Independence of the Miller-Rabin and Lucas Probable Prime Tests

Alec Leng

Mentor: David Corwin

March 30, 2017

Abstract

In the modern age, public-key cryptography has become a vital component for secure online communication. To implement these cryptosystems, rapid primality testing is necessary in order to generate keys. In particular, probabilistic tests are used for their speed, despite the potential for pseudoprimes. So, we examine the commonly used Miller-Rabin and Lucas tests, showing that numbers with many nonwitnesses are usually Carmichael or Lucas-Carmichael numbers in a specific form. We then use these categorizations, through a generalization of Korselt's criterion, to prove that there are no numbers with many nonwitnesses for both tests, affirming the two tests' relative independence. As Carmichael and Lucas-Carmichael numbers are in general more difficult for the two tests to deal with, we next search for numbers which are both Carmichael and Lucas-Carmichael numbers, experimentally finding none less than 10^{16}. We thus conjecture that there are no such composites and, using multivariate calculus with symmetric polynomials, begin developing techniques to prove this.

1 Introduction

In the current information age, cryptographic systems to protect data have become a fundamental necessity. With the quantity of data distributed over the internet, the importance of encryption for protecting individual privacy has greatly risen. Indeed, according to [EMC16], cryptography is allows for authentication and protection in online commerce, even when working with vital financial information (e.g. in online banking and shopping). Now that more and more transactions are done through the internet, rather than in person, the importance of secure encryption schemes is only growing.

Thus, as some commonly used public key cryptography algorithms rely on large semiprimes that are extremely difficult to factor, fast prime generation is vital for key generation. For example, the RSA cryptosystem is one of the most widely used systems for cryptography—even when not used directly, its often used to encrypt the keys for other cryptographic algorithms ([CSE11]). To implement it, RSA requires semiprimes that are around 2048 bits (about 600 decimal digits) for its key ([EMC16]). These semiprimes are the product of two primes, so one needs to quickly generate primes that are around 1048 bits (around 300 decimal digits). If we have a way to quickly determine if a number is prime, we can quickly generate the necessary primes by choosing "candidate" numbers in the right size, until we find one that is prime.

1.1 Primality Tests

Methods for determining whether or not a number n is prime are simply called primality tests. There are two distinct types of primality tests. On one hand, *deterministic* tests always decide for certain whether or not n is prime. On the other hand, *probabilistic* tests determine either that n is composite, or that it might be prime. This is done by checking whether or not n satisfies some properties which are true of all primes and few composites. While these probabilistic tests do not always correctly determine if a number is prime, they are generally far faster than deterministic tests. Indeed, when compared with the fast (in the sense that it runs in polynomial-time), deterministic, Agrawal-Kayal-Saxena (AKS) primality test, effective probabilistic primality tests are still millions of times faster [AKS04]. Thus, probabilistic primality tests remain very relevant. Indeed, even when attempting to prove that a number is prime, probabilistic tests can be rapidly applied to quickly exclude most composite numbers, reducing the overall time the primality test takes.

1.2 The Fermat Primality Test

The Fermat test is constructed from Fermat's Little Theorem, which says that for a prime p, and any a relatively prime to p, we have $a^{p-1} \equiv 1 \pmod{p}$. So, to turn this into a primality test, given an odd number n, we choose some positive integer $a < n$ that is relatively prime to n and see if $a^{n-1} \equiv 1 \pmod{n}$. If the congruence holds, then n might be prime. However, if the congruence does not hold, then we know n is a composite, and we call a a *witness* for n's compositeness. Similarly, if n is actually composite, and the congruence holds for some a, then we call that a a *nonwitness*, and n a *Fermat pseudoprime*. However, the Fermat Primality test itself is not particularly useful; there are some n for which every a is a nonwitness. These numbers are called *Carmichael numbers*, and they will play a vital role when looking at pseudoprimes to the Miller-Rabin test.

1.3 The Miller-Rabin Primality Test

In the Miller-Rabin test, we express our odd integer n as $n = 1 + d \cdot 2^k$, for d an odd integer. Then, as with the Fermat test, we choose a positive integer $a < n$, relatively prime to n, as a potential witness. However, with the Miller-Rabin test, we check that either $a^d \equiv 1 \pmod{n}$, or $a^{2^r \cdot d} \equiv -1 \pmod{n}$ for some $r < k$. If one of these conditions hold, then n is a probable prime. If n is actually composite, then we say that it is a *strong pseudoprime*, and that a is a nonwitness. Likewise, if neither of the conditions hold, then a is a witness to n and n is known to be composite. As this paper will not examine the Fermat test, "witness" and "nonwitness," when used to describe an integer a, will be used to mean a "witness" or "nonwitness" for the Miller-Rabin test. For a given n, we will use $N(n)$ to denote the number of Miller-Rabin nonwitnesses to n. We will focus on this test, and the Lucas Probable Prime test which we now introduce.

