10^5	10^6	10^7
	1	2	13	51	159	521
A	2	0	0	0	1	2
	3	0	0	0	3	12
	4	0	1	1	2	3
	1	4	13	59	206	575
B	2	0	1	3	3	3
	3	0	2	4	7	14
	4	0	0	0	3	3
	1	2	12	65	208	622
C	2	0	0	0	1	2
	3	0	0	4	5	11
	4	0	0	0	1	1
	1	3	17	70	207	576
D	2	1	1	1	1	2
	3	0	0	1	3	9
	4	0	0	1	2	4

Table 3.5.4: The number of pseudoprimes up to $x = 10^k$ for the four methods and four congruences of this chapter with $(D|n) = (R|n) = +1$, and $R \geq D + 8$.

M	C	10^3	10^4	10^5	10^6	10^7
A	1	1	11	44	156	531
	2	1	4	11	35	91
	3	1	4	11	36	96
	4	1	4	10	36	98
B	1	0	3	37	134	477
	2	0	1	4	13	51
	3	0	2	5	17	62
	4	0	1	5	17	58
C	1	0	14	55	163	493
	2	0	0	3	14	39
	3	1	1	4	14	38
	4	0	1	4	14	40
D	1	3	15	65	214	652
	2	2	15	48	136	384
	3	2	12	42	125	340
	4	2	13	43	127	346

For Congruence 2, we will look at the overlap in pseudoprimes for the various methods. Since there are so few pseudoprimes when $(RD|n) = -1$, looking for overlap is not practical. Hence, we purposely consider the less effective case $(D|n) = (R|n) = -1$, $R \geq D + 8$ in Table 3.5.1(b). We look at the number of pseudoprimes that remain when the test is run on n using two different methods.

Table 3.5.5: The number of pseudoprimes up to $x = 10^k$ that simultaneously pass two different methods of this chapter with $(D|n) = (R|n) = -1$, and $R \geq D + 8$.

Methods	10^3	10^4	10^5	10^6	10^7	10^8
A and B	0	0	0	0	1	4
A and C	0	0	0	0	0	0
A and D	0	0	0	0	0	0
B and C	0	0	0	0	1	1
B and D	0	0	0	0	0	4
C and D	0	0	0	0	0	2

The pseudoprimes for A and B are 9863461, 21306157, 51283501, and 56479897.

The pseudoprime for B and C is 3116107. The pseudoprimes for B and D are 42702661, 58980637, 79398901, and 94502701. The pseudoprimes for C and D are 20234341 and 61754941. It should be noted that none of these numbers appears twice, so that any combinations of three methods will eliminate all pseudoprimes up to 10^8.

The number of pseudoprimes that are exhibited by a given test is often highly dependent on the method for choosing parameters. We have only considered four simplistic methods, but they all have been successful as our tables illustrate and they seem to be somewhat independent. Specifically, they seem to be successful if we avoid the possibility of $Q = \pm 1$. In the following tables we experiment with other methods which avoid the cases $Q = \pm 1$. From these tables, it becomes more apparent that most methods which choose parameters at 'random' with $(RD|n) = -1$ and $Q \neq \pm 1$ will lead to few pseudoprimes.

In the following tables we use only Congruence 2 for comparison. These numbers should be compared to Tables 3.5.1b, 3.5.2b, 3.5.3, and 3.5.4 on the rows concerning Method C Congruence 2.

METHOD C': Choose D out of the sequence 3, 7, 11, 15, ... Then choose R out of the sequence $D^2 + 6, D^2 + 10, D^2 + 14, D^2 + 18$,....

Table 3.5.6: The number of pseudoprimes up to $x = 10^k$ for method C' and Congruence 2 with with designated Jacobi symbol values.

$(D\|n)$	$(R\|n)$	10^3	10^4	10^5	10^6	10^7	10^8
+1	+1	0	2	4	15	51	
+1	-1	0	0	0	1	1	1
-1	+1	0	0	0	0	0	1
-1	-1	0	0	4	8	18	

METHOD C*: Choose D out of the sequence 3, 7, 11, 15, ... Then choose R out of the sequence $D^3 + 4, D^3 + 8, D^3 + 12, D^3 + 16$,....

Table 3.5.7: The number of pseudoprimes up to $x = 10^k$ for method C* and Congruence 2 with with designated Jacobi symbol values.

$(D\|n)$	$(R\|n)$	10^3	10^4	10^5	10^6	10^7	10^8
+1	+1	0	0	2	8	20	
+1	-1	0	0	0	0	0	4
-1	+1	0	1	1	1	1	1
-1	-1	1	1	4	8	13	

These numbers are very similar to previous values when considering Method C and Congruence 2. This data suggests that Congruence 2 with Method C is indeed a good test. From our data as a whole, it seems that Congruence 2 is the least sensitive to change in methods as long as we ensure that $(RD|n) = -1$ and $Q \neq \pm 1$. With these stipulations, the evidence indicates that we have a very good probable primality test.

3.6 Conclusions

Congruence relations involving Lehmer sequences lead to effective probabilistic primality tests. We have illustrated this fact through theoretical and numerical results.

In the previous section we describe some methods for choosing parameters which we believe to be most effective.

The connections between the various tests described in Theorems 3.4.1 through 3.4.3 give some reasons for why one congruence may work better than another. These theorems were much easier to prove in the setting of Lehmer sequences due to the special form of the characteristic roots.

Chapter 4

Strong Lehmer Tests

The ideas of Euler and Strong testing have been used to provide more effective Fermat based and Lucas based tests. The Lehmer tests described in Chapter 3 are approachable by the same techniques. Here we investigate the standard techniques for strengthening primality tests and we give a generalized approach to these strengthening methods.

In addition, we produce methods that are strengthened versions of Congruence 2 of Chapter 3. Although such techniques are not difficult, we are not aware of any exposition of this topic in the current literature. The end of the chapter provides some numerical evidence concerning the effectiveness of such tests.

4.1 Introduction

Since n is odd, $n \pm 1$ is divisible by 2. This simple fact governs the improvements we are about to develop. Lehmer numbers satisfy useful identities at even values. This theorem is fundamental to what follows.

Theorem 4.1.1. *If k is a positive integer, then $U_{2k} = U_k V_k$.*

Proof. Apply Theorem 1.5.2, with $j = k$. □

If n is an odd prime, then we already know $U_{n-(RD|n)} \equiv 0$ $(mod\ n)$. Since there are no zero divisors modulo a prime n, the identity immediately gives $U_{\frac{n-(RD|n)}{2}} \equiv 0$ $(mod\ n)$ or $V_{\frac{n-(RD|n)}{2}} \equiv 0$ $(mod\ n)$. If either of these congruences is satisfied, then the original congruence is satisfied. Thus, testing each of these does indeed give a stronger criterion for primality. We clarify which of the two congruence must be zero below according to the Jacobi value $(RQ|n)$.

Theorem 4.1.2. *Euler Lehmer Criterion.*

If n is a prime and $(2DRQ, n) = 1$, then

$$U_{\frac{n-(RD|n)}{2}} \equiv 0\ (mod\ n)\ \textit{if}\ (RQ|n) = +1\ \textit{and}$$

$$V_{\frac{n-(RD|n)}{2}} \equiv 0\ (mod\ n)\ \textit{if}\ (RQ|n) = -1.$$

Proof. We show that $V_{\frac{n-(RD|n)}{2}} \equiv 0$ $(mod\ n)$ if and only if $(RQ|n) = -1$. Since $U_{\frac{n-(RD|n)}{2}} V_{\frac{n-(RD|n)}{2}} = U_{n-(RD|n)} \equiv 0$ $(mod\ n)$, this will prove the theorem. For a positive integer k, we have the double argument identity $V_k^2 = V_{2k} + 2Q^k$. Letting $k = \frac{n-(RD|n)}{2}$ and using Congruence 2 of Chapter 3, we have $V_{\frac{n-(RD|n)}{2}} \equiv 0$ $(mod\ n)$ if and only if $2(R|n)Q^{\frac{1-(RD|n)}{2}} + 2Q^{\frac{n-(RD|n)}{2}} \equiv 0$ $(mod\ n)$.

If $(RD|n) = +1$, then $2(R|n) + 2Q^{\frac{n-1}{2}} \equiv 2[(R|n) + (Q|n)] \equiv 0$ $(mod\ n)$ if and only if $(R|n) = -(Q|n)$. If $(RD|n) = -1$, then $2(R|n)Q + 2Q^{\frac{n+1}{2}} \equiv 2Q[(R|n) + (Q|n)] \equiv$

$0\ (mod\ n)$ if and only if $(R|n) = -(Q|n)$. In either case, $(RQ|n) = -1$. □

If $2|\frac{n-(RD|n)}{2}$, then we can use the identity $U_{2k} = U_kV_k$ to extend this congruence even further. Continuing in this way we can develop the Strong Lehmer Test based on the following criterion.

Theorem 4.1.3. *Strong Lehmer Criterion.*

If n is a prime, $(2RQD, n) = 1$, and $n - (RD|n) = 2^sd$ with d odd, then

$$U_d \equiv 0\ (mod\ n)\ \textit{or}$$

$$V_{2^rd} \equiv 0\ (mod\ n)\ \textit{for some}\ i, 0 \leq i < s.$$

Using the Strong Lehmer Criterion does in fact lead to a marked improvement in the reliability of the test without any significant increase in computation time. We illustrate this fact in Table 4.1.1. Here we fix the values of $R = 5$,$Q = 2$, and $D = -3$. In Chapter 3, we experimented with various methods of choosing R and D. We fix the parameters here simply to give a quick comparison between Congruence 1, the Euler Criterion, and the Strong Criterion.

Table 4.1.1: The number of pseudoprimes up to $x = 10^k$ with $R = 5$, $Q = 2$ and $D = -3$.

Test	10^3	10^4	10^5	10^6	10^7
$U_{n-(RD\|n)} \equiv 0\ (mod\ n)$	2	7	41	191	601
Euler Lehmer Criterion	0	4	18	101	306
Strong Lehmer Criterion	0	2	11	67	184

These strong tests exploit the fact that $n - (RD|n)$ is divisible by some power of two. If $n - (RD|n)$ is divisible by some other prime p, then we can exploit this prime as well. We develop these ideas in the next section.

4.2 Generalized Strong Lehmer Testing

The workhorse of Strong Lehmer Testing is the identity $U_{2k} = U_k V_k$ as we have illustrated. Similar, but more complicated, identities hold for U_{mk} and V_{mk} for any positive integer m. These identities are well-known.

Theorem 4.2.1. *If $\widetilde{U}_m = U_{mk}$ and $\widetilde{V}_m = V_{mk}$, then*

$$\widetilde{U}_m = V_k \widetilde{U}_{m-1} - Q^k \widetilde{U}_{m-2} \text{ with } \widetilde{U}_0 = 0, \widetilde{U}_1 = U_k \text{ and}$$

$$\widetilde{V}_m = V_k \widetilde{V}_{m-1} - Q^k \widetilde{V}_{m-2} \text{ with } \widetilde{V}_0 = 2, \widetilde{V}_1 = V_k.$$

Using this theorem, we compute the following identities.

Corollary 4.2.2. *For any positive integer k, we have*

m	U_{mk}	V_{mk}
2	$U_k V_k$	$V_k^2 - 2Q^k$
3	$U_k[V_k^2 - Q^k]$	$V_k[V_k^2 - 3Q^k]$
5	$U_k[V_k^4 - 3Q^k V_k^2 + Q^{2k}]$	$V_k[V_k^4 - 5Q^k V_k^2 + 5Q^{2k}]$
7	$U_k[V_k^6 - 5Q^k V_k^4 + 6Q^{2k} V_k^2 - Q^{3k}]$	$V_k[V_k^6 - 7Q^k V_k^4 + 14Q^{2k} V_k^2 - 7Q^{3k}]$
n	$U_k F(n,k)$	$V_k G(n,k)$

where n is an odd integer and $F(n,k)$ and $G(n,k)$ are $n-1$ degree polynomials in V_k and Q^k. We also define $F(2,k) = V_k$.

Let $n - (RD|n) = 2^{a_1} 3^{a_2} 5^{a_3} \dots p_k^{a_k} d$, where p_k is the k^{th} prime with $(p_k!, d) = 1$ and $a_i \geq 0$ for $i = 1, 2, 3, \dots, k$. If n is a prime, then $U_{n-(RD|n)} \equiv 0 \ (mod\ n)$. The standard Strong Lehmer Criterion says either:

$$(1) U_{3^{a_2}5^{a_3}\ldots p_k^{a_k}d} \equiv 0 \ (mod\ n) \text{ or}$$

$$(2) F(2, 2^{c_1}3^{a_2}5^{a_3}\ldots p_k^{a_k}d) = V_{2^{c_1}3^{a_2}5^{a_3}\ldots p_k^{a_k}d} \equiv 0 \ (mod\ n) \text{ for some } 0 \leq c_1 < a_1.$$

Note that the congruences are stated in terms of the notation of Corollary 4.2.2. We can break up congruence (1) even further by looking at the factor 3^{a_1} to get:

$$(1') U_{5^{a_3}\ldots p_k^{a_k}d} \equiv 0 \ (mod\ n) \text{ or}$$

$$(3) F(3, 3^{c_2}5^{a_3}\ldots p_k^{a_k}d) \equiv 0 \ (mod\ n) \text{ for some } 0 \leq c_2 < a_2.$$

The same idea will work for the primes $5, 7, \ldots, p_k$. Thus, we have the following criterion.

Theorem 4.2.3. *M-Strong Lehmer Criterion.*

If n is prime, $M \geq 2$, $(2RQD, n) = 1$, $n - (RD|n) = 2^{a_1}3^{a_2}5^{a_3}\ldots p_k^{a_k}d$, where p_k is the largest prime less than or equal to M, and $a_i \geq 0$ for $i = 1, 2, 3, \ldots, k$ with $(p_k!, d) = 1$, then

$U_d \equiv 0 \ (mod\ n)$ *or*

$F(2, 2^{c_1}3^{a_2}5^{a_3}\ldots p_k^{a_k}d) \equiv 0 \ (mod\ n)$ *for some* $0 \leq c_1 < a_1$ *or*

$F(3, 3^{c_2}5^{a_3}\ldots p_k^{a_k}d) \equiv 0 \ (mod\ n)$ *for some* $0 \leq c_2 < a_2$ *or*

$\vdots \qquad\qquad \vdots$

$F(p_k, p_k^{c_k}d) \equiv 0 \ (mod\ n)$ *for some* $0 \leq c_k < a_k$.

By the construction of these strong tests, it is immediately apparent that if n is a pseudoprime for the M-Strong Criterion with a given set of parameters R and Q, then it is also a pseudoprime for the M_0-Strong Lehmer Criterion for any $\mathrm{M}_0 < \mathrm{M}$ with the same set of parameters. We summarize this result below:

Theorem 4.2.4. *If R and Q are fixed parameters and $M_0 \leq M_1$, then the number of pseudoprimes up to x for the M_1-Strong Lehmer Criterion is less than or equal to the number of pseudoprimes up to x for the M_0-Strong Lehmer Criterion with respect to the parameters R and Q.*

One disadvantage of the M-Strong Criterion is that we are not guaranteed that $n - (RD|n)$ has a small prime factor other than 2. Yet we do know that if $3 \nmid n$, then either $n + 1$ or $n - 1$ has a factor of 3 depending on whether n is congruent to ± 1 modulo 6. At any rate, we can force $n - (RD|n)$ to be divisible by 3 if we choose $(RD|n) = \pm 1$ appropriately. In such an instance, we are guaranteed that $n - (RD|n) = 2^{a_1} 3^{a_2} d$ and $a_i \geq 1$ for $i = 1, 2$ with $(6, d) = 1$. Thus, we suggest the following 3-Strong Lehmer Algorithm:

Definition 4.2.1. 3-Strong Lehmer Algorithm.

Let n be an odd integer with $n \equiv \epsilon \ (mod\ 6)$ where $\epsilon = \pm 1$. The 3-Strong Lehmer Algorithm proceeds as follows:

1. Choose R and D such that $(RD|n) = \epsilon$ and $(RDQ, n) = 1$. Note $Q \equiv (R - D)/4 \ (mod\ n)$. If (RDQ, n) ever is greater than 1, then return n is composite.

2. Write $n - (RD|n) = 2^{a_1}3^{a_2}d$ with $(6, d) = 1$.

3. If $U_d \equiv 0 \ (mod\ n)$, then return that n is a probable prime.

4. If $V_{3^{c_2}d} \equiv Q^{3^{c_2}d} \ (mod\ n)$ for any value of c_2 with $0 \leq c_2 < a_2$, then return that n is a probable prime. Note that this is precisely the condition $F(3, 3^{c_2}d) \equiv 0 \ (mod\ n)$ from the M-Strong Lehmer Criterion, since $F(3, 3^{c_2}d) = V_{3^{c_2}d} - Q^{3^{c_2}d}$ by Corollary 4.2.2.

5. If $V_{2^{c_1}3^{a_2}d} \equiv 0 \ (mod\ n)$ for any value of c_1 with $0 \leq c_1 < a_1$, then return that n is a probable prime. Here we have the condition $F(2, 2^{c_1}3^{a_2}d) \equiv 0 \ (mod\ n)$ from the M-Strong Lehmer Criterion, since $F(2, 2^{c_1}3^{a_2}d) = V_{2^{c_1}3^{a_2}d}$ by Corollary 4.2.2.

6. If none of these congruences are satisfied, then return n is a composite.

In the following table we illustrate the improvement achieved by using this algorithm. For a given n with $3 \nmid n$, we set $D = 5$ and we choose R to be the smallest integer in the set $\{13, 17, 21, \dots\}$ such that $n - (RD|n)$ is divisible by 6. This is one possible realization of step one of the algorithm above. Since Q is determined by R and D, we use these three parameters in the following tests and we compare the number of pseudoprimes that each test allows.

Table 4.2.1: The number of pseudoprimes up to $x = 10^k$ for the 3-Strong Lehmer Algorithm as compared with the Euler and Strong Lehmer Criterion using the parameter choosing method in the last paragraph.

Test	10^3	10^4	10^5	10^6	10^7
Euler Lehmer Criterion	2	9	31	101	343
Strong Lehmer Criterion	2	6	24	73	232
3-Strong Lehmer Criterion	2	6	23	43	106

From Corollary 4.2.2, if m is an odd prime, then a factor of V_k can be taken out in much the same way as with the M-Strong Criterion above. We explore this situation now. Consider $n - (RD|n) = 2^{a_1}3^{a_2}5^{a_3} \dots p_k^{a_k} d$ and assume $(RQ|n) = -1$, so that the Euler Lehmer Criterion gives

$$V_{2^{a_1-1}3^{a_2}5^{a_3} \dots p_k^{a_k} d} \equiv 0 \ (mod\ n).$$

A factor of V_k can be taken out of V_{mk} of Corollary 4.2.2 if and only if m is odd. So we group 2^{a_1-1} and d together and remove factors of V_k. The congruence

$$V_{3^{a_2}5^{a_3} \dots p_k^{a_k} 2^{a_1-1} d} \equiv 0 \ (mod\ n)$$

implies the following

$$V_{5^{a_3} \dots p_k^{a_k} 2^{a_1-1} d} \equiv 0 \ (mod\ n) \text{ or}$$

$$G(3, 3^{c_2}5^{a_3} \dots p_k^{a_k} 2^{a_1-1} d) \equiv 0 \ (mod\ n) \text{ for some } 0 \leq c_2 < a_2.$$

Continuing in this manner, we arrive at the following.