1.4 The Lucas Probable Prime Test

To construct the weak Lucas test, we first define the Lucas Sequences U and V, when given two integers P and Q, by $U_0 = 0,\ U_1 = 1,\ U_{k+2} = PU_{k+1} - QU_k$, and $V_0 = 2,\ V_1 = P,\ V_{k+2} = PV_{k+1} - QV_k$. Then, let $D = P^2 - 4Q$, and let $\varepsilon(n)$ denote the Jacobi symbol $\left(\frac{D}{n}\right)$. We have the following as a well-known theorem:

Theorem. *[Arn97] Let p be a prime number, relatively prime to 2QD. Set* $p - \varepsilon(p) = 2^k q$ *for q an odd integer. Then,* $p | U_{2^k q}$.

Note that this condition can be viewed as analogous to the condition for the Fermat test. So, just like with the Fermat test, there is a stronger form of the statement; if p is prime, then one of the following conditions is satisfied: $p|U_q$ or there exists some i, $0 \leq i < k$, where $p|V_{2^i q}$.

Let $\mathscr{O}$ be the ring of algebraic integers in $\mathbb{Q}(\sqrt{D})$. Then, [Arn97] shows that each Lucas sequence is in a one-to-one correspondence with the norm-1 elements τ in $\mathscr{O}$ where $\tau - 1$ is a unit in $\mathscr{O}/n$. Furthermore, [Arn97] also shows that for a given Lucas sequence, if n is relatively prime to $2QD$, then $n|U_k \iff \tau^k \equiv 1 \pmod{n}$ and $n|V_k \iff \tau^k \equiv -1 \pmod{n}$. In light of these equivalences, we will often study the Lucas test with algebraic integers, not with Lucas sequences.

Now, we can turn the Lucas condition into a primality test, starting with some n relatively prime to 2QD and setting $n - \varepsilon(n) = 2^k q$ for q odd. If, for a composite n, either $n|U_q$ or there is some i, $0 \leq i < k$, where $p|V_{2^i q}$, then we call n a *strong Lucas pseudoprime*, since it satisfies the strong form of the Lucas test, and the pair of parameters (P,Q) (or the corresponding quadratic integer τ), a nonwitness.

We will now introduce some notation that is useful when talking about Lucas pseudoprimes. Suppose $n > 2$ factors into primes as $n = p_1^{e_1} \cdots p_m^{e_m}$. Let ε_i denote $\varepsilon(p_i)$. Then, for $1 \leq i \leq m$, let $p_i - \varepsilon_i = 2^{k_i} q_i$ for q_i odd. Finally, let $SL(D,n)$ denote the number of nonwitnesses, analogous to $N(n)$ for Miller-Rabin nonwitnesses.

The Lucas test, when used correctly, can be highly independent of the Miller Rabin test, making it particularly interesting. Indeed, several algorithms exploit this independence to yield extremely powerful primality tests; of particular note is the Baillie-PSW test, for which there are no known composite n which are "probably prime."

1.5 This Research

In Section 2, we begin by examining prior results about numbers with many nonwitnesses for both the Miller-Rabin and Lucas Pseudoprime tests. We define our concept of "Lucas-Carmichael numbers" as an analog of the Carmichael numbers, but for the Lucas Probable Prime test, and give a categorization of numbers with many nonwitnesses for both the Miller-Rabin and Lucas tests in terms of Carmichael and Lucas-Carmichael numbers. In order to prove that no numbers have many nonwitnesses for both tests, we prove that if a composite has three prime factors, then it cannot be a Carmichael number and a Lucas-Carmichael number. Then, in Section 3, we begin to generalize this result to show that there are no composites that are both Carmichael and Lucas-Carmichael numbers, developing

lemmas and techniques before applying them to a particular form of numbers with five prime factors to show that there are no numbers in that form that are both Carmichael and Lucas-Carmichael numbers. We conclude in Section 4 by considering possible future work.