Theorem 4.2.5. *M-V-Strong Lehmer Criterion.*

If n is prime, $M \geq 2$, $(2RQD, n) = 1$, $n - (RD|n) = 2^{a_1}3^{a_2}5^{a_3} \dots p_k^{a_k} d$, where p_k is *the largest prime less than* M*,* $a_i \geq 0$ *for* $i = 1, 2, 3, \dots k$ *with* $(p_k!, d) = 1$*, and, in addition,* $(RQ|n) = -1$*, then*

$V_{2^{a_1-1}d} \equiv 0$ *(mod n) or*

$G(3, 3^{c_2}5^{a_3} \dots p_k^{a_k}2^{a_1-1}d) \equiv 0$ *(mod n) for some* $0 \leq c_2 < a_2$ *or*

$G(5, 5^{c_3} \dots p_k^{a_k}2^{a_1-1}d) \equiv 0$ *(mod n) for some* $0 \leq c_3 < a_3$ *or*

$\vdots \qquad\qquad \vdots$

$G(p_k, p_k^{c_k}2^{a_1-1}d) \equiv 0$ *(mod n) for some* $0 \leq c_k < a_k$*.*

Note that the same idea could be used for any of the values of c_1 in $F(2, 2^{c_1}3^{a_2}5^{a_3} \dots p_k^{a_k}d) = V_{2^{c_1}3^{a_2}5^{a_3} \dots p_k^{a_k}d}$ from the M-Strong Criterion.

The case with only the prime 2 is the Euler Lehmer Criterion. Thus, let us consider the situation when $n - (RD|n) = 2^{a_1}3^{a_2}d$. For this case we can note that $F(3, k) = V_k^2 - Q^k$ and $G(3, k) = V_k^2 - 3Q^k$. So Theorems 4.2.3 and 4.2.4 become:

Theorem 4.2.6. *3-Strong Lehmer and 3-V-Strong Lehmer Combined Criterion. If* n *is prime,* $(2RQD, n) = 1$*,* $n - (RD|n) = 2^{a_1}3^{a_2}d$ *and* $a_i \geq 0$ *for* $i = 1, 2$ *with* $(6, d) = 1$*, then*

$U_d \equiv 0$ *(mod n) or*

$V_{2^{c_1}d} \equiv 0$ *(mod n) for some* $0 \leq c_1 < a_1$ *or*

$V_{3^{c_2}d}^2 \equiv Q^{3^{c_2}d}$ *(mod n) for some* $0 \leq c_2 < a_2$ *or*

$V_{3^{c_2}2^{c_1}d}^2 \equiv 3Q^{3^{c_2}2^{c_1}d}$ *(mod n) for some* $0 \leq c_1 < a_1$ *and* $0 \leq c_2 < a_2$*.*

Proof. The 3-Strong Criterion gives:

$$(1) U_d \equiv 0 \ (mod\ n) \text{ or}$$

$$(2)F(2,2^{c_1}3^{a_2}d) = V_{2^{c_1}3^{a_2}d} \equiv 0 \ (mod\ n) \text{ for some } 0 \leq c_1 < a_1 \text{ or}$$

$$(3)F(3,3^{c_2}d) = V^2_{3^{c_2}d} - Q^{3^{c_2}d} \equiv 0 \ (mod\ n) \text{ for some } 0 \leq c_2 < a_2.$$

Now we apply the 3-V-Strong Criterion to (2) and for some $0 \leq c_1 < a_1$ we obtain:

$$(2i)V_{2^{c_1}d} \equiv 0 \ (mod\ n) \text{ or}$$

$$(2ii)G(3,3^{c_2}2^{c_1}d) = V^2_{3^{c_2}2^{c_1}d} - 3Q^{3^{c_2}2^{c_1}d} \equiv 0 \ (mod\ n) \text{ for some } 0 \leq c_2 < a_2.$$

□

This test is a little cumbersome and somewhat more difficult to implement. Still these generalized techniques illustrate a mechanical way to strengthen the standard congruences.

We should note that if $n-1$ or $n+1$ can be completely factored into small primes, then there are relatively efficient methods for deterministically proving that n is or is not a prime. These ideas are not new and are discussed in [49], [59]. Some of these methods involve variations of Fermat's Theorem and others use Lucas sequences, but both make use of the idea of strong testing on all the prime factors of $n-1$ or $n+1$.

For large integers, it is unlikely that $n-1$ or $n+1$ can be completely factored. However, if we can find some small factors, then we can use strong testing and become fairly confident in the primality of n.

The method we used for choosing R and D in Table 4.2.1 was somewhat arbitrary. It would be interesting to investigate the effect of different methods for choosing these parameters. Yet even with this limited data, it is somewhat disconcerting that the 3-Strong Lehmer Tests allows 43 pseudoprimes out to 10^5. For all the work we have put in we would hope to find a test which exhibits many fewer pseudoprimes.

Part of the reason that these tests are somewhat less effective than we would hope is their origins. All of these strong tests stem from the congruence $U_{n-(RD|n)} \equiv 0 \ (mod\ n)$ for a prime n. Recall that this was Congruence 1 of Chapter 3. If we review the tables from that chapter, we see that Congruence 1 was by far the least effective in identifying composites.

Although Congruence 1 is the lease effective, it is also the easiest to generalize. All the generalizations in this section stem from the ability to factor U_{pk} and the fact that there are no zero divisors modulo a prime. In essence, it is much easier to work with terms that are congruent to zero. In the next section, we generalize Congruence 2 of Chapter 3. Although this is a more difficult task, we are rewarded with an extremely effective test.

4.3 Congruence 2 Strong Testing

Recall from Chapter 3, if n is a prime and $(2RQD, n) = 1$, then $V_{n-(RD|n)} \equiv 2(R|n)Q^{(1-(RD|n))/2} \ (mod\ n)$. We referred to this relation as Congruence 2. For a given composite n, little is known about the number of parameters that give n as a pseudoprime. However, the experimental evidence in Chapter 3 suggests that this test is far more effective than Congruence 1. Of the basic four congruences, this congruence is often the most accurate for a given method of choosing the parameters. In this section, we strengthen Congruence 2 and arrive at what we believe to be one of the most effective and efficient known tests.

Hence, our goal is to give congruences such that the set of pseudoprimes for these new congruences is a subset of the pseudoprimes for Congruence 2. The main tool we use is the computation of square roots.

Theorem 4.3.1. *If n is an odd prime and a is a quadratic residue, then $x^2 \equiv a\ (mod\, n)$ has exactly 2 incongruent solutions modulo n and, for $n \equiv 3, 5,$ or $7\ (mod\ 8)$, they are explicitly given by*

$$x \equiv \begin{cases} \pm a^{\frac{n+1}{2}}\ (mod\ n) & , \quad if\, n \equiv 3\ (mod\ 4) \\ \pm a^{\frac{n+3}{8}}\ (mod\ n) & , \quad if\, n \equiv 5\ (mod\ 8). \end{cases}$$

Note that the case when $n \equiv 1\ (mod\ 8)$ has no explicit formula. There are all purpose ways to compute square roots in this case, but they are slightly more cumbersome. As a result, this case will be more difficult to generalize. We will deal with this case last.

As with generalizations of Congruence 1, the main tool in decreasing the subscript of V_m is an identity known as the double argument formula. It was given in Chapter 1, but we repeat it here for convenience.

Theorem 4.3.2. *If k is a positive integer, then $V_k^2 = V_{2k} + 2Q^k$.*

Thus, any congruence relation for V_{2k}, can also generate a congruence relation for V_k^2. In essence, we have the ability to decrease the subscript of V_n by factors of 2. For a given composite integer n and parameters R, Q, and D with $(2RQD, n) = 1$, we write $n - (RD|n) = 2^s d$ where $2 \nmid d$ and we reduce $V_{2^s d}$ by factors of 2. To this end we define the following notation.

Definition 4.3.1. For n a positive integer with $n - (RD|n) = 2^s d$ where $2 \nmid d$, we define $A_i = A_i(R,Q) = V_{2^{s-i}k}(R,Q) + 2Q^{2^{s-i-1}d}$ for $i = 0, 1, \ldots, n-1$.

By Theorem 4.3.2, we see $V_{2^{s-i-1}d}^2 = A_i$. If n is a prime, then Congruence 2 implies

$$A_0 \equiv 2(R|n)Q^{\frac{1-(RD|n)}{2}} + 2Q^{\frac{n-(RD|n)}{2}} \equiv 2Q^{\frac{1-(RD|n)}{2}}[(R|n) + (Q|n)] \ (mod\ n)$$

Thus, if n is a prime, then $A_0 \equiv 0, 4Q^{\frac{1-(RD|n)}{2}}$, or $-4Q^{\frac{1-(RD|n)}{2}}$ $(mod\ n)$ according to the values of $(R|n)$ and $(Q|n)$. We keep the notation as we build up the general case, but in practice we may want to use a method of choosing R and Q that gives particular cases of Jacobi symbol values.

From the definition, if n is a prime, we have $V_{2^{s-1}d}^2 \equiv A_0$ $(mod\ n)$. We could use this congruence for primality testing, but it is equivalent to Congruence 2 because $V_{2^{s-1}d}^2 = A_0$ whether n is a prime or not. To strengthen the test, we use Theorem 4.3.1 to find a square root. Since this theorem is valid only for a prime, this change will increase the accuracy of the criterion.

Theorem 4.3.3. *Strong Lehmer 2 Criterion for* $n \not\equiv 1$ $(mod\ 8)$.

If n *is a prime such that* $n \not\equiv 1$ $(mod\ 8)$, $(2RQD, n) = 1$, *and* $n - (RD|n) = 2^s d$

where $2 \nmid d$*, then*

$$V_{2^s d} \equiv 2(R|n)Q^{\frac{1-(RD|n)}{2}} \ (mod\ n) \ and$$

$$V_{2^{s-i-1}d} \equiv \pm A_i^t \ (mod\ n) \ for\ all\ i, 0 \leq i < s-1 \ and$$

$$V_d \equiv \pm \tfrac{A_{s-1}^t}{R^t}\sqrt{R} \ (mod\ n)$$

where t *is defined by*

$$t = \begin{cases} \frac{n+1}{4} & , \ for\ n \equiv 3\ (mod\ 4) \\ \frac{n+3}{8} & , \ for\ n \equiv 5\ (mod\ 8). \end{cases}$$

Proof. The first congruence is precisely Congruence 2. When k is even, V_k is an integer, so we can apply Theorem 4.3.1 to the cases $V_{2^{s-i-1}d}^2 \equiv A_i \ (mod\ n)$ when $s-i-1>0$. If $s=1$, it should be noted that the middle case does not occur. It remains to discuss the final case.

Since d is odd, we have $V_d = B\sqrt{R}$ for some integer B. By definition $B^2R = V_d^2 \equiv A_{s-1} \ (mod\ n)$. Since $(R,n)=1$, we have $B^2 \equiv \frac{A_{s-1}}{R} \ (mod\ n)$. Now we can apply Theorem 4.3.1, to obtain $\frac{V_d}{\sqrt{R}} = B \equiv \pm\frac{A_{s-1}^t}{R^t} \ (mod\ n)$. Multiplying by $\sqrt{R}$ yields the result. □

Observe that there are fundamental differences between the Strong Lehmer Criterion and Strong Lehmer 2 Criterion. The former only required that one of the congruences was satisfied and the latter requires that all the congruences are satisfied. In addition, the Strong Lehmer Criterion would be implemented by first testing U_d, *i.e.* bottom-up, but the Strong Lehmer 2 Criterion would first test $V_{2^s d}$, *i.e.* top-down.

However, both tests compute the same number of values of the Lehmer sequence. The only added computation time is computation of A_i^t $(mod\ n)$. Compared to the computation of the values of the Lehmer sequence, the additional computation time is negligible. Thus, this criterion is fast in practice.

We will experiment with this test at the end of this chapter, but first we must consider the case when $n \equiv 1$ $(mod\ 8)$. In this case, there is no simple formula for the computation of square root as a power. However, efficient algorithms for calculating square roots are known and could be used here. We do not use these techniques here, but instead we investigate methods that are relatively easy to express in a closed form.

If n is a prime and $n \equiv 1$ $(mod\ 8)$, then we can write $n-1 = 2^a d_1$ and $n+1 = 2d_2$ with $2 \nmid d_1$ and $2 \nmid d_2$ and $a \geq 3$. Since $(RD|n)$ could be +1 or -1, we consider these cases separately.

If $(RD|n) = 1$, then we are in the case $n-1 = 2^a d_1$ with $2 \nmid d_1$ and $a \geq 3$. Thus, Congruence 2 gives $V_{2^a d_1} \equiv 2(R|n)$ $(mod\ n)$. Applying the identity of Theorem 4.3.2, we get

$$V_{2^{a-1}d_1}^2 \equiv 2[(R|n) + (Q|n)]\ (mod\ n).$$

We summarize this case in the following theorem.

Theorem 4.3.4. *Strong Lehmer 2 Criterion for $n \equiv 1$ $(mod\ 8)$ and $(RD|n) = +1$. If n is a prime such that $n \equiv 1$ $(mod\ 8)$, $(2RQD, n) = 1$, $(RD|n) = +1$, and*

$n - 1 = 2^a d$ where $2 \nmid d$ and $a \geq 3$, then

$$V_{2^a d} \equiv 2(R|n) \ (mod \ n) \ and$$

$$V_{2^{a-1}d} \equiv \begin{cases} 0 \ (mod \ n) & , \quad if \ (RQ|n) = -1 \\ \pm 2 \ (mod \ n) & , \quad if \ (R|n) = (Q|n) = +1 \\ \pm 2R^{(n-1)/4} \equiv \pm 2Q^{(n-1)/4} \ (mod \ n) & , \quad if \ (R|n) = (Q|n) = -1. \end{cases}$$

Proof. Since $a \geq 3$, we have $2^{a-1}d$ is even and, therefore, $V_{2^{a-1}d}$ is an integer. The first case is immediate from the congruence preceding the theorem. If $(R|n) = (Q|n) = +1$, then $V^2_{2^{a-1}d} \equiv 4 \ (mod \ n)$. Since n is a prime, there are exactly the two solutions $V_{2^{a-1}d} \equiv \pm 2 \ (mod \ n)$.

If $(R|n) = (Q|n) = -1$, then $V^2_{2^{a-1}d} \equiv -4 \ (mod \ n)$. For any integer with $(b|n) = -1$ and n prime, the Euler-Criteria gives $b^{(n-1)/2} \equiv -1 \ (mod \ n)$. Since $4|(n-1)$, we have $[b^{(n-1)/4}]^2 \equiv -1 \ (mod \ n)$. Again, there are exactly 2 solutions so we deduce $V^2_{2^{a-1}d} \equiv \pm 2b^{(n-1)/4} \ (mod \ n)$. Observe that $(R|n) = (Q|n) = -1$ in this case implies that $b = R$ or $b = Q$ would be obvious choices for b. □

If $(RD|n) = -1$, then we are in the case $n + 1 = 2d_2$. Thus, Congruence 2 gives $V_{2d_2} \equiv 2(R|n)Q \ (mod \ n)$. Applying the same identity as before we get

$$V^2_{d_2} \equiv 2Q[(R|n) + (Q|n)] \ (mod \ n).$$

We summarize this case here.

Theorem 4.3.5. *Strong Lehmer 2 Criterion for $n \equiv 1 \ (mod \ 8)$ and $(RD|n) = -1$. If n is a prime such that $n \equiv 1 \ (mod \ 8)$, $(2RQD, n) = 1$, $(RD|n) = -1$, and*

$n + 1 = 2d$ where $2 \nmid d$, then

$$V_{2d} \equiv 2(R|n)Q \ (mod\ n) \ and$$

$$V_d \equiv \begin{cases} 0 \ (mod\ n) & , \quad if\ (RQ|n) = -1 \\ \pm 2w\sqrt{R} \ (mod\ n) & , \quad if\ (R|n) = (Q|n) = +1 \\ \pm 2R^{(n-1)/4}w\sqrt{R} \equiv \pm 2Q^{(n-1)/4}w\sqrt{R} \ (mod\ n) & , \quad if\ (R|n) = (Q|n) = -1 \end{cases}$$

where $w^2 \equiv \frac{Q}{R}$ $(mod\ n)$.

Proof. Since d is odd, we have $V_d = B\sqrt{R}$ for some integer B. The case $(RQ|n) = -1$ follows from the congruence preceding the theorem. If $(R|n) = (Q|n) = +1$, then $B^2R \equiv 4Q$ $(mod\ n)$. Thus, $B^2 \equiv \frac{4Q}{R}$ $(mod\ n)$ which implies $\frac{V_d}{\sqrt{R}} = B \equiv \pm 2w$ $(mod\ n)$.

In the case $(R|n) = (Q|n) = -1$, $B^2R \equiv -4Q$ $(mod\ n)$. Thus, $B^2 \equiv -\frac{4Q}{R}$ $(mod\ n)$ which implies $\frac{V_d}{\sqrt{R}} = B \equiv \pm 2b^{(n-1)/4}w$ $(mod\ n)$ for any b with $(b|n) = -1$. As before $b = R$ and $b = Q$ are convenient values to choose. □

The condition $w^2 \equiv \frac{Q}{R}$ $(mod\ n)$ seems to require another square root computation. However, we can choose w in pre-computation. For a given R, we randomly choose w and compute $Q \equiv w^2R$ $(mod\ n)$.

Using Theorem 4.5.3, 4.5.4, and 4.5.5 in conjunction, we have an algorithm which we have proved to be stronger than Congruence 2. We summarize the Strong Lehmer 2 Algorithm below:

Definition 4.3.2. Strong Lehmer 2 Algorithm.

Let n be an odd integer and compute $n \equiv \gamma$ $(mod\ 8)$ where $\gamma \in \{1, 3, 5, 7\}$.

1. For $\gamma = 3$ or 7, compute $t = (n+1)/4$ and use Theorem 4.5.3 with any choice of parameters.

2. For $\gamma = 5$, compute $t = (n+3)/8$ and use Theorem 4.5.3 with any choice of parameters.

3. For $\gamma = 1$ and $(RD|n) = +1$, use Theorem 4.5.4 with any choice of parameters under the restraint $(RD|n) = +1$.

4. For $\gamma = 1$ and $(RD|n) = -1$, use Theorem 4.5.5, choose w and compute $Q \equiv w^2 R \ (mod\ n)$ under the restraint $(RD|n) = -1$.

5. If any congruence is not satisfied, then n is composite. Otherwise, we say n is a probable prime with respect to this test.

The remainder of this chapter is devoted to illustrating the effectiveness our algorithm. In addition, we experiment with methods for choosing parameters.

4.4 Numerical Results

Although this algorithm can be quickly implemented in practice, it is slightly more complicated that previous tests. The complication is due to the different cases modulo 8. Since the only major restrictions occur in the case $n \equiv 1 \ (mod\ 8)$, it seems reasonable that any method we suggest will deal with this case differently. Thus, each method we describe will have two parts (i) the case when $n \not\equiv 1 \ (mod\ 8)$ and

(ii) the case when $n \equiv 1$ $(mod\ 8)$. Whenever possible we will illustrate for which congruence classes the tests are most effective.

The following tables give the number of pseudoprimes exhibited by each congruence for certain methods. The methods are described below (These are the same methods from Chapter 3):

METHOD A(i) – Let D be the first element in the sequence 5, 9, 13, 17, 21, ..., to satisfy the desired Jacobi value, $(D|n)$. Using the same sequence, let R be the next value to satisfy the desired Jacobi value, $(R|n)$. Then $Q = (R - D)/4$.

METHOD A(ii)– Let R be the first element in the sequence 5, 9, 13, ..., to satisfy the desired Jacobi value, $(R|n)$. Using the same sequence, let w be the next value to satisfy the desired Jacobi value, $(R(1-4w^2)|n)$. Then let $D \equiv R(1-4w^2) \equiv R - 4Q$ where $Q \equiv Rw^2$. Using this method, we are allowed to choose $(R|n)$ and $(D|n)$ as in the other case.

METHOD B(i)(ii) – Use the sequence 2, 6, 10, 14, 18, ...

METHOD C(i)(ii) – Use the sequence 3, 7, 11, 15, 19, ...

METHOD D(i)(ii) – Use the sequence 4, 8, 12, 16, 20, ...

In all the following tables: M = Method, and we designate whether we have $R \geq D + 4$ or $R \geq D + 8$. In addition, we explore the various choices for $(D|n)$ and $(R|n)$ as before. All tables give the number of pseudoprimes up to $x = 10^k$, that is, the number of composite integers which satisfy the test for given method. Since the pseudoprimes for this test are a subset of the pseudoprimes for Congruence 2, it should be noted that the number of pseudoprimes in each column must be smaller than those of the corresponding entries in the tables for Congruence 2 in Chapter 3.

Since $R = D+4$ gives $Q = 1$, we noted in Chapter 3 that the condition $R \geq D+8$ tends to give better results. As a result, we have decided to tabulated part (b) further out to 10^7 instead of 10^6.

Table 4.4.1: The number of pseudoprimes up to $x = 10^k$ as separated by congruence class modulo 8 of the Strong Lehmer 2 Algorithm using the four methods of this section with $(D|n) = (R|n) = -1$.

M	*mod* 8	10^3	10^4	10^5	10^6
	3 or 7	0	3	11	20
A	5	0	0	0	0
	1	0	0	0	0
	3 or 7	1	1	3	9
B	5	0	1	2	8
	1	0	0	0	0
	3 or 7	0	1	4	18
C	5	0	1	2	5
	1	0	0	0	0
	3 or 7	0	2	5	14
D	5	0	1	2	5
	1	0	0	0	0

(a) $R \geq D+4$

M	*mod* 8	10^3	10^4	10^5	10^6	10^7
	3 or 7	0	0	0	3	6
A	5	0	0	0	0	0
	1	0	0	0	0	1
	3 or 7	0	0	0	0	8
B	5	0	0	1	2	4
	1	0	0	0	0	0
	3 or 7	0	0	1	2	7
C	5	0	0	0	0	0
	1	0	0	0	0	0
	3 or 7	0	0	0	1	2
D	5	0	1	2	5	0
	1	0	0	0	1	1

(b) $R \geq D+8$

The data in this first table illustrates the improvements attained by using the Strong Lehmer 2 Testing. For instance, using Congruence 2 with Method A and $R \geq D+4$, we get 34 pseudoprimes up to 10^6 as stated in Table 3.5.1. Here we have 20 pseudoprimes up to 10^6. Similar improvements can be seen by comparing the other columns against Table 3.5.1. Although these are not major improvements, it is a check on our work that these new tests are stronger versions of Congruence 2.

Notice that Table 4.4.1(b) has fewer pseudoprimes. This is consistent with the observations made in Chapter 3. Additionally, we see that the case $n \equiv 1$ $(mod\ 8)$ has very few pseudoprimes for any method.

In the following pages, we give all the tables for the various choices in Jacobi symbol. We will see that with appropriate choices in Jacobi symbols theses stronger tests give marked improvement.

Table 4.4.2: The number of pseudoprimes up to $x = 10^k$ as separated by congruence class modulo 8 of the Strong Lehmer 2 Algorithm using the four methods of this section with $(D|n) = -1$ and $(R|n) = +1$.

M	*mod* 8	10^3	10^4	10^5	10^6
A	3 or 7	0	0	0	0
	5	0	0	4	20
	1	0	0	0	0
B	3 or 7	0	0	0	0
	5	1	1	3	9
	1	0	0	0	0
C	3 or 7	0	0	0	0
	5	0	0	1	3
	1	0	0	0	0
D	3 or 7	0	0	0	0
	5	0	0	2	2
	1	0	0	0	0

(a) $R \geq D + 4$

M	*mod* 8	10^3	10^4	10^5	10^6	10^7
A	3 or 7	0	0	0	0	0
	5	0	0	0	0	0
	1	0	0	0	0	0
B	3 or 7	0	0	0	0	0
	5	0	0	0	0	0
	1	0	0	0	0	0
C	3 or 7	0	0	0	0	0
	5	0	0	0	0	0
	1	0	0	0	0	0
D	3 or 7	0	0	0	0	0
	5	0	0	0	0	0
	1	0	0	0	0	0

(b) $R \geq D + 8$

Table 3.5.2 of Chapter 3 also looked at the situation where $(D|n) = -1$ and $(R|n) = +1$. In Table 3.5.2, Congruence 2 was extremely effective in identifying composites. In total, Congruence 2 only allowed 5 pseudoprimes up 10^7 for all methods with $R \geq D + 8$. Here we see that the Strong Lehmer 2 Algorithm eliminates all of these pseudoprimes and identifies all composites up to 10^7.

It also appears that $(D|n) = -1$ and $(R|n) = +1$ is a better choice than $(D|n) = (R|n) = -1$. Looking at the next table we will see that $(D|n) = +1$ and $(R|n) = -1$ is also a good overall choice. Thus, $(RD|n) = -1$ seems like an optimal choice as is consistent with observations in Chapter 3.

Table 4.4.3: The number of pseudoprimes up to $x = 10^k$ as separated by congruence class modulo 8 of the Strong Lehmer 2 Algorithm using the four methods of this section with $(D|n) = +1$ and $(R|n) = -1$.

M	*mod* 8	10^3	10^4	10^5	10^6
A	3 or 7	0	0	1	1
	5	0	0	1	2
	1	0	0	0	0
B	3 or 7	0	2	5	21
	5	0	2	7	12
	1	0	0	0	0
C	3 or 7	0	0	0	2
	5	0	0	2	13
	1	0	0	0	0
D	3 or 7	0	1	6	23
	5	0	1	1	2
	1	0	0	0	0

(a) $R \geq D + 4$

M	*mod* 8	10^3	10^4	10^5	10^6	10^7
A	3 or 7	0	0	0	0	0
	5	0	0	0	1	1
	1	0	0	0	0	0
B	3 or 7	0	0	0	0	0
	5	0	1	3	3	3
	1	0	0	0	0	0
C	3 or 7	0	0	0	0	0
	5	0	0	0	0	0
	1	0	0	0	0	0
D	3 or 7	0	0	0	0	0
	5	1	1	1	1	1
	1	0	0	0	0	0

(b) $R \geq D + 8$

Table 4.4.4: The number of pseudoprimes up to $x = 10^k$ as separated by congruence class modulo 8 of the Strong Lehmer 2 Algorithm using the four methods of this section with $(D|n) = (R|n) = +1$.

M	*mod* 8	10^3	10^4	10^5	10^6
A	3 or 7	0	5	16	46
	5	0	0	0	0
	1	0	0	3	11
B	3 or 7	0	2	6	10
	5	0	0	0	0
	1	0	1	3	8
C	3 or 7	1	1	3	8
	5	0	0	0	0
	1	0	1	6	9
D	3 or 7	1	5	19	52
	5	0	0	1	7
	1	0	0	1	7

(a) $R \geq D + 4$

M	*mod* 8	10^3	10^4	10^5	10^6	10^7
A	3 or 7	1	4	8	18	42
	5	0	0	0	0	1
	1	0	0	3	8	26
B	3 or 7	0	1	1	2	6
	5	0	0	0	0	1
	1	0	0	0	3	11
C	3 or 7	0	0	2	6	8
	5	0	0	0	1	1
	1	0	0	4	7	13
D	3 or 7	2	10	35	93	249
	5	0	0	1	7	7
	1	0	0	3	11	25

(b) $R \geq D + 8$

These tables suggests that the Strong Lehmer 2 Algorithm gives an probable prime test with high confidence, especially when the parameters are chosen such that $(RD|n) = -1$.

Chapter 5

Lehmer Criteria Modulo Prime Powers

In the previous chapters, we explored congruences which hold modulo a prime and give efficient primality tests. These congruences stem from a characterization of primes involving binomial coefficients. If we could test all the binomial coefficients directly, then we would know for certain that an integer is prime. Since this isn't practical, we gave tests which in essence tested sums of binomial coefficients. Thus, a pseudoprime is an integer in which a sum of binomial coefficients, relative to the test being used, satisfies the same conditions as a prime, while the individual coefficients do not satisfy the same conditions as a prime. Making the assumption that this situation occurs in a random manner, then involving more binomial coefficients should give a more reliable test. This assumption is not entirely valid, but it gives heuristic reasons to develop tests which incorporate more binomial coefficients. We accomplish this by looking at tests modulo prime powers.

Once we develop new tests, we combine them with existing ones. These combined versions are numerically shown to be quite good in practice.

5.1 Introduction

All of the primality test congruences in the previous chapters were proved at least in part using congruences of binomial coefficients known to hold modulo a prime. Specifically we used the fact that $\binom{p}{k} \equiv 0 \ (mod\ p)$ for p prime and $0 < k < p$. We will discuss similar properties of binomial coefficients modulo prime powers.

A fundamental result in the study of divisibility of binomial coefficients is Kummer's Theorem.

Theorem 5.1.1. *Kummer's Theorem.*
If n and k are integers and p is a prime, then the largest power of p dividing $\binom{n}{k}$ is given by the number of borrows required when subtracting the base p representations of k from n.

Kummer's Theorem is useful in situations where the binomial coefficient is divisible by a prime power. However, if the binomial coefficient is not congruent to zero, then the question remains for a way to simplify the expression. In [15], Davis and Webb give the following result concerning the simplification of such binomial coefficients.

Theorem 5.1.2. *If $n = a_tp^t + a_{t-1}p^{t-1} + \cdots + a_1p + a_0$ and $k = b_tp^t + b_{t-1}p^{t-1} + \cdots + b_1p + b_0$ are written in the base p and $s < t$, then*

$$\left(\begin{array}{c} n \\ k \end{array}\right) \equiv \left(\begin{array}{c} a_tp^t + a_{t-1}p^{t-1} + \cdots + a_1p^1 + a_0 \\ b_tp^t + b_{t-1}p^{t-1} + \cdots + b_1p^1 + b_0 \end{array}\right) \equiv$$

$$\frac{\left(\begin{array}{c} a_tp^{t-s} + \cdots + a_{t-s} \\ b_tp^{t-s} + \cdots + b_{t-s} \end{array}\right) \cdots \left(\begin{array}{c} a_sp^{t-s} + \cdots + a_0 \\ b_sp^{t-s} + \cdots + b_0 \end{array}\right)}{\left(\begin{array}{c} a_{t-1}p^{t-s-1} + \cdots + a_{t-s+1} \\ b_{t-1}p^{t-s-1} + \cdots + b_{t-s+1} \end{array}\right) \cdots \left(\begin{array}{c} a_{s-1}p^{t-s-1} + \cdots + a_0 \\ b_{s-1}p^{t-s-1} + \cdots + b_0 \end{array}\right)} \ (mod\ p^s).$$

If $m = m_rp^r + m_{r-1}p^{r-1} + \cdots + m_1p + m_0$ and $l = l_rp^r + l_{r-1}p^{r-1} + \cdots + l_1p + l_0$ and $l_r > m_r$, we define

$$\left(\begin{array}{c} m_rp^r + m_{r-1}p^{r-1} + \cdots + m_0 \\ l_rp^r + l_{r-1}p^{r-1} + \cdots + l_0 \end{array}\right) = p \left(\begin{array}{c} m_{r-1}p^{r-1} + \cdots + m_0 \\ l_{r-1}p^{r-1} + \cdots + l_0 \end{array}\right).$$

For help in understanding this theorem, we offer the following example:

$$\begin{aligned} \left(\begin{array}{c} 386 \\ 154 \end{array}\right) &= \left(\begin{array}{c} 3 \cdot 11^2 + 2 \cdot 11 + 1 \\ 11^2 + 3 \cdot 11 \end{array}\right) \equiv \frac{\left(\begin{array}{c} 3 \cdot 11 + 2 \\ 11 + 3 \end{array}\right)\left(\begin{array}{c} 2 \cdot 11 + 1 \\ 3 \cdot 11 \end{array}\right)}{\left(\begin{array}{c} 2 \\ 3 \end{array}\right)} \\ &\equiv \left(\begin{array}{c} 3 \cdot 11 + 2 \\ 11 + 3 \end{array}\right)\left(\begin{array}{c} 1 \\ 0 \end{array}\right) \equiv \left(\begin{array}{c} 35 \\ 14 \end{array}\right) \ (mod\ 11^2). \end{aligned}$$

More importantly, this theorem can be used to simplify general classes of binomial coefficients. In particular, we can prove the following.

Theorem 5.1.3. *If p is a prime and $0 \leq a_0, a_1 < p$, then*

$$\left(\begin{array}{c} p^t \\ k \end{array}\right) \equiv \begin{cases} 0 & (mod\ p^t) \quad , \quad if\ (k,p) = 1 \\ \left(\begin{array}{c} p^{t-1} \\ k/p \end{array}\right) & (mod\ p^t) \quad , \quad if\ (k,p) > 1. \end{cases}$$

Proof. If $(k,p) = 1$, then the number of borrows when subtracting the base p representation of k from p^t is t. Thus, Kummer's Theorem gives the first case. If $(k,p) > 1$, then $k = k_1p^t + k_0p$ for positive integers k_1 and k_0 with $k_0 < p^{t-1}$. Thus, Theorem 5.1.2 gives

$$\left(\begin{array}{c} p^t \\ k \end{array}\right) \equiv \frac{\left(\begin{array}{c} p^{t-1} \\ k_1p^{t-1}+k_0 \end{array}\right)\left(\begin{array}{c} 0 \\ k_0p \end{array}\right)}{\left(\begin{array}{c} 0 \\ k_0 \end{array}\right)} \equiv \left(\begin{array}{c} p^{t-1} \\ k_1p^{t-1}+k_0 \end{array}\right) \equiv \left(\begin{array}{c} p^{t-1} \\ k/p \end{array}\right) \ (mod\ p^t).$$

□

Theorems of a similar nature could be given with $\left(\begin{array}{c} n \\ k \end{array}\right)$ where n is a more general expression in the base p. However, the situation becomes more complicated. We proved the case above for its simplicity and ease of use in the development of Lehmer sequence congruences.

5.2 Lehmer Sequences modulo Prime Powers

Given integers R and Q, let $U_k = U_k(\sqrt{R}, Q)$ and $V_k = V_k(\sqrt{R}, Q)$ as in previous chapters. Using the binomial coefficient theorems from the last section, we create congruences for the Lehmer sequences modulo n^t. Note that any of these congruences also hold for the Lucas sequences if the parameter R is replaced by P^2.

Theorem 5.2.1. *Lehmer n^t Criteria.*

Let n be a given odd integer with parameters satisfying $(2RQD, n) = 1$ and define $\widetilde{U}_k = U_k(\sqrt{R^n}, (R^n - D^n)/4)$ and $\widetilde{V}_k = V_k(\sqrt{R^n}, (R^n - D^n)/4)$. If n is an odd prime and $\epsilon = \pm 1$, then

1. $2Q^{(1+\epsilon)/2}U_{n^t-\epsilon} \equiv \sqrt{R}D^{(n-1)/2}\widetilde{U}_{n^{t-1}} - \epsilon\widetilde{V}_{n^{t-1}}$ *(mod n^t).*

2. $2Q^{(1+\epsilon)/2}V_{n^t-\epsilon 1} \equiv \sqrt{R}\widetilde{V}_{n^{t-1}} - \epsilon D^{(n+1)/2}\widetilde{U}_{n^{t-1}} \ (mod\ n^t)$.

3. $U_{n^t} \equiv D^{(n-1)/2}\widetilde{U}_{n^{t-1}} \ (mod\ n^t)$.

4. $V_{n^t} \equiv \widetilde{V}_{n^{t-1}} \ (mod\ n^t)$.

Proof. We prove Congruences 3 and 4 first. Using the identity of Theorem 1.4.3 and applying the congruences of Theorem 5.1.3, we get

$$\begin{aligned} 2^{n^t-1}U_{n^t} &= \textstyle\sum_{i\ odd} \begin{pmatrix} n^t \\ i \end{pmatrix} R^{(n^t-i)/2}D^{(i-1)/2} \\ &\equiv \textstyle\sum_{j\ odd} \begin{pmatrix} n^t \\ jn \end{pmatrix} R^{(n^t-jn)/2}D^{(jn-1)/2} \\ &\equiv D^{(n-1)/2}\textstyle\sum_{j\ odd} \begin{pmatrix} n^{t-1} \\ j \end{pmatrix} (R^n)^{(n^{t-1}-j)/2}(D^n)^{(j-1)/2} \\ &\equiv D^{(n-1)/2}2^{n^{t-1}-1}\widetilde{U}_n \ (mod\ n^t). \end{aligned}$$

Thus, $2^{n^t-n^{t-1}}U_{n^2} \equiv D^{(n-1)/2}\widetilde{U}_n \ (mod\ n^t)$. Since $\phi(n^t) = n^t - n^{t-1}$ for n prime, by Euler's Theorem, $2^{n^t-n^{t-1}} \equiv 1 \ (mod\ n^t)$.

Congruence 4 is proved in an identical way. For $\epsilon = \pm 1$, by direct substitution into the identities of Corollary 1.5.3 we obtain the first two congruences. □

A disadvantage of using such a criteria in testing for primality is the size of the numbers. Thus, any computation will require much more storage than computations modulo n. It would be interesting to study the general case, but, for the time and computation issues mentioned here, we will focus on the case when $t = 2$. With $t = 2$, we get the following corollary.