2 Finding Composites with Many Nonwitnesses

2.1 Prior Results

In the case of the Miller-Rabin test, we have the below classification for the numbers with high amounts of nonwitnesses, where $\varphi(n)$ denotes the Euler totient function, and $v_2(n)$ is the greatest natural number so that $2^{v_2(n)}|n$. $v_2(n)$ is also known as the 2-adic valuation.

Theorem 1. *[Nar14] Suppose n is an odd composite number* ≥ 81. *Then* $N(n) = \frac{\varphi(n)}{4}$ *iff n is of the form* $(2k+1)(4k+1)$, *for k odd and* $2k+1$, $4k+1$ *prime, or n is a Carmichael number of the form pqr, where p,q, and r are distinct primes* $\equiv 3 \pmod 4$. *Furthermore,* $\frac{\varphi(n)}{6} < N(n) < \frac{\varphi(n)}{4}$ *iff n is of the form* $(2k+1)(6k+1)$, *for k odd and* $2k+1$, $6k+1$ *prime, and* $N(n) = \frac{\varphi(n)}{6}$ *iff n has the form* $(2k+1)(4k+1)$ *where k is even. Finally,* $\frac{\varphi(n)}{7} < N(n) < \frac{5\varphi(n)}{32}$ *iff n is a Carmichael number of the form pqr, where* $v_2(p-1) = v_2(q-1) = v_2(r-1) > 1$. *Otherwise,* $N(n) \leq \frac{\varphi(n)}{8}$.

[Ami15] provides a similar theorem for the Lucas test.

Theorem 2. *[Ami15]* $SL(D,n) \leq \frac{n}{6}$ *unless* $n = 9$ *or* 25, $m = 2$ *and either* $n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$, *where n is the product of twin primes, or* $n = (2^{k_1}q_1 + \varepsilon_1)(2^{k_1+1}q_1 + \varepsilon_2)$, *or* $m = 3$, *and* $n = (2^{k_1}q_1 + \varepsilon_1)(2^{k_1}q_2 + \varepsilon_2)(2^{k_1}q_3 + \varepsilon_3)$, *where* $q_1, q_2, q_3 | q$.

2.2 Carmichael and Lucas-Carmichael Numbers

In Theorem 1, several of the cases are Carmichael numbers. So, we state a well-known theorem about Carmichael numbers that will allow us to talk about them more easily:

Theorem 3 (Korselt's Criterion)**.** *A positive composite number n is a Carmichael number if and only if it is square-free, and for all its prime factors* p_i, $p_i - 1 | n - 1$ *[Con].*

Now, just like how Carmichael numbers completely defeat the weaker form of the Miller-Rabin test (the Fermat test), we consider the numbers that completely defeat the weak Lucas test:

Definition 1 (Lucas-Carmichael Number)**.** *A Lucas-Carmichael number for a given value of D is a composite number n, relatively prime to 2D, such that for every Lucas sequence (P,Q), $n|U_{n-\varepsilon(n)}$. Equivalently, for every τ that is a norm-1 element in $\mathscr{O}$ where $\tau-1$ is a unit in $\mathscr{O}/n$, $\tau^{n-\varepsilon(n)} \equiv 1 \pmod{n}$. (A norm-1 element is the image of some $x \in \mathscr{O}$ under the canonical map $\phi : \mathscr{O} \mapsto \mathscr{O}/n$, where $Norm(x) \equiv 1$. We will denote the multiplicative group of such elements by $(\mathscr{O}/n)^{\wedge}$.)*

We are then able to devise an analog of Korselt's Criterion for these Lucas-Carmichael numbers, proving our theorem by working with quadratic integers.

Theorem 4. *A positive composite number n, relatively prime to 2D, is a Lucas-Carmichael number (with respect to D) if and only if it is square-free, and for every prime $p_i|n$, $p_i - \varepsilon(p_i)|n-\varepsilon(n)$.*

Proof. We first prove that if n is a Lucas-Carmichael number, then it is square free, and for every prime $p_i|n$, $p_i-\varepsilon(p_i)|n-\varepsilon(n)$.

Suppose n factors as $p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m}$. Consider the multiplicative group of norm-1 elements in $(\mathscr{O}/p_i^{e_i})$. Arnault shows that this group is cyclic, with order $p_i^{e_i-1}(p_i-\varepsilon(p_i))$. [Arn97] So suppose some g_i is a generator. Then, by the Chinese Remainder Theorem, there is some norm-1 $g \in \mathscr{O}$ with $g \equiv g_i \pmod{p_i^{e_i}}$ for all i. Now, we claim $g-1$ must be invertible in $\mathscr{O}$—for the sake of contradiction, suppose otherwise.