Corollary 5.2.2. *Lehmer n^2 Criteria.*

Let n be a given odd integer with parameters satisfying $(2RQD, n) = 1$ and define

$\widetilde{U}_k = U_k(\sqrt{R^n}, (R^n - D^n)/4)$ *and* $\widetilde{V}_k = V_k(\sqrt{R^n}, (R^n - D^n)/4)$. *If* n *is an odd prime and* $\epsilon = \pm 1$, *then*

1. $2Q^{(1+\epsilon)/2}U_{n^2-\epsilon} \equiv \sqrt{R}D^{(n-1)/2}\widetilde{U}_n - \epsilon\widetilde{V}_n$ *(mod* n^2*)*.

2. $2Q^{(1+\epsilon)/2}V_{n^2-\epsilon 1} \equiv \sqrt{R}\widetilde{V}_n - \epsilon D^{(n+1)/2}\widetilde{U}_n$ *(mod* n^2*)*.

3. $U_{n^2} \equiv D^{(n-1)/2}\widetilde{U}_n$ *(mod* n^2*)*.

4. $V_{n^2} \equiv \widetilde{V}_n$ *(mod* n^2*)*.

A composite integer n which satisfies Congruence i in the theorem above is called a Lehmer Squared pseudoprime with respect to the parameters R and Q and Congruence i (or $\mathrm{lehpsp}_i^2(R,Q)$) for $i = 1$, 2, 3, or 4. Notice that this definition is ambiguous in the case of Congruence 1 and 2, since we do not know if $\epsilon = \pm 1$. Our experimental evidence has shown no obvious advantage between the two cases, so we will always take $\epsilon = -1$ as implied by the notation $\mathrm{lehpsp}_i^2(R,Q)$. If we ever intend $\epsilon = +1$ we will make this explicit.

We explore these four congruences in Tables 5.4.1 through 5.4.4 of the numerical results section at the end of this chapter.

5.3 Combining Tests

The standard Lucas sequences and the Lehmer sequences of Chapter 3 give good tests for primality. We will also see that the congruences in the last section are effective, but do not eliminate pseudoprimes. By combining ideas from both of these, we can create a tests which numerical appears to exhibits even fewer pseudoprimes.

By rewriting the Lehmer congruences of Theorem 3.2.1 in terms of n^2, instead of n, we arrive at the following combined congruences. We prove this theorem in terms of the Lehmer sequences first as they are more general than the standard Lucas sequences.

Theorem 5.3.1. *Combined Lehmer n^2 Criteria.*

Using the notation of Theorem 5.2.2. If n is an odd prime with parameters satisfying $(2RQD, n) = 1$, then

1. $4(RD|n)\sqrt{R}Q^{(1+\epsilon)/2}U_{n^2-\epsilon} \equiv RD^{(n-1)/2}(R|n)[\widetilde{U}_n^2+1]-\epsilon(D|n)[\widetilde{V}_n^2+R]$ $(mod\ n^2)$.

2. $4(RD|n)Q^{(1+\epsilon)/2}V_{n^2-\epsilon} \equiv (D|n)[\widetilde{V}_n^2+R]-\epsilon(R|n)D^{(n+1)/2}[\widetilde{U}_n^2+1]$ $(mod\ n^2)$.

3. $2(D|n)U_{n^2} \equiv D^{(n-1)/2}[\widetilde{U}_n^2+1]$ $(mod\ n^2)$.

4. $2(R|n)\sqrt{R}V_{n^2} \equiv \widetilde{V}_n^2+R$ $(mod\ n^2)$.

Proof. We illustrate the techniques by first proving Congruences 3 and 4. From Theorem 3.2.1, we have $\widetilde{U}_n \equiv (D^n|n) \equiv (D|n)$ $(mod\ n)$ and $\widetilde{V}_n \equiv (R^n|n)\sqrt{R^n} \equiv (R|n)\sqrt{R}$ $(mod\ n)$. Note the parameters $R^n \equiv R$ $(mod\ n)$ by Fermat's Little Theorem, so the parameters R and R^n are equivalent for a prime n. We can restate these congruences modulo n^2 by noting $n|(\widetilde{U}_n-(D|n))$ if and only if $n^2|(\widetilde{U}_n^2-2(D|n)\widetilde{U}_n+1)$. Thus, $2(D|n)\widetilde{U}_n \equiv \widetilde{U}_n^2+1$ $(mod\ n^2)$. Similarly, we find $2(R|n)\sqrt{R}\widetilde{V}_n \equiv \widetilde{V}_n^2+$

R $(mod\ n^2)$. Now we take the congruences from Theorem 5.2.2 and replace $\widetilde{U}_n$ and $\widetilde{V}_n$ to get the combined congruences.

Thus, $U_{n^2} \equiv D^{(n-1)/2}\widetilde{U}_n$ $(mod\ n^2)$ and $V_{n^2} \equiv \widetilde{V}_n$ $(mod\ n^2)$ imply

$$2(D|n)U_{n^2} \equiv D^{(n-1)/2} 2(D|n)\widetilde{U}_n \equiv D^{(n-1)/2}[\widetilde{U}_n^2 + 1]\ (mod\ n^2) \quad \text{and}$$

$$2(R|n)\sqrt{R}V_{n^2} \equiv 2(R|n)\sqrt{R}\widetilde{V}_n \equiv \widetilde{V}_n^2 + R\ (mod\ n^2).$$

Replacing the corresponding terms in Congruences 1 and 2 of Theorem 5.2.2 gives the other two combined congruences. □

In the proof, we rewrote the standard Lehmer congruences in terms of n^2. That is, we wrote $n|(\widetilde{U}_n - (D|n))$ if and only if $n^2|(\widetilde{U}_n^2 - 2(D|n)\widetilde{U}_n + 1)$. Thus, testing this second fact alone would not give an improvement in identifying composites. However, using this change allowed for our new approach concerning congruence relations modulo n^2 to be combined with standard criteria.

A composite integer n which satisfies Congruence i in the theorem above is called a Combined Lehmer Squared pseudoprime with respect to the parameters R and Q and Congruence i (or $\text{clehpsp}_i^2(R, Q)$) for $i = 1, 2, 3$, or 4. Notice that we are only looking at 2 congruences here. Numerically, we explore only Congruences 3 and 4, since the first two congruences are somewhat more complicated.

5.4 Numerical Data

In this section we examine the number of Lehmer Squared pseudoprimes and the number of Combined Lehmer Squared pseudoprimes up to $x = 10^k$. For ease in comparison, we use the same methods as used in the previous chapters. For brevity, we restate these methods below.

METHOD A (1 mod 4) – Let D be the first element in the sequence 5, 9, 13, 17, 21, ..., such that $(D|n)$ has the desired value. Using the same sequence, let R be the next value such that $(R|n)$ has the desired value. We will either start by checking beginning with $R = D + 4$ or $R = D + 8$. Note $Q = (R - D)/4$.

METHOD B (2 mod 4) – Use the sequence 2, 6, 10, 14, 18, ...

METHOD C (3 mod 4) – Use the sequence 3, 7, 11, 15, 19, ...

METHOD D (4 mod 4) – Use the sequence 4, 8, 12, 16, 20, ...

Using the same conventions as the previous chapters, if a Jacobi Symbol ever is evaluated to be zero, then we have a divisor of n and we immediately stop the tests and return that n is composite.

In all the following tables: M = Method, C = Congruence and we designate when we have $R \geq D + 4$ or $R \geq D + 8$. All of these tables give the number of pseudoprimes up to $x = 10^k$, that is, the number of composite integers which satisfy the congruence using the given method. Tables 5.4.1 through 5.4.4 are concerning Lehmer Squared pseudoprimes and Tables 5.4.5 through 5.4.8 are concerning Combined Lehmer Squared pseudoprimes.

Table 5.4.1: The lehpsp$_i^2$ up to $x = 10^k$ for $(D|n) = (R|n) = -1$.

M	C	10^3	10^4	10^5	10^6
A	1	0	0	5	10
	2	0	0	5	10
	3	0	0	5	10
	4	0	0	5	10
B	1	0	0	2	10
	2	0	0	2	9
	3	0	1	5	16
	4	1	3	7	16
C	1	0	0	0	5
	2	0	0	0	4
	3	0	0	1	7
	4	1	1	2	10
D	1	0	0	2	9
	2	0	0	3	10
	3	0	0	3	11
	4	0	1	6	15

(a) $R \geq D + 4$

M	C	10^3	10^4	10^5	10^6
A	1	0	0	3	7
	2	0	0	3	8
	3	1	1	4	9
	4	0	0	3	7
B	1	0	0	1	10
	2	0	0	1	11
	3	0	1	4	16
	4	0	1	5	18
C	1	0	1	1	3
	2	0	1	1	4
	3	0	1	3	11
	4	0	2	3	10
D	1	0	0	1	8
	2	0	0	2	9
	3	0	0	2	10
	4	0	1	5	18

(b) $R \geq D + 8$

Notice several distinctions from the tables of previous chapters. First, there is not a major distinction between the cases $R \geq D + 4$ and $R \geq D + 8$. In addition, no one congruence seems significantly better than any of the others. As we look to the next tables, these observations are still true. In addition, we will see that no one table seems better than any of the others.

Table 5.4.2: The lehpsp$_i^2$ up to $x = 10^k$ for $(D|n) = -1$ and $(R|n) = +1$.

M	C	10^3	10^4	10^5	10^6
A	1	0	0	0	4
	2	0	1	1	4
	3	0	1	3	11
	4	0	0	1	7
B	1	0	0	0	2
	2	1	2	2	5
	3	0	0	1	7
	4	0	1	2	7
C	1	0	2	2	4
	2	0	2	2	4
	3	0	2	3	5
	4	0	2	4	9
D	1	0	0	1	5
	2	0	1	2	6
	3	0	2	4	8
	4	1	3	6	16

(a) $R \geq D + 4$

M	C	10^3	10^4	10^5	10^6
A	1	0	0	0	2
	2	1	2	2	4
	3	0	0	0	2
	4	0	1	5	8
B	1	0	1	1	2
	2	0	2	2	3
	3	0	2	2	5
	4	0	2	3	8
C	1	0	0	0	2
	2	0	0	0	3
	3	0	1	2	6
	4	1	1	1	5
D	1	0	2	3	5
	2	1	3	5	7
	3	0	2	4	10
	4	2	5	8	16

(b) $R \geq D + 8$

Table 5.4.3: The lehpsp$_i^2$ up to $x = 10^k$ for $(D|n) = +1$, $(R|n) = -1$, and $R \geq D + 8$.

M	C	10^3	10^4	10^5	10^6
A	1	0	0	1	4
	2	0	2	3	8
	3	0	0	4	12
	4	0	2	4	13
B	1	0	0	0	3
	2	1	1	1	5
	3	0	0	0	4
	4	0	0	3	8
C	1	0	0	2	6
	2	0	1	2	7
	3	0	0	4	10
	4	0	0	3	12
D	1	0	0	0	3
	2	1	1	1	6
	3	0	0	0	3
	4	0	0	2	6

Table 5.4.4: The lehpsp$_i^2$ up to $x = 10^k$ for $(D|n) = +1$, $(R|n) = +1$, and $R \geq D + 8$.

M	C	10^3	10^4	10^5	10^6
	1	0	2	4	10
A	2	0	2	5	13
	3	1	4	8	18
	4	0	2	6	17
	1	0	1	2	9
B	2	0	1	3	12
	3	0	1	5	16
	4	0	1	3	17
	1	0	1	4	11
C	2	0	1	4	12
	3	0	1	3	16
	4	0	2	4	14
	1	0	2	9	22
D	2	0	2	10	23
	3	0	2	11	33
	4	3	12	30	73

These tables are somewhat discouraging. Comparing the Tables 5.4.1 through 5.4.4 with the standard Lehmer pseudoprime tables of Section 3.5 we see very little improvement. It could be that composite integers satisfying these criteria also are likely to satisfy the standard criteria due to some intrinsic nature of the way we devised our tests. However, one would think that some method of looking at binomial coefficients modulo prime powers could be advantageous and perhaps we have not used the correct set of congruences. In any event, we can note that none of these tables contain the astronomical kinds of numbers that appear in several entries of the tables of Chapter 3. All the numbers stay relatively small.

Now we try to salvage the situation somewhat. The following tables refer to

Combined Lehmer Squared pseudoprimes for Congruences 3 and 4. Recall that Congruences 1 and 2 were of somewhat of a complicated nature. Although Congruences 1 and 2 would not have significantly more computation time, we elect to only examine Congruences 3 and 4 for simplicity. Notice that all of the following tables are tabulated out further than the Tables 5.4.1 through 5.4.4.

Table 5.4.5: The clehpsp^2_i up to $x = 10^k$ for $(D|n) = (R|n) = -1$.

M	C	10^3	10^4	10^5	10^6	10^7
A	3	0	0	1	2	8
	4	0	0	0	0	0
B	3	0	0	2	6	13
	4	0	0	0	0	0
C	3	0	0	0	2	7
	4	0	0	0	0	0
D	3	0	0	2	4	10
	4	0	0	0	0	0

(a) $R \geq D + 4$

M	C	10^3	10^4	10^5	10^6	10^7
A	3	0	0	0	2	7
	4	0	0	0	0	0
B	3	0	0	0	3	9
	4	0	0	0	0	0
C	3	0	1	1	3	7
	4	0	0	0	0	0
D	3	0	0	2	4	9
	4	0	0	0	0	0

(b) $R \geq D + 8$

It is quite surprising that Congruence 4 exhibits no pseudoprimes out to 10^7 for any of the methods, while Congruence 3 exhibits several. From this data, we might suspect that Congruence 4 gives a much better test. However, our conjecture would be disproved by the following table.

Table 5.4.6: The clehpsp$_i^2$ up to $x = 10^k$ for $(D|n) = -1$ and $(R|n) = +1$.

M	C	10^3	10^4	10^5	10^6	10^7
A	3	0	0	0	0	0
	4	0	0	0	3	9
B	3	0	0	0	0	0
	4	0	0	1	2	5
C	3	0	0	0	0	0
	4	0	1	1	3	4
D	3	0	1	2	2	2
	4	0	2	5	16	21

(a) $R \geq D + 4$

M	C	10^3	10^4	10^5	10^6	10^7
A	3	0	0	0	0	0
	4	0	0	0	2	4
B	3	0	0	0	0	0
	4	0	0	0	1	2
C	3	0	0	0	0	0
	4	0	1	1	3	4
D	3	0	0	0	0	0
	4	0	0	3	6	17

(b) $R \geq D + 8$

In this instance, we see that Congruence 3 exhibits fewer pseudoprimes than Congruence 4 out to 10^7. We see a slight trend that Method D may be a bad choice, but overall it seems that the method makes little difference. As we look at the next two tables it is interesting to conjecture on the conditions that cause Congruence 3 to be better than Congruence 4 and vice versa.

Table 5.4.7: The clehpsp$_i^2$ up to $x = 10^k$ for $(D|n) = +1$, $(R|n) = -1$, and $R \geq D + 8$.

M	C	10^3	10^4	10^5	10^6	10^7
A	3	0	0	2	5	14
	4	0	0	0	0	0
B	3	0	0	0	2	6
	4	0	0	0	0	0
C	3	0	0	3	4	8
	4	0	0	0	0	0
D	3	0	0	0	2	5
	4	0	0	0	0	0

Comparing Table 5.4.5, 5.4.6, and 5.4.7, one might conjecture that Congruence 4 is better in the situations where $(R|n) = -1$ and Congruence 3 is better in the situations where $(R|n) = +1$ and $(D|n) = -1$. This last table is the case when both Jacobi symbols are $+1$ and it appears to be by far the worst.

Table 5.4.8: The clehpsp$_i^2$ up to $x = 10^k$ for $(D|n) = +1$, $(R|n) = +1$ and $R \geq D + 8$.

M	C	10^3	10^4	10^5	10^6	10^7
A	3	1	2	4	10	22
	4	1	1	6	16	35
B	3	0	1	2	7	23
	4	0	1	3	15	51
C	3	0	0	1	5	21
	4	0	2	4	16	40
D	3	0	4	12	31	88
	4	2	9	25	65	155

From this data, it would seem wise in practice to either use Congruence 3 and the methods of Table 5.4.6 or use Congruence 4 and the methods of Table 5.4.7. In these specific instances our methods have given no pseudoprimes.

All of these tests are somewhat less efficient than the tests of the previous sections. However, these last few tables raise some interesting theoretical questions. Certainly, if we could prove that two congruences cannot be simultaneously satisfied by a composite and are always satisfied for a prime, then we would have a deterministic test for primality. If such a test require only two simultaneous tests using Lehmer sequences, then it would be a major breakthrough. Further research needs to be done in this direction.

The standard technique would be to examine these congruences and the types of parameters that lead to pseudoprimes modulo a composite n when the prime factorization of n is known. These equations are difficult to analyze, but perhaps with the data and conjectures set form here some direction can be found towards a solution. These issues must be studied further.

Chapter 6

Characteristic Root Analysis

In the Chapters 3-5 we investigated several probabilistic primality tests using Lehmer sequences. Since these sequences satisfy the Binet formula, all of the congruences we discussed can be reformulated in terms of the characteristic roots. Here we make this reformulation to allow for comparisons between tests and to give some reasons for the anomalies we have seen in various tables. In [22], various techniques are given which in essence examine characteristic roots directly in a field extension. These techniques are effective, but require computations in a finite field. The tests we have presented have the advantage of staying in the base field for all computations. In this chapter, we examine the characteristic roots to give some information about our integer based tests. These methods are not difficult, yet they are rarely used in the literature. In [8], characteristic roots are partially used to find the number of parameters that give an odd composite integer n as a pseudoprime for a fixed D using the Strong Lucas Criterion. We use the characteristic roots in a different way to help give some heuristic reasons why certain criteria are better than others. The reason this type of argument is not found in the literature perhaps is due to the prevalence of Lucas testing with the parameter P. Expressed in terms of Lehmer sequences, the characteristic roots are easier to work with and the methods described become clearer.

6.1 Introduction

The Binet formula allows for comparison of the various tests. First we restate the congruence relations of previous chapters in terms of the characteristic roots. As the congruences stand it is difficult to see how they are related, but with the same roots in similar expressions it will be easier to recognize relationships.

In Chapter 3, 4, and 5, we investigated several different congruences including the Lehmer, the M-Strong Lehmer, the Strong Lehmer 2, Lehmer Squared, and the Combined Lehmer Squared Criteria. Anywhere U_k or V_k appears in these congruences, they can be replaced by the appropriate Binet formula. By doing so we can restate all of our criteria in terms of the characteristic roots $\alpha, \beta = (\sqrt{R} \pm \sqrt{D})/2$.

We already used this technique in Chapter 3 to show that various connections between the four congruences of Lehmer Criteria. Some of the criteria we have examined are not as easily studied in terms of these characteristic roots. However, in certain instances this type of analysis can give special insight.

In the following sections, we summarize several results concerning the criteria from previous chapters all obtained by using this method.

6.2 Lehmer Criteria

Consider the four congruences given in the Lehmer Criteria of Chapter 3. Any prime must satisfy all of these congruences and we defined a lehpsp$_i(R, Q, D)$ if n satisfied Congruence i for $i = 1$, 2, 3, or 4 under the conditions that $(2RQD, n) = 1$ and $D = R - 4Q$. Although any set of three parameters is completely determined by knowing only two of them, we gave this definition for convenience as we compared sets of parameters.

The following theorem is true for any odd integer, but we will be chiefly concerned with pseudoprimes.

Theorem 6.2.1. *Lehmer Criteria via Characteristic Roots.*
If n is a positive integer with parameters satisfying $(2RQD, n) = 1$ and $\alpha, \beta = \frac{\sqrt{R} \pm \sqrt{D}}{2}$, then

1. *$U_{n-(RD|n)} \equiv 0$ (mod n) if and only if $\alpha^{n-(RD|n)} \equiv \beta^{n-(RD|n)}$ (mod n).*

2. *$V_{n-(RD|n)} \equiv 2(R|n)Q^{\frac{1-(RD|n)}{2}}$ (mod n). if and only if*
   $\alpha^{n-(RD|n)} + \beta^{n-(RD|n)} \equiv 2(R|n)(\alpha\beta)^{\frac{1-(RD|n)}{2}}$ (mod n).

3. *$U_n \equiv (D|n)$ (mod n) if and only if $\alpha^n - \beta^n \equiv (D|n)(\alpha - \beta)$ (mod n).*

4. *$V_n \equiv (R|n)\sqrt{R}$ (mod n) if and only if $\alpha^n + \beta^n \equiv (R|n)(\alpha + \beta)$ (modn).*

Proof. For the first equivalence, we have $U_{n-(RD|n)} \equiv 0$ $(mod\ n)$ if and only if $\frac{\alpha^{n-(RD|n)}-\beta^{n-(RD|n)}}{\alpha-\beta} \equiv 0$ $(mod\ n)$ if and only if $\alpha^{n-(RD|n)} \equiv \beta^{n-(RD|n)}$ $(mod\ n)$. All of the other congruences are proved in essentially the same way. We replace all of the parameters and Lehmer sequences using Theorem 1.5.1. □

In the proof we used Theorem 1.5.1. As a reminder, we recall some of the essential relationships, $\sqrt{R} = \alpha + \beta$, $\sqrt{D} = \alpha - \beta$, and $Q = \alpha\beta$. Using these restatements we can see connections between tests and parameters.

The first congruence above can be restated as $\left(\frac{\alpha}{\beta}\right)^{n-(RD|n)} \equiv 1$ $(mod\ n)$. Looking at the congruence this way it is more clear how Lucas and Lehmer sequences generalize Fermat's Little Theorem.

Recall in Chapter 3, we made use of these ideas to prove the following 3 theorems.

Theorem 6.2.2. *Parameter Reciprocity of Congruences 1 and 2.*
If n is an odd composite integer, then

i. n is a lehpsp$_1(R, Q, D)$ if and only if n is a lehpsp$_1(D, -Q, R)$.

ii. n is a lehpsp$_2(R, Q, D)$ if and only if n is a lehpsp$_2(D, -Q, R)$.

Theorem 6.2.3. *Parameter Bi-Reciprocity Between Congruences 3 and 4.*
If n is an odd composite integer, then n is a lehpsp$_3(R, Q, D)$ if and only if n is a lehpsp$_4(D, -Q, R)$.

Theorem 6.2.4. *Families of Parameters for Congruence 1.*

If n is a lehpsp$_1(R, Q, D)$, then

i. n is a lehpsp$_1(cR, cQ, cD)$ for all c with $(n, c) = 1$.

ii. n is a lehpsp$_1(cD, -cQ, cR)$ for all c with $(n, c) = 1$.

In addition, these families of parameters are different if $D \not\equiv -R \pmod{n}$.

Recall that the Parameter Bi-Reciprocity Between Congruences 3 and 4 allowed us to deduce that a composite number n was a Lehmer pseudoprimes for Congruence 3 for the same number of parameters as it was a Lehmer pseudoprime for Congruence 4. Thus, they give equally good tests for primality when random parameters are chosen.

We can use this theorem to give the following corollary:

Corollary 6.2.5. *The number n is a lehpsp$_1(R, Q, D)$ if and only if n is a lpsp$_1(R^2, RQ, RD)$.*

Proof. Take $c = R$ in Theorem 6.2.4. Note that the characteristic roots in this case become $\frac{R \pm \sqrt{RD}}{2}$ and so $(R^2 - RD)/4 = R(R - D)/4 = RQ$ give the new parameter value. □

This theorem says that Congruence 1 for Lehmer sequences with parameters R, Q, and D is equivalent to Congruence 1 for Lucas sequences using the parameters

$P = R^2$, RQ, and RD. From this we may want to conclude that Lucas and Lehmer sequences are equivalent tools in testing for primality. In the sense of Corollary 6.2.5, these test are related, yet the nature of the parameters for Lehmer sequences is in general different from that of the parameters for Lucas sequences. In particular, we see that the relationship in Corollary 6.2.5 only allows for P values which are quadratic residues. For various reason as illustrated in previous and the current chapters, we believe that the formulation in terms of Lehmer sequences is more theoretically sound. In addition, the majority of the results in this chapter only hold for the parameters of the Lehmer sequences.

Continuing with our analysis of Congruence 1 of the Lehmer Criteria, we have the following.

Theorem 6.2.6. *If n is lehpsp$_1(R, Q, D)$, then n is a lehpsp$_1([(R+D)/2]^2, 4Q^2, RD)$*

Proof. By the hypothesis, n satisfies $\alpha^{n-(RD|n)} \equiv \beta^{n-(RD|n)}$ $(mod\ n)$ which implies $(\alpha^2)^{n-(RD|n)} \equiv (\beta^2)^{n-(RD|n)}$ $(mod\ n)$. Expanding the characteristic roots gives $\alpha^2 = \frac{(R+D)/2+\sqrt{RD}}{2}$ and $\beta^2 = \frac{(R+D)/2-\sqrt{RD}}{2}$, which are precisely the roots given by the parameters in the conclusion. Note $RD = (R^2 + 2RD + D^2)/4 - (R^2 - 2RD + D^2)/4 = [(R + D)/2]^2 - [2(R - D)/4]^2$, this last term is precisely $[2Q]^2$. □

For a composite integer n, we used Theorem 6.2.4 to show that one set of parameters giving n as a pseudoprime for Congruence 1 can be used to create several sets of parameters that give n as a pseudoprime. We can take this idea further to show that two sets of parameters giving n as a pseudoprime can be combined to give even more sets of parameters giving n as a pseudoprime. Such arguments suggest that Congruence 1 may have a large number of parameters that give n as a pseudoprime.

Theorem 6.2.7. *If n is a lehpsp$_1(f^2, Q_0, g^2D)$ and n is a lehpsp$_1(h^2, Q_1, j^2D)$, then n is a lehpsp$_1([(fh+gjD)/2]^2, Q_2, [(fj+gh)/2]^2D)$. The parameter Q_i is defined implicitly by the corresponding R and D values for $i = 0, 1, 2$.*

Proof. Let $\alpha = \frac{f+g\sqrt{D}}{2}$,$\beta = \frac{f-g\sqrt{D}}{2}$,$\widehat{\alpha} = \frac{h+j\sqrt{D}}{2}$, and $\widehat{\beta} = \frac{h-j\sqrt{D}}{2}$. Thus, $\alpha^{n-(D|n)} \equiv \beta^{n-(D|n)}$ and $\widehat{\alpha}^{n-(D|n)} \equiv \widehat{\beta}^{n-(D|n)}$. So $(\alpha\widehat{\alpha})^{n-(D|n)} \equiv (\beta\widehat{\beta})^{n-(D|n)}$. Finally, note $\alpha\widehat{\alpha} = \frac{\frac{fh+gjD}{2}^2 + \frac{fj+gh}{2}\sqrt{D}}{2}$. □

Given two sets of parameters of the required form which yield a composite integer n as a pseudoprime, this theorem gives a method for systematically combining these parameters to get other 'bad' parameters.

In fact, we can prove the following:

Corollary 6.2.8. *If n is a lehpsp$_1(1, (1-D)/4, D)$ and n is a lehpsp$_1(a^2, Q_0, b^2D)$, where $Q_0 = (a^2 - b^2D)/4$ and if we define the sequences a_k and b_k by $a_0 = a$, $b_0 = b$, $a_k = \frac{a_{k-1}+b_{k-1}D}{2}$, and $b_k = \frac{a_{k-1}+b_{k-1}}{2}$ for $k > 0$, then n is a lehpsp$_1(a_k^2, Q_k, b_k^2D)$ for all k where $Q_k = (a_k^2 - b_k^2D)/4$.*

Proof. For a fixed nonnegative integer k, apply Theorem 6.2.7 with the substitutions $f = g = 1$, $h = a_k$ and $j = b_k$. The set of parameters in the conclusion of Theorem

6.2.7 satisfy $([(fh+gjD)/2]^2, Q_{k+1}, [(fj+gh)/2]^2D) = ([(a_k+b_kD)/2]^2, Q_{k+1}, [(b_k+a_k)/2]^2D) = (a_{k+1}^2, Q_{k+1}, b_{k+1}^2D)$. By induction, the statement is true for all $k \geq 0$. □

In order to illustrate the ideas expressed in the theorems of this section let us consider an example. Let $n = 35 = 5 \cdot 7$. Here we give all the parameters that yield n as a pseudoprime for Congruence 1. These were found by exhaustive search. It turns out that all of the parameters can be classified into 5 families.

Table 6.2.1: The parameters that give $n = 35$ as a pseudoprime for Congruence 1 of the Lehmer Criteria separated into distinct families and $(c, 35) = 1$.

c	$c(2,9,1)$	$c(18,13,1)$	$c(23,23,1)$	$c(32,34,1)$	$c(34,17,1)$
1	$(2,9,1)$	$(18,13,1)$	$(23,23,1)$	$(32,34,1)$	$(34,17,1)$
2	$(4,18,2)$	$(1,26,2)$	$(11,11,2)$	$(29,33,2)$	$(33,34,2)$
3	$(6,27,3)$	$(19,4,3)$	$(34,34,3)$	$(26,32,3)$	$(32,16,3)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Using this information, we see that the total number of parameters is $5\phi(n) = 5(4)(6) = 120$, which is precisely the value found by exhaustive search.

By Theorem 6.2.5, if n were found to satisfy Congruence 1 for any one set of parameters in one of these families, then n would also satisfy the congruence for all the parameters in the same column. In addition, the reciprocity of the parameters R and D would allow us to deduce that two of these columns would be satisfied. For instance, interchanging R and D in $(2, 9, 1)$ yields $(1, -9, 2) \equiv (1, 26, 2)$ $(mod\ 35)$ which appears in column 2.

These observations suggest some methods for choosing parameters. In particular, we would never want to choose parameters in the same family, since they automatically will satisfy the same congruence. These ideas need to be further developed, but they appear to be promising future research topics.

In Theorem 3.2.4, we gave a parameter count for the number of parameters that yielded a composite integer n as a pseudoprimes for a given fixed D. As illustrated in Table 6.2.1, Theorem 6.2.5 allows for the classification of parameters in families. In particular, we choose a representative of the family of parameters where $D = 1$. Thus, by simply counting the parameters that give a pseudoprime when $D = 1$, we immediately get a count on all parameters as follows.

Theorem 6.2.9. *Total Parameter Count for lehpsp*$_1(R, Q, D)$.
If $n = \prod_{i=1}^{k} p_i^{a_i}$ *is odd, then the number of distinct* D, R *and* Q *values modulo* n *satisfying* $R - 4Q \equiv D \pmod{n}$ *and* $(RQD, n) = 1$ *for which* $U_{n-(RD|n)}(\sqrt{R}, Q) \equiv 0 \pmod{n}$ *is given by*

$$\phi(n) \sum_{x\in\{-1,+1\}^k} \prod_{i=1}^{s} \left[\frac{1}{2}(n - h(x), p_i - x_i) - 1\right],$$

where $h(x) = \prod_{i=1}^{k} x_i^{a_i}$.

This theorem gives a count on all ‘bad’ parameters. To my knowledge, there is no analogous theorem for Lucas sequences. In addition, the bound of Theorem 3.3.2 can be applied to give a bound on the total number of parameters.

Theorem 6.2.10. *Total Parameter Bound for lehpsp*$_1(R, Q, D)$.

If n *is odd, then the number of distinct* D*,* R *and* Q *values modulo* n *satisfying* $R - 4Q \equiv D \pmod{n}$ *and* $(RQD, n) = 1$ *for which* $U_{n-(RD|n)}(\sqrt{R}, Q) \equiv 0 \pmod{n}$ *is bounded by* $\frac{\phi(n)^2}{2}$.

In the next section we explore various stronger Lehmer criteria.

6.3 Stronger Lehmer Criteria

We introduced several different stronger Lehmer criteria in Chapter 4. Here we illustrate what is happening in terms of the characteristic roots. The essential idea is the factoring of the expression $\alpha^{2^s d} - \beta^{2^s d}$. If the expression is congruent to zero, then at least one of the factors is congruence to zero. Using this simple argument we arrive at the following restatement of the Euler Criterion and the Strong Lehmer Criterion.

Theorem 6.3.1. *Euler and Strong Lehmer Criteria via Characteristic Roots.*

If n *is a positive integer with parameters satisfying* $(2RQD, n) = 1$*, then*

i. n *satisfies the Euler Lehmer Criterion if and only if* $\alpha^{\frac{n-(RD|n)}{2}} \equiv (RD|n)\beta^{\frac{n-(RD|n)}{2}} \pmod{n}$.

ii. n *satisfies the Strong Lehmer Criterion if and only if*

$\alpha^d \equiv \beta^d \pmod{n}$ *or* $\alpha^{2^r d} \equiv -\beta^{2^r d} \pmod{n}$ *for some* r *with* $0 \leq r < s$*, where* $n - (RD|n) = 2^s d$ *with* d *odd.*

By using the formula for factoring $x^3 - y^3$, we could also reformulate the 3-Strong Criterion. However, we elect to stay in the simpler case. The techniques used for

Congruence 1 of the Lehmer Criteria can be applied almost directly to these congruences.

Theorem 6.3.2. *Parameter Reciprocity of the Euler and Strong Lehmer Criteria. If n be an odd composite integer, then*

i. n is a elehpsp(R, Q, D) if and only if n is a elehpsp$(D, -Q, R)$.

ii. n is a slehpsp(R, Q, D) if and only if n is a slehpsp$(D, -Q, R)$.

Proof. We prove the second statement only, the first is proved in a similar way. Let $\alpha, \beta = \frac{\sqrt{R} \pm \sqrt{D}}{2}$ be the characteristic roots of $U(\sqrt{R}, Q, D)$. If $\widetilde{\alpha}$ and $\widetilde{\beta}$ are the characteristic roots of $U_k(\sqrt{D}, -Q, R)$, then $\widetilde{\alpha} = \alpha$ and $\widetilde{\beta} = -\beta$.

For $r > 0$, $\alpha^{2^r d} \equiv -\beta^{2^r d}$ $(mod\ n)$ if and only if $\widetilde{\alpha}^{2^r d} \equiv -\widetilde{\beta}^{2^r d}$ $(mod\ n)$. For $r = 0$, $\alpha^d \equiv \pm\beta^d$ $(mod\, n)$ if and only if $\widetilde{\alpha}^d \equiv \mp\widetilde{\beta}^d$ $(mod\, n)$. In any event, we have n satisfying the criteria with (R, Q, D) if and only if n satisfies the criteria with $(D, -Q, R)$. □

Theorem 6.3.3. *Strong Lehmer Families of Parameters. If n is a slehpsp$_1(R, Q, D)$, then*

i. n is a slehpsp$_1(cR, cQ, cD)$ for all c with $(n, c) = 1$.

ii. n is a slehpsp$_1(cD, -cQ, cR)$ for all c with $(n, c) = 1$.

Proof. If n is a slehpsp$_1(R, Q, D)$, then define $\alpha_c, \beta_c = \frac{\sqrt{cR} \pm \sqrt{cD}}{2} = \sqrt{c}\alpha_1, \sqrt{c}\beta_1$. Then $\alpha_1^{n-(RD|n)} \equiv \beta_1^{n-(RD|n)}$ $(mod\, n)$ if and only if $(\sqrt{c}\alpha_1)^{n-(RD|n)} \equiv (\sqrt{c}\beta_1)^{n-(RD|n)}$ $(mod\, n)$

if and only if $\alpha_c^{n-(c^2RD|n)} \equiv \beta_c^{n-(c^2RD|n)}$ $(mod\ n)$. The second claim follows from Theorem 3.4.1.

For $r > 0$, $\alpha^{2^r d} \equiv -\beta^{2^r d}$ $(mod\ n)$ if and only if $\alpha_c^{2^r d} \equiv -\beta_c^{2^r d}$ $(mod\ n)$. For $r = 0$, $\alpha^d \equiv \pm\beta^d$ $(mod\ n)$ if and only if $\alpha_c^d \equiv \pm\beta_c^d$ $(mod\ n)$. Thus, we have n satisfying the criteria with (R, Q, D) if and only if n satisfies the criteria with (cR, cQ, cD).

The second statement follows from 6.3.2. □

A similar statement would be true for Euler-Lehmer pseudoprimes. The last two results are interesting in that they are identical to the results for the Lehmer Congruence 1 theorems of the last section. Heuristically, we can argue by the theorems of this section and the last that if n is a pseudoprime for one parameter then it is a pseudoprime for many parameters. However, numerical evidence shows that strong Lehmer testing can significantly decrease the number of pseudoprimes when compared to Lehmer Congruence 1 testing. Thus, if Strong Lehmer testing eliminates one ‘bad’ parameter set for an odd composite n when compared to Congruence 1 testing, then Strong Lehmer testing eliminates a whole family of parameters. Actually, since we have parameter reciprocity, eliminating one parameters with Strong Lehmer testing implies that 2 families of parameters have been eliminated except in the special case where reciprocity gives the same family.

Going back to the example of the last section, let us examine the parameters that give $n = 35 = 5 \cdot 7$ as a Strong Lehmer pseudoprime. The discussion of the last section makes the claim that the Strong Lehmer Criterion can only eliminate entire families of parameters. It is not possible for the Strong Lehmer Criterion to eliminate only part of a family. This is indeed the case in our example.

Table 6.3.1: The parameters that give $n = 35$ as a pseudoprime for the Strong Lehmer Criterion separated into distinct families and $(c, 35) = 1$.

c	$c(23, 23, 1)$	$c(32, 34, 1)$	$c(34, 17, 1)$
1	$(23, 23, 1)$	$(32, 34, 1)$	$(34, 17, 1)$
2	$(11, 11, 2)$	$(29, 33, 2)$	$(33, 34, 2)$
3	$(34, 34, 3)$	$(26, 32, 3)$	$(32, 16, 3)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Notice that the first two columns that appeared in Table 6.2.1 have vanished. Thus, in this case, Strong Lehmer testing has eliminated exactly two families of parameters. This lowers the total number of bad parameters from 120 to $120 - 2\phi(n) = 120 - 2(4)(6) = 72$. Thus, we see more explicitly the advantages of Strong Lehmer testing.