If $D \not\equiv 1 \pmod 4$, then $\mathscr{O} = \mathbb{Z}[\sqrt{D}]$, so we can express $g = a+b\sqrt{D}$. Then, we know $N(g) = N(a+b\sqrt{D}) = a^2-Db^2 = 1$. Note that $N(g-1) = N(a-1+b\sqrt{D}) = (a-1)^2 - Db^2 = a^2-Db^2-2a+1 = N(g)-2a+1 = 2-2a$. If this is relatively prime to n in $\mathbb{Z}$, then $N(g-1)$ is invertible, which would imply that $g-1$ is invertible in $\mathscr{O}$. So there is some $p_i|n$ with $p_i|N(g-1)$. Then $2 \equiv 2a \pmod{p_i}$. We assumed that n was relatively prime to $2D$, so $p_i \neq 2$. So $a \equiv 1 \pmod{p_i}$. Now, $N(g) = a^2-Db^2 = 1$, so $a^2 \equiv 1+Db^2 \pmod{p_i}$, taking the canonical mapping from $\mathbb{Z}$ to $\mathbb{Z}/p_i$. Then, as $a \equiv 1 \pmod{p_i}$, $a^2 \equiv 1 \pmod{p_i}$, so $Db^2 \equiv 0 \pmod{p_i}$. So $p_i|D$ or $p_i|b$. But $p_i|n$, and we assumed that n was relatively prime to $2D$. So $p_i|b$. Therefore in $\mathscr{O}/p_i$, $g \equiv 1 \pmod{p_i}$.

Alternatively, if $D \equiv 1 \pmod 4$, then $\mathscr{O} = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, and we can write $g = a+b\frac{1+\sqrt{D}}{2}$. Substitute $A = 2a+b, B = b$, so that $g = \frac{A+B\sqrt{D}}{2}$. Then, $1 = N(g) = N(\frac{A+B\sqrt{D}}{2}) = \frac{A^2-DB^2}{4}$. Also, $N(g-1) = N(\frac{A-2+B\sqrt{D}}{2}) = \frac{(A-2)^2-DB^2}{4} = N(g)-A+1 = 2-A$. If this is relatively prime to n, then it is invertible, which would make $g-1$ invertible. So as before, there is some $p_i|n$ with $N(g-1) = 2-A \equiv 0 \pmod{p_i}$. Then as $p_i \neq 2$, $\frac{A}{2} \equiv 1 \pmod{p_i}$. So $\frac{A^2}{4} \equiv 1 \pmod{p_i}$. Then, as $1 = N(g) = \frac{A^2-DB^2}{4}$, $DB^2 \equiv 0 \pmod{p_i}$. Thus, as before, we

get that $p_i|B$, as D and n are relatively prime. So, in $\mathscr{O}/p_i$, $g \equiv 1 \pmod{p}$, regardless of the choice of D.

Now, g is a generator of $(\mathscr{O}/{p_i}^{e_i})$. But there are only $p_i^{e_i-1} < p_i^{e_i-1}(p_i - \varepsilon(p_i))$ elements in $\mathscr{O}/{p_i}^{e_i}$ which are congruent to $1 \pmod{p_i}$, so g cannot generate the whole group. Thus, $g-1$ is invertible in $\mathscr{O}$.

But then g is a norm-1 element in $\mathscr{O}$ where $g-1$ is invertible. So by our initial assumption, $g^{n-\varepsilon(n)} \equiv 1 \pmod{n}$. So certainly, for any p_i, $g^{n-\varepsilon(n)} \equiv 1 \pmod{p_i^{e_i}}$. So, as the order of g is $p_i^{e_i-1}(p_i - \varepsilon(p_i))$, as it is congruent to some g_i that is a generator, $p_i^{e_i-1}(p_i - \varepsilon(p_i))|n - \varepsilon(n)$. But as $p_i^{e_i}|n$, $p_i^{e_i}$ is relatively prime to $n - \varepsilon(n)$. So, we must have that $e_i = 1$. So n is square-free. Then, plugging in $e_i = 1$, we have that for any $p_i|n$, $p_i - \varepsilon(p_i)|n - \varepsilon(n)$, as desired.