We noted earlier that the characteristic root analysis of this section can also be applied to the M-Strong Lehmer Criteria. In particular, it is interesting to note that the 3-Strong Lehmer Criteria has families of parameters and these families are a subset of the families for the Strong Lehmer Criterion. Instead of digressing into a detailed analysis of this case, we continue with the example $n = 35$ as an illustration of these ideas.

Table 6.3.2: The parameters that give $n = 35$ as a pseudoprime for the 3-Strong Lehmer Criterion separated into distinct families and $(c, 35) = 1$.

c	$c(32, 34, 1)$
1	$(32, 34, 1)$
2	$(29, 33, 2)$
3	$(26, 32, 3)$
$\vdots$	$\vdots$

While the parameters still are separated into families for the 3-Strong Lehmer Criterion, it should be noted that we no longer have parameter reciprocity. In this example, if $(R, Q, D) = (32, 34, 1)$, then $(D, -Q, R) = (1, -34, 32)$. Taking $c = R^{-1} = 23$, we see that this parameter set belongs to the family $(23, 23, 1)$. From Table 6.3.2, we see that this family does not give n as a pseudoprime for the 3-Strong Criteria. In 3-Strong Testing, the exponents of the characteristic roots are not necessarily even. Noting this fact, it is not surprising that reciprocity does not hold.

We do not give a characteristic root analysis of the Strong Lehmer 2 Criterion. It would require a more detailed treatment.

6.4 Lehmer Squared Criteria

In Chapter 5, we explored criteria for primality modulo n^2 using Lehmer sequences. We were somewhat disappointed in the effectiveness of the Lehmer Squared Criteria. However, we improved our results by using a Combination of tests. In this section, we give some partial explanations for these observations.

Theorem 6.4.1. *Lehmer Squared Criteria via Characteristic Roots.*

If n is a positive integer with parameters satisfying $(2RQD, n) = 1$, $\alpha, \beta = \frac{\sqrt{R} \pm \sqrt{D}}{2}$, and $\widetilde{\alpha}, \widetilde{\beta} = \frac{\sqrt{R^n} \pm \sqrt{D^n}}{2}$, then

1. $2U_{n^2+1} \equiv \sqrt{R} D^{(n-1)/2} \widetilde{U}_n + \widetilde{V}_n$ *(mod n^2) if and only if*

   $\alpha^{n^2+1} - \beta^{n^2+1} \equiv \alpha\widetilde{\alpha}^n - \beta\widetilde{\beta}^n$ *(mod n^2).*

2. $2V_{n^2+1} \equiv D^{(n+1)/2} \widetilde{U}_n + \sqrt{R}\widetilde{V}_n$ *(mod n^2) if and only if*

   $\alpha^{n^2+1} + \beta^{n^2+1} \equiv \alpha\widetilde{\alpha}^n + \beta\widetilde{\beta}^n$ *(mod n^2).*

3. $U_{n^2} \equiv D^{(n-1)/2} \widetilde{U}_n$ *(mod n^2) if and only if*

   $\alpha^{n^2} - \beta^{n^2} \equiv \widetilde{\alpha}^n - \widetilde{\beta}^n$ *(mod n^2).*

4. $V_{n^2} \equiv \widetilde{V}_n$ *(mod n) if and only if*

   $\alpha^{n^2} + \beta^{n^2} \equiv \widetilde{\alpha}^n + \widetilde{\beta}^n$ *(mod n^2).*

Proof. The same techniques as before work here, but we prove the third relationship to illustrate the origins of these statements. Recall $\alpha - \beta = \sqrt{D}$ and $\widetilde{\alpha} - \widetilde{\beta} = \sqrt{D^n}$. Thus, the Binet formulas give $U_{n^2} \equiv D^{(n-1)/2} \widetilde{U}_n$ *(mod n^2)* if and only if $\frac{\alpha^{n^2} - \beta^{n^2}}{\sqrt{D}} \equiv D^{(n-1)/2} \frac{\widetilde{\alpha}^n - \widetilde{\beta}^n}{\sqrt{D^n}}$ if and only if $\alpha^{n^2} - \beta^{n^2} \equiv \widetilde{\alpha}^n - \widetilde{\beta}^n$ *(mod n^2).* □

These congruences satisfy many of the same properties as summarized in the next two theorems.

Theorem 6.4.2. *Parameter Reciprocity for Congruence 1 and 2.*

If n is an odd composite integer, then

i. n is a lehpsp$_1^2(R, Q, D)$ if and only if n is a lehpsp$_1^2(D, -Q, R)$.

ii. n is a lehpsp$_2^2(R, Q, D)$ if and only if n is a lehpsp$_2^2(D, -Q, R)$.

Proof. Define $\alpha_1 = \frac{\sqrt{D}+\sqrt{R}}{2} = \alpha$, $\beta_1 = \frac{\sqrt{D}-\sqrt{R}}{2} = -\beta$, $\widetilde{\alpha}_1 = \frac{\sqrt{D^n}+\sqrt{R^n}}{2} = \widetilde{\alpha}$, and $\widetilde{\beta}_1 = \frac{\sqrt{D^n}-\sqrt{R^n}}{2} = -\widetilde{\beta}$.

Noting that the key fact is that n is odd, we have $\alpha^{n^2+1} - \beta^{n^2+1} \equiv \alpha\widetilde{\alpha}^n - \beta\widetilde{\beta}^n$ $(mod\ n^2)$ if and only if $\alpha_1^{n^2+1} - \beta_1^{n^2+1} \equiv \alpha_1\widetilde{\alpha}_1^n - (-\beta_1)(-\widetilde{\beta}_1^n)$. The same technique proves the second claim. □

Theorem 6.4.3. *Parameter Bi-Reciprocity Between Congruences 3 and 4.*

If n is an odd composite integer, then n is a lehpsp$_3^2(R, Q, D)$ if and only if n is a lehpsp$_4^2(D, -Q, R)$.

Proof. Define $\alpha_1 = \frac{\sqrt{D}+\sqrt{R}}{2} = \alpha$, $\beta_1 = \frac{\sqrt{D}-\sqrt{R}}{2} = -\beta$, $\widetilde{\alpha}_1 = \frac{\sqrt{D^n}+\sqrt{R^n}}{2} = \widetilde{\alpha}$, and $\widetilde{\beta}_1 = \frac{\sqrt{D^n}-\sqrt{R^n}}{2} = -\widetilde{\beta}$. Once again, we note that n is odd.

So $\alpha^{n^2} - \beta^{n^2} \equiv \widetilde{\alpha}^n - \widetilde{\beta}^n$ $(mod\ n^2)$ if and only if $\alpha_1^{n^2} + \beta_1^{n^2} \equiv \widetilde{\alpha}_1^n + \widetilde{\beta}_1^n$ $(mod\ n^2)$. □

From this theorem, we conclude that Congruences 3 and 4 of the Lehmer Squared Criteria will always have exactly the same number of parameters yielding a pseudoprime. Therefore, in a sense these tests are equally good.

Theorem 6.4.4. *Lehmer Squared Families of Parameters.*

If n is an odd composite integer, then

i. n is a lehpsp$_3^2(R,Q,D)$ if and only if n is a lehpsp$_3^2(cR,cQ,cD)$ for all c with $(n,c)=1$.

ii. n is a lehpsp$_4^2(R,Q,D)$ if and only if n is a lehpsp$_4^2(cR,cQ,cD)$ for all c with $(n,c)=1$.

Proof. Define $\alpha_1 = \frac{\sqrt{cD}+\sqrt{cR}}{2} = \sqrt{c}\alpha$, $\beta_1 = \frac{\sqrt{cR}-\sqrt{cD}}{2} = -\sqrt{c}\beta$,$\widetilde{\alpha}_1 = \frac{\sqrt{(cD)^n}+\sqrt{(cR)^n}}{2} = \sqrt{c^n}\widetilde{\alpha}$, and $\widetilde{\beta}_1 = \frac{\sqrt{(cR)^n}-\sqrt{(cD)^n}}{2} = -\sqrt{c^n}\widetilde{\beta}$.

Thus, $\alpha^{n^2}-\beta^{n^2} \equiv \widetilde{\alpha}^n - \widetilde{\beta}^n \ (mod\ n^2)$ if and only if $(\sqrt{c}\alpha)^{n^2}-(\sqrt{c}\beta)^{n^2} \equiv (\sqrt{c^n}\widetilde{\alpha})^n - (\sqrt{c^n}\widetilde{\beta})^n \ (mod\ n^2)$ if and only if $\alpha_1^{n^2}-\beta_1^{n^2} \equiv \widetilde{\alpha}_1^n - \widetilde{\beta}_1^n \ (mod\ n^2)$. This gives the first claim. The second is proved in a similar way. □

This theorem suggest that we may not be making a marked improvement on the standard tests, since we are proving exactly the same types of theorems concerning parameters. By no means have we proved that these congruences should be better or worse than the standard criteria, but it at least gives a partial explanations for why the numerical data was not as good as we would have suspected.

6.5 Combined Lehmer Squared Criteria

Finally, in this section we explore the Combined Lehmer Squared Criteria of Chapter 5. We gave 4 congruences for the Combined Lehmer Squared Criteria, however, Congruences 3 and 4 were much simpler than 1 and 2. For simplicity we focus on Congruences 3 and 4 alone.

Theorem 6.5.1. *Combined Lehmer Squared Criteria via Characteristic Roots. If n is a positive integer with parameters satisfying $(2RQD, n) = 1$, $\alpha, \beta = \frac{\sqrt{R}\pm\sqrt{D}}{2}$, and $\widetilde{\alpha}, \widetilde{\beta} = \frac{\sqrt{R^n}\pm\sqrt{D^n}}{2}$, then*

1. $2\left(\frac{D}{n}\right) U_{n^2} \equiv D^{(n-1)/2}[\widetilde{U}_n^2 + 1]$ $(mod\ n^2)$ *if and only if*

   $2\left(\frac{D}{n}\right)(\alpha^{n^2} - \beta^{n^2}) \equiv \frac{(\widetilde{\alpha}^n - \widetilde{\beta}^n)^2}{\widetilde{\alpha}-\widetilde{\beta}} + \widetilde{\alpha} - \widetilde{\beta}$ $(mod\ n^2)$.

2. $2\left(\frac{R}{n}\right)\sqrt{R}V_{n^2} \equiv \widetilde{V}_n^2 + R$ $(mod\ n^2)$ *if and only if*

   $2\left(\frac{R}{n}\right)(\alpha^{n^2} + \beta^{n^2}) \equiv \frac{(\widetilde{\alpha}^n + \widetilde{\beta}^n)^2}{\alpha+\beta} + \alpha + \beta$ $(mod\ n^2)$.

Proof. We prove the first relationship. The second is proved in a similar way. The Binet formulas give $2\left(\frac{D}{n}\right) U_{n^2} \equiv D^{(n-1)/2}[\widetilde{U}_n^2+1]$ $(mod\ n^2)$ if and only if $2\left(\frac{D}{n}\right)\frac{\alpha^{n^2}-\beta^{n^2}}{\sqrt{D}} \equiv D^{(n-1)/2}[\frac{(\widetilde{\alpha}^n-\widetilde{\beta}^n)^2}{D^n}+1]$ $(mod\ n^2)$ if and only if $2\left(\frac{D}{n}\right)(\alpha^{n^2}-\beta^{n^2}) \equiv \frac{(\widetilde{\alpha}^n-\widetilde{\beta}^n)^2}{\sqrt{D^n}}+\sqrt{D^n}$ $(mod\ n^2)$. Making the replacement $\sqrt{D^n} = \widetilde{\alpha} - \widetilde{\beta}$ gives the result. □

In terms of the characteristic roots, these congruences do not possess the same relationships as the other criteria explored in this chapter. If $R^n \equiv R$ $(mod\ n)$ and $D^n \equiv D$ $(mod\ n)$, then we could say more. However, if we wish to make general statements relating parameters for an odd composite integer n, then this assumption is rarely valid.

Since the techniques of the previous sections do not give way to relationships giving many parameters from one, we at least have a heuristic explanation for why these congruences were numerically more effective in Chapter 5.

Chapter 7

Finite Commutative Ring Lehmer Testing

In [22] and [23], finite rings are effectively used to give strong probable prime tests. However, there is currently no study where elements of a finite ring are taken as the coefficients in a Lehmer sequences. This chapter is devoted to this topic. We prove that even with this generality, many of the parameter properties discussed in Chapter 6 still hold.

7.1 Introduction

Of the various primality tests we have studied none are infallible. They all exhibit pseudoprimes. We have seen that the number of pseudoprimes can be greatly effected by the method in which parameters are chosen. By taking a broad look at the numerical results, one might suspect that pseudoprimes occur at random. Even though there is intrinsic order to the pseudoprimes that occur for each tests, heuristically the fact that n turns out to be a pseudoprime for a given method could be attributed to some kind of randomness, or "luck". Using this way of thinking, we might want to argue that the output of say U_n $(mod\ n)$ is almost random for a composite n and if it happens to satisfy a congruence which would be true if n were a prime, then this is due to some sort of luck. Thus, by increasing the possible output values of U_n $(mod\ n)$, we would make it less likely that n turns out to be a pseudoprime. With this in mind we turn to larger finite rings to accomplish exactly this task.

7.2 Lehmer Sequences in Finite Commutative Rings

Let $\mathbb{R}$ denote a finite commutative ring with identity. In Section 1.7, we discussed such rings. These ideas where defined as one would expect, but refer to back for more details.

As with integer Lehmer sequences, if $R \in \mathbb{R}$, we define $\sqrt{R}$ to be an object that when squared gives R. We never evaluate $\sqrt{R}$ and we define $a\sqrt{R} + b \equiv c\sqrt{R} + d$ $(mod\ n)$ if $a \equiv c$ $(mod\ n)$ and $b \equiv d$ $(mod\ n)$.

For $R, Q \in \mathbb{R}$, we define the Lehmer sequences

$$U_k(\sqrt{R}, Q) = \sqrt{R}U_{k-1}(\sqrt{R}, Q) - QU_{k-2}(\sqrt{R}, Q), \quad U_0(\sqrt{R}, Q) = 0, U_1(\sqrt{R}, Q) = 1$$

$$V_k(\sqrt{R}, Q) = \sqrt{R}V_{k-1}(\sqrt{R}, Q) - QV_{k-2}(\sqrt{R}, Q), \quad V_0(\sqrt{R}, Q) = 2, V_1(\sqrt{R}, Q) = \sqrt{R}.$$

As before $D = R - 4Q \in \mathbb{R}$. All computations are done in the ring. Since $\sqrt{R}$ is only defined when it is squared, we can use the companion sequences in Chapter 3 to compute the terms as coefficients without evaluating the expression $\sqrt{R}$.

In the general setting of commutative rings with identity, the characteristic roots $\alpha, \beta = \frac{\sqrt{R} \pm \sqrt{D}}{2}$ are in a ring extension. These sequences still satisfy the Binet formulas, $U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}$ and $V_k = \alpha^k + \beta^k$.

Now we are prepared to give the four congruences of the Lehmer Criteria in the general setting of $\mathbb{R}$. Since we have not defined the Jacobi symbol when D and R are elements in a general finite ring, we will give the congruences with both subscripts $n-1$ and $n+1$.

Theorem 7.2.1. *The Commutative Ring Lehmer Criteria.*

If n is an odd prime, $\epsilon = \pm 1$, $R, Q \in \mathbb{R}$ where $\mathbb{R}$ is a commutative ring with identity, and $D = R - 4Q$, then

1. $2Q^{(1+\epsilon)/2} U_{n-\epsilon}(\sqrt{R}, Q) \equiv [D^{(n-1)/2} - \epsilon R^{(n-1)/2}]\sqrt{R}$ *(mod n).*

2. $2Q^{(1+\epsilon)/2} V_{n-\epsilon}(\sqrt{R}, Q) \equiv R^{(n+1)/2} - \epsilon D^{(n+1)/2}$ *(mod n).*

3. $U_n(\sqrt{R}, Q) \equiv D^{(n-1)/2}$ *(mod n).*

4. $V_n(\sqrt{R}, Q) \equiv R^{(n-1)/2}\sqrt{R}$ *(mod n).*

Proof. For any integer k, the identity of Theorem 1.5.4 applies, since it only depends on the binomial expansion of the Binet formulas and the commutativity of the ring:

$$2^{k-1} U_k = \sum_{i\ odd} \left(\begin{array}{c} k \\ i \end{array} \right) R^{(k-i)/2} D^{(i-1)/2}$$

$$2^{k-1} V_k = \sum_{i\ even} \left(\begin{array}{c} n \\ i \end{array} \right) R^{(k-i)/2} D^{i/2}.$$

Using the characterization of primes via binomial coefficients (Theorem 1.2.1), we replace k by n in the above sums and eliminate terms congruent to zero modulo n. The definition of congruence in the ring and the reduction of the identities above yields Congruences 3 and 4 of the theorem.

$$U_n \equiv 2^{n-1}U_n \equiv D^{(n-1)/2} \ (mod\ n)$$

$$V_n \equiv 2^{n-1}V_n \equiv R^{n/2} \equiv R^{(n-1)/2}\sqrt{R} \ (mod\ n).$$

Using the identities of Corollary 1.5.3 gives the first 2 congruences

$$2Q^{(1+\epsilon)/2}U_{n-\epsilon} = U_nV_1 - \epsilon V_n \equiv [D^{(n-1)/2} - \epsilon R^{(n-1)/2}]\sqrt{R} \ (mod\ n)$$

$$2Q^{(1+\epsilon)/2}V_{n-\epsilon} = V_nV_1 - \epsilon U_n \equiv R^{(n+1)/2} - \epsilon R^{(n+1)/2} \ (mod\ n).$$

□

If n is an odd composite integer satisfying Congruence i, then we say n is a Lehmer pseudoprime with respect to the parameters R, Q, and D in the ring $\mathbb{R}$ (denoted $\mathbb{R}$-lehpsp$_i(R, Q, D)$) for $i = 3$ or 4. In the first two congruence the notation must distinguish between $\epsilon = +1$ and $\epsilon = -1$. We accomplish this by letting $i = 1^+$ or 1^- according to $\epsilon = +1$ or $\epsilon = -1$. The same convention is used for $i = 2^{\pm}$. Note that all these definitions are only defined for parameters that satisfy $D = R - 4Q$.

If n is a prime and R and D are integers with $(RD, n) = 1$, then $R^{(n-1)/2} \equiv (R|n) \ (mod\ n)$ and $D^{(n-1)/2} \equiv (D|n) \ (mod\ n)$. Thus, if n is a prime, $\mathbb{R} = \mathbb{Z}_n$, and

$\epsilon = (RD|n)$, then each of the congruences above reduce to the standard Lehmer Criteria of Chapter 2.

In the next section we will examine the characteristic roots of the congruences of Theorem 7.2.1 in the case of a general commutative ring with identity $\mathbb{R}$. Then we give realizations of this criteria in quotient rings.

7.3 Characteristic Root Analysis of General Case

Since the characteristic roots have the same form, we can apply the techniques of Chapter 6 to get relationship between parameters where a given integer satisfies the congruence. First we reformulate the congruences in Theorem 7.2.1 in terms of the characteristic roots.

Theorem 7.3.1. *The Commutative Ring Lehmer Criteria via Characteristic Roots. If n is an odd integer, $\epsilon = \pm 1$, $R, Q \in \mathbb{R}$ where $\mathbb{R}$ is a commutative ring with identity, and $D = R - 4Q$, then*

1. $2Q^{(1+\epsilon)/2}U_{n-\epsilon} \equiv [D^{(n-1)/2} - \epsilon R^{(n-1)/2}]\sqrt{R}$ *(mod n) if and only if*

   $2(\alpha\beta)^{(1+\epsilon)/2}(\alpha^{n-\epsilon} - \beta^{n-\epsilon}) \equiv [(\alpha-\beta)^{n-1} - \epsilon(\alpha+\beta)^{n-1}](\alpha^2 - \beta^2)$ *(mod n).*

2. $2Q^{(1+\epsilon)/2}V_{n-\epsilon}(\sqrt{R}, Q) \equiv R^{(n+1)/2} - \epsilon D^{(n+1)/2}$ *(mod n) if and only if*

   $2(\alpha\beta)^{(1+\epsilon)/2}(\alpha^{n-\epsilon} + \beta^{n-\epsilon}) \equiv (\alpha+\beta)^{n+1} - \epsilon(\alpha-\beta)^{n+1}$ *(mod n).*

3. $U_n \equiv D^{(n-1)/2}$ *(mod n) if and only if*

   $\alpha^n - \beta^n \equiv (\alpha - \beta)^n$ *(mod n).*

4. $V_n \equiv R^{(n-1)/2}\sqrt{R}$ *(mod n) if and only if*

$\alpha^n + \beta^n \equiv (\alpha+\beta)^n$ *(mod n).*

Congruences 1 and 2 are not as easy to analyze in this general setting. By examining, $\epsilon = +1$ and $\epsilon = -1$ separately we can prove specific results.

Theorem 7.3.2. *Parameter Reciprocity for Congruence 1 and 2 (ϵ = -1). If n is an odd composite integer, then*

i. n is a $\mathbb{R}$*-lehpsp*$_{1^-}(R,Q,D)$ *if and only if n is a* $\mathbb{R}$*-lehpsp*$_{1^-}(D,-Q,R)$.

ii. n is a $\mathbb{R}$*-lehpsp*$_{2^-}(R,Q,D)$ *if and only if n is a* $\mathbb{R}$*-lehpsp*$_{2^-}(D,-Q,R)$.

Proof. Define α , β and α_1 , β_1 to represent the characteristic roots for the parameter sets (R,Q,D) and $(D,-Q,R)$ respectively. Note that these roots satisfy $\alpha = \alpha_1$ and $\beta = -\beta_1$. Using the characteristic root reformulation in Theorem 7.3.1, we see that the Congruences 1 and 2 are satisfied in the case $\epsilon = -1$ with α and β, if and only if they are satisfied with α_1 and β_1. □

The case $\epsilon = +1$ is somewhat more cumbersome, so we elect to focus the remainder of our analysis on Congruences 3 and 4.

Theorem 7.3.3. *Parameter Bi-Reciprocity for Congruences 3 and 4. If n is an odd composite integer, then n is a* $\mathbb{R}$*-lehpsp*$_3(R,Q,D)$ *if and only if n is a* $\mathbb{R}$*-lehpsp*$_4(D,-Q,R)$.

Proof. We use the same relationships between the characteristic roots of these parameters as discussed in the last proof. The roots satisfy the characterization of Congruence 3 in Theorem 7.3.1 if and only if the corresponding roots satisfy Congruence 4 in Theorem 7.3.1. □

Thus, in the general case, we can conclude that Congruences 3 and 4 have the same number of parameters giving n as a pseudoprime. We can also prove quite a bit more in the case of Congruences 3 and 4.

Theorem 7.3.4. *Families of Parameters for Congruences 3 and 4.*
If n is an odd composite integer and c is any integer such that $(c, n) = 1$, then

i. n is a $\mathbb{R}$-lehpsp$_3(R, Q, D)$ if and only if n is a $\mathbb{R}$-lehpsp$_3(cR, cQ, cD)$.

ii. n is a $\mathbb{R}$-lehpsp$_4(R, Q, D)$ if and only if n is a $\mathbb{R}$-lehpsp$_4(cR, cQ, cD)$.

Proof. Here we consider the roots $\alpha_c = \sqrt{c}\alpha$ and $\beta_c = \sqrt{c}\beta$ where $\alpha, \beta = \frac{\sqrt{R} \pm \sqrt{D}}{2}$. For any c value with $(c, n) = 1$, we can multiply both sides of Congruences 3 in Theorem 7.3.1 by $\sqrt{c^n}$ to see that the congruence is satisfied with α and β if and only if it is satisfied with α_c and β_c. Finally, noting that these roots are exactly the roots corresponding to the parameters in the theorem, we see that the first claim is true. The same technique gives the second claim. □

This is a powerful theorem and it is interesting that it holds in the general case. It allows us to conclude that all of the parameters can be classified into families as we did in the examples in Chapter 6. Also notice that we were unable to prove a corresponding theorem in the specific case of Congruences 3 and 4 of the standard Lehmer criteria. This seems like a contradiction. However, in the standard Lehmer criteria we not only use the congruences here, but we also make use of Jacobi symbols and the values they should give at primes. Thus, the standard Lehmer criteria we discussed had extra conditions placed upon it.

All of these theorems apply broadly to Lehmer sequences over any commutative ring with identity. Until now the only cases discussed in the literature were limited to the instances when $\mathbb{R}$ was Z_n for some integer n. For the remainder of this chapter, we explore the case where $\mathbb{R}$ is a quotient ring.

7.4 Lehmer Sequences in Quotient Rings

For a given integer n and a nonzero polynomial $f(x)$, let R and Q be elements of the finite ring $\mathbb{Z}_n[x]/(f(x))$ and consider the same Lehmer sequences as before:

$$U_k = \sqrt{R}U_{k-1} - QU_{k-2}, \quad U_0 = 0, U_1 = 1$$

$$V_k = \sqrt{R}V_{k-1} - QV_{k-2}, \quad V_0 = 2, V_1 = \sqrt{R}.$$

All computations are done in the ring.

Most mathematical software packages now come with commands that implement finite ring and finite field arithmetic. In addition, these computations can be realized via matrices using the finite ring representation discussed in Chapter 1. The tests we develop here are slower in practice, but have the same order of magnitude. That is, the tests will still take O(log(n)) time, but the constant multiplier will be larger in this case.

Notice that $\mathbb{Z}_n[x]/(f(x))$ is in general only a ring. However, if n is a prime and $f(x)$ is an irreducible polynomial, then this set is a field. In this chapter, we first let $f(x)$ be an arbitrary polynomial of any degree d and consider the resulting congruences. Then in subsequent sections we will investigate special forms for $f(x)$.

Setting $\mathbb{R} = \mathbb{Z}_n[x]/(f(x))$ in Theorem 7.2.1 we obtain the following.

Theorem 7.4.1. *The Lehmer Criteria in a Quotient Ring.*

If n is an odd prime, $\epsilon = \pm 1$, $R, Q \in \mathbb{Z}_n[x]/(f(x))$ where $f(x)$ is a nonzero polynomial, and $D = R - 4Q$, then

1. $2Q^{(1+\epsilon)/2}U_{n-\epsilon} \equiv [D^{(n-1)/2} - \epsilon R^{(n-1)/2}]\sqrt{R}$ $(mod\ f(x), n)$.

2. $2Q^{(1+\epsilon)/2}V_{n-\epsilon} \equiv R^{(n+1)/2} - \epsilon D^{(n+1)/2}$ $(mod\ f(x), n)$.

3. $U_n \equiv D^{(n-1)/2}$ $(mod\ f(x), n)$.

4. $V_n \equiv R^{(n-1)/2}\sqrt{R}$ $(mod\ f(x), n)$.

Note that we use the notation $(mod\ f(x), n)$ as a reminder that reduction in the quotient ring must be done modulo $f(x)$ and n. See [22] for an elaborate discussion of this notation and the corresponding operations.

These congruences are somewhat less satisfying than those for the integer sequences. However, they do not require a great deal more calculation. Computations take slightly longer since they are all being done in a finite ring and now we have to exponentiate where we only need to compute a Jacobi symbol before.

Before we consider special polynomials $f(x)$, we first discuss the situations where R and/or D are in the base field. In these case, the Jacobi Symbol can be used. Note that these are major restrictions and may greatly hinder the effectiveness of the resulting primality tests. However, they are interesting for comparison with tests we have previously examined and they give simpler characterizations.

Corollary 7.4.2. *D in the Base Field.*

If n is an odd prime, $\epsilon = \pm 1$, $R, Q \in \mathbb{Z}_n[x]/(f(x))$ where $f(x)$ is a nonzero polynomial, and $D = R - 4Q \in \mathbb{Z}_n$, then

1. $2Q^{(1+\epsilon)/2}U_{n-\epsilon} \equiv [(D|n) - \epsilon R^{(n-1)/2}]\sqrt{R}$ *(mod $f(x), n$).*

2. $2Q^{(1+\epsilon)/2}V_{n-\epsilon} \equiv R^{(n+1)/2} - \epsilon(D|n)D$ *(mod $f(x), n$).*

3. $U_n \equiv (D|n)$ *(mod $f(x), n$).*

4. $V_n \equiv R^{(n-1)/2}\sqrt{R}$ *(mod $f(x), n$).*

Corollary 7.4.3. *R in the Base Field.*

If n is an odd prime, $\epsilon = \pm 1$, $Q \in \mathbb{Z}_n[x]/(f(x))$ where $f(x)$ is a nonzero polynomial, $R \in \mathbb{Z}_n$ and $D = R - 4Q$, then

1. $2Q^{(1+\epsilon)/2}U_{n-\epsilon} \equiv [D^{(n-1)/2} - \epsilon(R|n)]\sqrt{R}$ *(mod* $f(x), n)$.

2. $2Q^{(1+\epsilon)/2}V_{n-\epsilon} \equiv (R|n)R - \epsilon D^{(n+1)/2}$ *(mod* $f(x), n)$.

3. $U_n \equiv D^{(n-1)/2}$ *(mod* $f(x), n)$.

4. $V_n \equiv (R|n)\sqrt{R}$ *(mod* $f(x), n)$.

If R and D are in the base field, then Q is automatically in the base field. Thus, choosing any two parameters in the base field reduces to the standard Lehmer criteria of Chapter 3. Note that both of these Corollaries could be implemented by choosing D or R in the base field first and then choosing the second parameter and computing the third.

Any of these congruences could be tested as they stand. For ease in implementation and efficiency in testing we will spend the next section looking into special types of parameters that will lead to tests which involve fewer computations. By simplifying, we may be losing some the effectiveness of the test. Numerical calculations at the end of this chapter will illustrate the effectiveness of various simplifications.

7.5 Special Types of Quotient Rings

The easiest way to simplify our criteria is by restricting the form of the polynomial $f(x)$. In this section, we will investigate what happens in Theorem 7.4.1 when $f(x)$ has the very specific form, $x^d - f_0$.

Let n be an odd integer. Consider a polynomial of the form $f(x) = x^d - f_0$ where $f_0 \in \mathbb{Z}_n$ and $d|(n-1)$. The test will be at its simplest when $d = 2$, but the development is essentially the same for any $d|(n-1)$. The elements of this ring satisfy the following properties.

Theorem 7.5.1. *If n is an odd prime and $f(x) = x^d - f_0$ such that $d|(n-1)$, then*

i. $x^d \equiv f_0$ *(mod $f(x), n$).*

ii. $x^n \equiv f_0^{\frac{n-1}{d}} x$ *(mod $f(x), n$).*

iii. $(a_{d-1}x^{d-1} + \cdots + a_1 x + a_0)^n \equiv a_{d-1} f_0^{\frac{(n-1)(d-1)}{d}} x^{d-1} + \cdots + a_1 f_0^{\frac{n-1}{d}} x + a_0$ *(mod $f(x), n$).*

Proof. The first claim follows immediately from the definition. Since $d|n-1$, we have

$$x^{n-1} \equiv (x^d)^{\frac{n-1}{d}} \equiv (f_0)^{\frac{n-1}{d}} \equiv f_0^{\frac{n-1}{d}} \ (mod\ f(x), n).$$

Thus, $x^n \equiv f_0^{\frac{n-1}{d}} x \ (mod\ f(x), n)$.

For the third claim, the multinomial theorem gives

$$\begin{aligned}(\textstyle\sum_{k=0}^{d-1} a_k x^k)^n &= \textstyle\sum_{k_0+\cdots+k_{d-1}=n} \begin{pmatrix} n \\ k_0, k_1, \ldots, k_{d-1} \end{pmatrix} a_0^{k_0} (a_1 x)^{k_1} \ldots (a_{d-1}x^{d-1})^{k_{d-1}} \\ &\equiv \textstyle\sum_{k=0}^{d-1} a_k^n x^{kn} \equiv \sum_{k=0}^{d-1} a_k (f_0^{\frac{n-1}{d}} x)^k \ (mod\ f(x), n).\end{aligned}$$

□

Letting $d = 2$ yields the following corollary.

Corollary 7.5.2. *If n is an odd prime and $f(x) = x^2 - f_0$, then*

i. $x^2 \equiv f_0$ *(mod* $f(x), n)$.

ii. $x^n \equiv (f_0|n)x$ *(mod* $f(x), n)$.

iii. $(a_1x + a_0)^n \equiv a_1(f_0|n)x + a_0$ *(mod* $f(x), n)$.

Note that these congruences in themselves could be used as tests for primality. But we intend to first return to the Lehmer sequences before we examine the testing effectiveness. Rather than restate each congruence in these special rings we only restate Congruences 3 and 4. Congruences 1 and 2 can be created from these two congruences and are somewhat more complicated.

Using the special polynomials of this section, we get the following criteria for primality.

Theorem 7.5.3. *If n is a prime, $d|(n-1)$, $\mathbb{R} = \mathbb{Z}_n[x]/(x^d - f_0)$, and*

i. if $\bar{D} = \sum_{i=0}^{d-1} \bar{D}_i x^i \in \mathbb{R}$, $D = \bar{D}^2$, *and* $D = R - 4Q$ *with* $R, Q \in \mathbb{R}$, *then*

$$\bar{D}U_n(\sqrt{R}, Q) \equiv \bar{D}_{d-1} f_0^{\frac{(n-1)(d-1)}{d}} x^{d-1} + \cdots + \bar{D}_1 f_0^{\frac{n-1}{d}} x + \bar{D}_0 \ (mod\ x^d - f_0, n).$$

ii. if $P = \sum_{i=0}^{d-1} P_i x^i \in \mathbb{R}$, $R = P^2$ *and* $Q \in \mathbb{R}$, *then*

$$V_n(P, Q) \equiv P_{d-1} f_0^{\frac{(n-1)(d-1)}{d}} x^{d-1} + \cdots + P_1 f_0^{\frac{n-1}{d}} x + P_0 \ (mod\ x^d - f_0, n).$$

Proof. Apply Theorem 7.5.1 to expand the right hand sides of Congruences 3 and 4 in Theorem 7.4.1. □

Note the special case when $d = 2$. This case will be examined in more detail in the numerical section. From the general theory, we know that Congruences 3 and 4 give roughly the same accuracy in testing for primality. Thus, we will focus on the following simplified case of the theorem above.

Corollary 7.5.4. *If n is a prime and $P, Q \in \mathbb{Z}_n[x]/(x^2 - f_0)$ with $P = P_1x + P_0$, then $V_n(P, Q) \equiv P_1(f_0|n)x + P_0 \pmod{x^2 - f_0, n}$.*

Note that this test contains the standard integer test. If $P_1 = 0$, then we get $V_n \equiv P_0 \pmod{n}$. Thus, we generally never choose $P_1 = 0$ unless we wish to revert to integer testing.

So far we have used the special form of $f(x)$ to allow for easy computation of P^n and thus simplify Congruence 4 of Theorem 7.4.1. Before we continue, we look at the conditions under which we get a more direct generalization of the Standard Lehmer Criteria. We do this by forcing D to be in the base field. As an aside, if $P = P_1x + P_0$ and $Q = Q_1x + Q_0$, then $D = P^2 - 4Q = [2P_0P_1 - 4Q_1]x + [P_1^2f_0 + P_0^2 - 4Q_0]$. Thus, the condition for D to be in the base field becomes $P_0P_1 = 2Q_1$ and we get $D = P_1^2f_0 + P_0^2 - 4Q_0$.

Theorem 7.5.5. *If n is an odd prime, $f(x) = x^2 - f_0$ and $P = P_1x + P_0$ and $Q = Q_1x + Q_0$ are in $Z_n[x]/(f(x))$ such that $D = P^2 - 4Q$ is in Z_n, then*

1. $2Q^{(1+\epsilon)/2}U_{n-\epsilon}(P, Q) \equiv [(D|n) - \epsilon(f_0|n)]P_1x + [(D|n) - \epsilon]P_0 \pmod{f(x), n}$.

2. $2Q^{(1+\epsilon)/2}V_{n-\epsilon}(P,Q) \equiv [1+(f_0|n)]P_0P_1x+[(f_0|n)P_1^2f_0+P_0^2-\epsilon(D|n)D]$ *(mod $f(x), n$).*

3. $U_n(P,Q) \equiv (D|n)$ *(mod $f(x), n$).*

4. $V_n(P,Q) \equiv P_1(f_0|n)x + P_0$ *(mod $f(x), n$).*

Proof. In Corollary 7.4.2, make the substitutions $R = P^2$ and P^n using Theorem 7.5.1. Then use $x^2 = f_0$ and collect like terms. □

Finally, we ask under what conditions does this completely reduce to the standard Lucas Criteria. The required conditions are $\epsilon = (D|n)$ and $(f_0|n) = +1$. Under these restriction we obtain:

Corollary 7.5.6. *If n is an odd prime, $f(x) = x^2 - f_0$ and $P, Q \in Z_n[x]/(f(x))$ such that $D = P^2 - 4Q \in Z_n$ and if $(f_0|n) = +1$, then*

1. $U_{n-(D|n)}(P,Q) \equiv 0$ *(mod $f(x), n$).*

2. $V_{n-(D|n)}(P,Q) \equiv 2Q^{(1-(D|n))/2}$ *(mod $f(x), n$).*

3. $U_n(P,Q) \equiv (D|n)$ *(mod $f(x), n$).*

4. $V_n(P,Q) \equiv P$ *(mod $f(x), n$).*

Proof. All of these congruences are immediate except perhaps Congruence 2. From the previous theorem, $2Q^{(1+(D|n))/2}V_{n-(D|n)}(P,Q) \equiv [1+1]P_0P_1x + [P_1^2f_0 + P_0^2 -$

$(D|n)(D|n)D]$ $(mod\ f(x), n)$. Note the conditions on D discussed before the last theorem give $2Q^{(1+(D|n))/2}V_{n-(D|n)}(P,Q) \equiv 4Q_1x{+}4Q_0$ $(mod\ f(x), n)$. Thus, $V_{n-(D|n)}(P,Q) \equiv 2Q^{(1-(D|n))/2}$ $(mod\ f(x), n)$. □

These special choices may actually make our primality test worse, but it illustrates that we are in fact building a more general theory.