Conversely, suppose that we can factor n into distinct primes $n = p_1 p_2 \cdots p_m$ where, for all p_i, $p_i - \varepsilon(p_i)|n - \varepsilon(n)$. Then, for any $\tau \in \mathscr{O}$ with norm 1, $\tau \in \mathscr{O}/{p_i}^{\wedge}$. So, as the order of $\mathscr{O}/{p_i}^{\wedge}$ is $p_i - \varepsilon(p_i)$, $\tau^{p_i-\varepsilon(p_i)} \equiv 1 \pmod{p_i}$. So, as $p_i - \varepsilon(p_i)|n - \varepsilon(n)$, $\tau^{n-\varepsilon(n)} \equiv 1 \pmod{p_i}$. So, by the Chinese Remainder Theorem, $\tau^{n-\varepsilon(n)} \equiv 1 \pmod{n}$, as desired. □

The following two lemmas will allow us to restate Theorem 2.

Lemma. *For n with two prime factors, n is a Lucas-Carmichael number if and only if it is the product of twin primes, $p, p+2$, where $\varepsilon(p) = -1, \varepsilon(p+2) = 1$.*

Proof. Suppose n is a Lucas-Carmichael number with two prime factors. Using the previously defined notation, $n = 2^k q + \varepsilon(n) = (2^{k_1} q_1 + \varepsilon_1)(2^{k_2} q_2 + \varepsilon_2)$. Multiplying out, $n = (2^{k_1+k_2} q_1 q_2 + 2^{k_2} q_2 \varepsilon_1 + 2^{k_1} q_1 \varepsilon_2) + \varepsilon_1 \varepsilon_2$. Note that $\varepsilon(n) = \varepsilon_1 \varepsilon_2$. Now, suppose without loss of generality that $k_1 \leq k_2$. n is a Lucas-Carmichael number, so $2^{k_2} q_2 | n - \varepsilon = (2^{k_1+k_2} q_1 q_2 + 2^{k_2} q_2 \varepsilon_1 + 2^{k_1} q_1 \varepsilon_2)$. So, $2^{k_2} | 2^{k_1} q_1 \varepsilon_2)$. But q_1 is odd, so it is relatively prime to 2_{k_2}. So $2^{k_2} | 2^{k_1}$. Thus, $k_2 \leq k_1$. But we assumed $k_1 \leq k_2$. So $k_1 = k_2$. Furthermore, from $2^{k_2} q_2 | n - \varepsilon = (2^{k_1+k_2} q_1 q_2 + 2^{k_2} q_2 \varepsilon_1 + 2^{k_1} q_1 \varepsilon_2)$, we get that $q_2 | 2^{k_1} q_1 \varepsilon_2$. So as q_2 is odd, $q_2 | q_1$. One can similarly show that $q_1 | q_2$. So, $q_1 = q_2$. Then, $n = (2^{k_1} q_1 + \varepsilon_1)(2^{k_1} q_1 + \varepsilon_2)$. $\varepsilon_1 \neq \varepsilon_2$, or the two factors would be the same, contradicting that n is square-free. So, assume without loss of generality that $\varepsilon_1 = -1$, $\varepsilon_2 = 1$. Now, setting $p = 2^{k_1} q_1 + \varepsilon_1 = 2^{k_1} q_1 - 1$, we see that we have factored n into the product of twin primes, $p \cdot (p+2)$, where $\varepsilon(p) = \varepsilon_1 = -1$ and $\varepsilon(p+2) = \varepsilon_2 = 1$, as desired.

Conversely, suppose $n = p(p+2)$ where $\varepsilon(p) = -1, \varepsilon(p+2) = 1$. Then $\varepsilon(n) = -1$, so $n - \varepsilon(n) = n + 1 = p(p+2) + 1 = p^2 + 2p + 1 = (p+1)^2$. Note that $p - \varepsilon(p) = p + 2 - \varepsilon(p+2) = p + 1$. So, $p - \varepsilon(p), p + 2 - \varepsilon(p+2)$ both divide $n - \varepsilon(n)$. So, as n is clearly square-free, it is a Lucas-Carmichael number. □

Lemma. *For n with three prime factors, if and only if n factors as $(2^{k_1}q_1+\varepsilon_1)(2^{k_1}q_2+\varepsilon_2)(2^{k_1}q_3+\varepsilon_3)$, where $q_1,q_2,q_3|q$, then n is a Lucas-Carmichael number with $v_2(p_1-\varepsilon_1)=v_2(p_2-\varepsilon_2)=v_2(p_3-\varepsilon_3)$.*