7.6 Testing Sums of Binomial Coefficients

When we first introduced primality testing, we discussed the characterization of primes through binomial coefficients. In particular, n is a prime if and only if $\left(\begin{array}{c} n \\ k \end{array}\right) \equiv 0$ $(mod\ n)$ for all value of k with $1 \leq k \leq n-1$. For a large integer n, we commented earlier that these binomial coefficients could not efficiently tested directly. However, we discovered that we were able to evaluate a sum of binomial coefficients in an efficient way. With the theory of the previous sections, we will now be able to evaluate many different types of sums involving binomials coefficients and, therefore, we should expect to be able to provide better primality tests.

Let us recall how we first were able to incorporate sums into primality testing. Note in the following theorem we are not assuming that n is a prime.

Theorem 7.6.1. *If n and a are positive integers such that $(a+1)^n \equiv a+1$ $(mod\ n)$, then*

$$\sum_{k=1}^{n-1} \left(\begin{array}{c} n \\ k \end{array}\right) a^k \equiv 0\ (mod\ n).$$

Proof. Using the binomial theorem, the result follows from simplifying the congruence

$$a + 1 \equiv (a + 1)^n \equiv \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^k \ (mod\ n).$$

□

Therefore, if n is a pseudoprime for the standard Fermat test, then the equation above is satisfied. In essence, the main change that was made when we moved from Fermat based tests to Lucas sequence based test was the sums we were considering. Recall that the Lucas sequence U_n satisfies

$$2^{n-1}U_n = \sum_{i \text{ odd}} \left(\begin{array}{c} n \\ i \end{array} \right) P^{n-i} D^{(i-1)/2}.$$

If we use the Lucas sequence above, then we get a similar formula for the sum as in Theorem 7.6.1. However, now we look at a sum of half the binomial coefficients. Note that if $P = a$ and $Q = (a^2 - b)/4$, then $D = b$.

Theorem 7.6.2. *If n is an odd positive integer and a is a positive integer such that $U_n(a, (a^2 - b)/4) \equiv (b|n)\ (mod\ n)$, $2^{n-1} \equiv 1\ (mod\ n)$, and $b^{(n-1)/2} \equiv (b|n)\ (mod\ n)$, then*

$$\sum_{\substack{k odd \\ k \neq n}} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} b^{(k-1)/2} \equiv 0 \ (mod\ n).$$

Proof. The result follows immediately since

$$(b|n) \equiv U_n(a, (a^2 - b)/4) \equiv 2^{n-1}U_n \equiv b^{(n-1)/2} + \sum_{\substack{k \text{odd} \\ k \neq n}} \left(\begin{array}{c} n \\ k \end{array} \right) P^{n-k} b^{(k-1)/2} \ (mod\ n).$$

□

Experimental evidence and various theories in the literature suggest that Lucas sequences provide more accurate primality testing than the Fermat based tests. One heuristic explanation for this improvement is that the sum for Lucas sequences involve a more sparse and random sampling of the binomial coefficients.

Now with the use of specific polynomials $f(x) = x^d - a$, we can use Lucas sequences over finite rings to sample many other sums of binomial coefficients. The following theorem summaries various sums of binomial coefficients we can now access. Here we require $D = x$

Theorem 7.6.3. *If n is an odd positive integer, $d|(n-1)$ and $f(x) = x^d - b$ is irreducible in $\mathbb{Z}_n[x]$ such that $U_n(a, (a^2 - x)/4) \equiv x^{(n-1)/2}$ $(mod\ f(x), n)$ and $2^{n-1} \equiv 1$ $(mod\ n)$, then*

$$\sum_{\substack{m=0\\2dm+i<n}} \begin{pmatrix} n \\ 2dm+i \end{pmatrix} a^{n-2dm-i} b^m \equiv 0\ (mod\ n)\ \textit{for all } i \textit{ odd with } 1 \le i \le 2d-1.$$

Proof. Since $x^d \equiv b$ $(mod\ f(x), n)$, observe

$$x^{\frac{j-1}{2}} \equiv \begin{cases} b^m & ,(j-1)/2 = dm \text{ or } j = 2dm+1 \\ b^m x & ,(j-1)/2 = dm+1 \text{ or } j = 2dm+3 \\ \vdots & \qquad\vdots \\ b^m x^{d-1} & ,(j-1)/2 = dm+(d-1) \text{ or } j = 2dm+2d-1 \end{cases}$$

Notice that the power of x is simply given by j $(mod\ 2d)$. From the hypothesis we have

$$\begin{aligned} x^{(n-1)/2} &\equiv U_n(a, (a^2-x)/4) \equiv 2^{n-1} U_n(a, (a^2-x)/4) \\ &\equiv \textstyle\sum_{j \text{ odd}} \begin{pmatrix} n \\ j \end{pmatrix} a^{n-j} x^{(j-1)/2}\ (mod\ f(x), n). \end{aligned}$$

Now we reduce the powers of x in the sum and group like terms. This seems like a difficult task, but using the fact at the beginning of the proof we can simply look at odd congruence classes modulo $2d$.

$$x^{(n-1)/2} \equiv x^{(n-1)/2} + \sum_{\substack{i \text{ odd} \\ i \leq 2d-1}} x^i \sum_{\substack{m=0 \\ 2dm+i<n}} \binom{n}{2dm+i} a^{n-2dm-i} b^m \ (mod\ f(x), n).$$

Since the sum is congruent to zero and the polynomial $f(x)$ is irreducible, we conclude that each coefficient of x^i must be congruent to zero modulo n. Thus, we get the result. □

Rephrased in terms of arithmetic progressions, we obtain the following.

Corollary 7.6.4. *If n is an odd positive integer, $d|(n-1)$, and $f(x) = x^d - b$ is irreducible in $\mathbb{Z}_n[x]$ such that $U_n(a, (a^2 - x)/4) \equiv x^{(n-1)/2}$ $(mod\ f(x), n)$ and $2^{n-1} \equiv 1$ $(mod\ n)$, then*

$$\sum_{\substack{j \equiv i \ (mod\ 2d) \\ j \neq n}} \binom{n}{j} a^{n-j} b^{\frac{j-i}{2d}} \equiv 0 \ (mod\ n) \text{ for all } i \text{ odd with } 1 \leq i \leq 2d-1.$$

Thus, we have the tools to test many arithmetic sums of binomial coefficients. A prime obviously satisfies all of these tests, since the binomial coefficients are all congruence to zero except the first and last. But a composite must have other binomial coefficients that are not zero.

7.7 Numerical Results

Many different primality testing algorithms could be developed using the congruences of this chapter. In general, we are no longer in the setting of integers, so the methods of choosing parameters of Chapters 3 through 5 are no longer applicable. Thus, we face the two problems of (1) finding algorithms that most effectively use the theory of this chapter, and (2) developing appropriate methods for choosing parameters. Both of these problems will take considerable numerical work. In this section, we give explore numerical data for one specific algorithm from this chapter.

We will consider Corollary 7.5.4 for the remainder of this chapter. That is, for a given integer n, we let $f(x) = x^2 - f_0$ and $P, Q \in \mathbb{Z}_n[x]/(f(x))$ with $P = P_1x + P_0$ and we test the congruence $V_n(P, Q) \equiv P_1(f_0|n)x + P_0$. Note that we have to choose all the values f_0, P_0, P_1, Q_0, and Q_1 in $\mathbb{Z}_n$. Note that we could also choose the values for D and P or D and Q, since any two of the three parameters determines the third.

We give a brief summary of this algorithm here:

Definition 7.7.1. Quadratic Extension Lucas Testing.

For a given odd positive integer n, the algorithm proceeds as follows:

1. Choose $f_0 \in Z_n$ so that $(f_0|n)$ has the desired value.

   If $(f_0|n) = 0$ is encountered, return n is composite.

2. Choose $P_1, P_0, Q_1, Q_0, D_1,$ and D_0 such that $D_0 = P_0 + 4Q_0$ and $D_1 = P_1 + 4Q_1$.

Let $P = P_1x + P_0$, $Q = Q_1x + Q_0$, and $D = D_1x + D_0$.

3. If n satisfies $V_n(P, Q) \equiv P_1(f_0|n)x + P_0 \ (mod\ f(x), n)$, return n is a probable prime. If n not, return n is a composite.

Before this algorithm can be implemented, we need an effective way to implement Step 2 of the algorithm above. It seems natural to require that each parameter be relatively prime to n, or zero, and if this is not true, then return that n is composite. Note that this still does not give a method for choosing these parameters.

In Chapters 3-5, we choose parameters based on Jacobi symbols involving n. Fixing the same parameters for all n in the integer test seems to give less effective primality testing. However, fixing the same parameters for all n in the Quadratic Extension Lucas Test does not seem to hinder its effectiveness as we will see. Thus, we will fix a set of parameters and then we will look at the number of pseudoprimes up to $x = 10^k$.

Table 7.7.1: The number of pseudoprimes up to $x = 10^k$ for the Quadratic Extension Lucas Test with $f(x) = x^2 - 2$ and various fixed choices for P and Q.

P	Q	10^3	10^4	10^5	10^6	10^7	10^8
3	2	3	22	78	245	750	2057
$x+1$	$x+1$	3	27	203			
$x+1$	$2x+1$	0	0	0	0	0	0
$x+2$	$2x+1$	15	116	888			
$7x+5$	$2x+3$	0	0	0	0	0	5

The parameters in the first row of Table 7.7.1 are in the base field. Thus, the first row is simply Lucas primality testing. Most random choices for P and Q seem to give results as in rows three and five. That is, many fixed P and Q give zero pseudoprimes out to 10^8. This is quite remarkable since Lucas testing in the base field tests to be most effective when methods are used to dynamically choose parameters. However, the second and fourth rows raise some questions. All of the pseudoprimes in the second row are divisible by 7 and all the pseudoprimes in the fourth row are divisible by 3. The author has yet been unable to predict why this is the case.

Computations in the finite field slows down efficiency of these primality tests. However, the data shown here suggests that such testing can give extremely accurate results.

Bibliography

[1] Adams, W.W.: Characterizing Pseudoprimes for Third-Order Linear Recurrences. Math. Comp. 48, 1-15 (1987).

[2] Adams, W.W., Shanks, D.: Strong primality tests that are not sufficient. Math. Comp. 39, 255-300 (1982).

[3] Adleman, L.M., Pomerance, C., Rumely, R.S.: On distinguishing prime numbers from composite numbers. Ann. of Math. 117, 173-206 (1983).

[4] Agrawal, M., Kayal, N., Saxena, N.: PRIMES is in P. http://www.cse.iitk.ac.in/news/primality.pdf. Preprint.

[5] Alford, W.R., Granville, A., Pomerance, C.: There are infinitely many Carmichael numbers. Ann. of Math. 139, 703-722 (1994).

[6] Alford, W.R., Granville, A., Pomerance, C.: On the difficulty of finding reliable witnesses, Algorithmic Number Theory (L.M. Adleman and M.-D. Huang, eds.), Lecture Notes in Comput. Sci. 1-16, Springer-Verlag, New York (1994).

[7] Andrews, G.E.: Number Theory. Dover Publications, Inc. (1971).

[8] Arnault, F.: The Rabin-Monier Theorem for Lucas Pseudoprimes. Math. Comp. 66, 869-881 (1997).

[9] Arnault, F.: Rabin-Miller Primality Test: Composite Numbers which Pass it. Math. of Comp. 64, 335-361 (1995).

[10] Arnault, F.: Constructing Carmichael Numbers which are Strong Pseudoprimes to Several Bases. J. Symbolic Computation 20, 151-161 (1995).

[11] Arno, S.: A note on Perrin pseudoprimes. Math. Comp. 56, 371-376 (1991).

[12] Atkin, A.O.: Intelligent Primality Test Offer. Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Proceedings of a Congerence in Honor of A. O. L. Atkin 1-11, International Press, (1998).

[13] Baillie, R., Wagstaff, S.S., Jr.: Lucas pseudoprimes. Math. Comp. 35, 1391-1417 (1980).

[14] Carmichael, R.D.: The Theory of Numbers. Mathematical Monographs No. 13. John Wiley & Sons, Inc., New York (1914).

[15] Davis, K.S., Webb, W.A.: Lucas' Theorem for prime powers. European J. Combin. 11, 229-233 (1990).

[16] Dummit, D.S., Foote, R.M.: Abstract Algebra. John Wiley and Sons, Inc. (1999).

[17] Erdös, P.: On pseudoprimes and Carmichael numbers. Publ. Math. Debrecen 4, 201-206 (1956).

[18] Erdös, P., Kiss, P., Sárközy, A.: A Lower Bound for the Counting Function of Lucas Pseudoprimes. Math. Comp. 51, 315-323 (1988).

[19] Gallian, J.A.: Contemporary Abstract Algebra. Houghton Miffline Company, New York, (1998).

[20] Gordon, D.M.: Pseudoprimes on elliptic curves. Theorie des nombres (J. M. DeKoninck and C. Levesques, eds.) 290-305, de Gruyter, Berlin (1989).

[21] Gordon, D.M., Pomerance, C.: The distribution of Lucas and elliptic pseudoprimes. Math. Comp. 57, 825-838 (1991) 60, 877 (1993).

[22] Grantham, J.: Frobenius Pseudoprimes. Math. Comp. 70, 873-891 (2000).

[23] Grantham, J.: A probable Prime Test with High Confidence. J. Number Theory 72, 32-47 (1998).

[24] Grantham, J.: There are infinitely many Perrin Pseudoprimes. http://www.pseudoprime.com/pseudo3.pdf. Preprint.

[25] Granville, A.: It is easy to determine whether a given integer is prime. Bull. Amer. Math. Soc. 42, 3-38 (2005).

[26] Gurak, S. Pseudoprimes for higher-order linear recurrence sequences. Math. Comp. 55, 783-813 (1990).

[27] Hardy, G.H., Wright, E.M.: The Theory of Numbers (Fourth Edition). Oxford University Press, New York (1965).

[28] Jaeschke, G.: On strong pseudoprimes to several bases. Math. Comp. 61, 915-926 (1993).

[29] Koblitz, N.: A Course in Number Theory and Cryptography. Springer-Verlag, New York (1987).

[30] Kurtz, G.C., Shanks, D., Williams, H.C.: Fast primality tests for numbers less that $50\dot{1}0^9$. Math. Comp. 46, 691-701 (1986).

[31] Lucas, E.: Théorie des fonctions numériques simplement périodiques. Amer. J. Math. 1, 184-240 and 289-321 (1878).

[32] Lehmer, D.H.: On the converse of Fermat's theorem. Amer. Math. Monthly. 43, 347-354 (1936).

[33] Lehmer, D.H.: An Extended Theory of Lucas' Functions, Ann. of Math. 31, 419-448 (1930).

[34] Miller, G.: Riemann's hypothesis and tests for primality. J. Comput. System Sci. 13, 300-317 (1976).

[35] Monier, L. Evaluation and coparison of two efficient probabilistic primality testing algorithms, Theoretical Computer Science 12, 97-108 (1980).

[36] Morrison, M.A.: A note on primality testing using Lucas sequences. Math. Comp. 29, 181-182 (1975).

[37] Muller, S.: A Probable Prime Test with Very High Confidence for $n \equiv 3 \ (mod\, n)$. J. Cryptology 16, 117-139 (2003).

[38] Muller, S.: Some remarks on primality testing based on Lucas functions. In Number Theory for the Millennium 3, 1-22 (2001).

[39] Muller, S.: On the rank of appearance and the number of zeros of the Lucas sequences over $\mathbb{F}_q$. In Finite Fields and Applications, 390-408. Springer-Verlag, Berlin (2001).

[40] Muller, S.: On probable prime testing and the computation of square roots mod n. In Algorithmic Number Theory (Leiden, 2001), 423-437. Springer-Verlag, Berlin (2001).

[41] Muller, S.: On the combined Fermat/Lucas probable prime test. In Cryptography and Coding, 222-235. Springer-Verlag, Berlin (1999).

[42] Muller, S.: A Note on Strong Dickson Psuedoprimes. Applicable Algebra In Engineering, Communications, and Computing. 247-264. Springer-Verlag (1998).

[43] Muller, S.: On strong Lucas pseudoprimes. In Contributins to General Algebra, 10 (Klagenfurt, 1997), 237-249. Heyn, Klagenfurt, (1998).

[44] Pinch, R.G.E.: The Carmichael numbers up to 10^{15}. Math. Comp. 61, 381-391 (1993).

[45] Pomerance, C.: A new lower bound for the pseudoprime counting function. Illinois J. Math. 26, 4-9 (1982).

[46] Pomerance, C.: On the Distribution of Pseudoprimes. Math. Comp. 37, 587-593 (1981).

[47] Pomerance, C., Selfridge, J.L., Wagstaff, S.S.,Jr.: The pseudoprimes up to $25 \cdot 10^9$. Math. Comp. 39, 1003-1025 (1980).

[48] Rabin, M.O.: Probabilistic Algorithm for Testing Primality. J. Number Theory 12, 128-138 (1980).

[49] Ribenhoim, P.: The Book of Prime Number Records. Berlin: Springer (1988).

[50] Robinson, R. M.: The converse of Fermat's theorem, Amer. Math. Monthly 64, 703-710 (1957).

[51] Rotkiewicz, A.: On strong Lehmer pseudoprimes in the case of negative discriminant in arithmetic progressions. Acta Arith. 68, 145-151 (1994).

[52] Rotkiewicz. A.: On Euler Lehmer pseudoprimes and Strong Lehmer pseudoprimes with parameters L, Q in arithmetic progressions. Mathh. Comp. 39, 239-247. (1982).

[53] Rotkiewicz. A.: On the pseudoprimes of the form ax+b with respect to the sequence of Lehmer, Bull. Acad. Polon. Sci. Sr. Sci. Math. Astronom. Phys. 20, 349-354 (1972).

[54] Rotkiewicz, A., Wasén, R.: Lehmer Numbers, Acta Arith. 36, 203-217 (1980).

[55] Szekeres, G.: Higher order pseudoprimes in primality testing. Combinatoric. Paul Erdos is eighty, Bolyai Soc. Math. Stud. 2, 1996, 451-458, Janos Bolyai Math Soc., Budapest (1996).

[56] Wagstaff, S.S., Jr.: Cryptanalysis of Number Theoretic Ciphers. Chapman & Hall/CRC (2003).

[57] Williams, H.C.: Edouard Lucas and Primality Testing. volume 22 of Canadian Mathematics Society Series of Monographs and Advanced Texts. John Wiley & Sons, New York, (1998).

[58] Williams, H.C.: On numbers analogous to the Carmichael numbers. Canad. Math. Bull. 20, 133-143 (1977).

[59] Williams,H.C., Judd, J.S. Some algorithms for prime testing using generalized Lehmer functions, Math. Comp. 30, 867-886 (1976).