Proof. Clearly, if n factors in that way, then as the q_i are odd, $v_2(p_1-\varepsilon_1)=v_2(p_2-\varepsilon_2)=v_2(p_3-\varepsilon_3)$. Now, we can multiply out the expression for n to get $n=2^{3\cdot k_1}q_1q_2q_3+2^{2\cdot k_1}q_2q_3\varepsilon_1+2^{2\cdot k_1}q_1q_3\varepsilon_2+2^{2\cdot k_1}q_1q_2\varepsilon_3+2^{k_1}q_1\varepsilon_2\varepsilon_3+2^{k_1}q_2\varepsilon_1\varepsilon_3+2^{k_1}q_3\varepsilon_1\varepsilon_2+\varepsilon_1\varepsilon_2\varepsilon_3$. So then, $2^{k_1}|n-\varepsilon$, as $\varepsilon=\varepsilon_1\varepsilon_2\varepsilon_3$. So, as $n-\varepsilon=2^kq$, $2^{k_1}|n-\varepsilon$, and q is odd, $2_{k_1}|2^k$. So as $q_i|q$, $2_{k_1}|2^k$, and 2_{k_1} and q_i are relatively prime, since the q_i are odd, $p_i-\varepsilon_i=2_{k_1}q_i|2^kq=n-\varepsilon$. So n is a Lucas-Carmichael number with $v_2(p_1-\varepsilon_1)=v_2(p_2-\varepsilon_2)=v_2(p_3-\varepsilon_3)$.

Conversely, suppose n is a Lucas-Carmichael number with $v_2(p_1-\varepsilon_1)=v_2(p_2-\varepsilon_2)=v_2(p_3-\varepsilon_3)$. Certainly, without loss of generality, we can factor $n=(2^{k_1}q_1+\varepsilon_1)(2^{k_2}q_2+\varepsilon_2)(2^{k_3}q_3+\varepsilon_3)$. Then, the 2-adic valuations are equal, so we must have $k_1=k_2=k_3$. Finally, $p_i-\varepsilon_i|n-\varepsilon$, so $2^{k_i}q_i|2^kq$. But q_i is relatively prime to 2^k, so $q_i|q$. So $n=(2^{k_1}q_1+\varepsilon_1)(2^{k_1}q_2+\varepsilon_2)(2^{k_1}q_3+\varepsilon_3)$, where $q_1,q_2,q_3|q$. □

We then restate Theorem 2:

Theorem 5 (Restatemenet of Result by [Ami15])**.** *$SL(D,n)\leq\dfrac{n}{6}$ unless $n=9$ or 25, $m=2$ and either n is a Lucas-Carmichael number or $n=(2^{k_1}q_1+\varepsilon_1)(2^{k_1+1}q_1+\varepsilon_2)$, or $m=3$, and n is a Lucas-Carmichael number where $v_2(p_1-\varepsilon_1)=v_2(p_2-\varepsilon_2)=v_2(p_3-\varepsilon_3)$.*

2.3 Properties of Problematic Composites

We now want to examine numbers that have $N(n)>\dfrac{\varphi(n)}{8}$ and $SL(D,n)>\dfrac{n}{6}$; call such n *problematic*. Assume that $n>81$, since when testing for primality, we would check that no small primes divide into the number, taking care of these smaller cases. Now, according to Theorem 1 and Theorem 2, problematic numbers can only have two or three prime factors. The case for two prime factors can be easily dealt with, so we will do that now.

Lemma 1. *Suppose we choose a D such that $\left(\dfrac{D}{n}\right)=-1$. Then there are no problematic numbers n that have two prime factors.*

Proof. By Theorem 1, we know that if $N(n)>\dfrac{\varphi(n)}{8}$, and $n>81$ has two prime factors, then $n=(2k+1)(4k+1)$ for some integer k, or $n=(2k+1)(6k+1)$ for some odd k. By Theorem 2, we also know that either n is the product of twin primes, or $n=(2^{k_1}q_1+\varepsilon_1)(2^{k_1+1}q_1+\varepsilon_2)$. Now, clearly, if $n=(2k+1)(4k+1)$ or $(2k+1)(6k+1)$, the prime

factors of n differ by more than 2. So $n = (2^{k_1}q_1 + \varepsilon_1)(2^{k_1+1}q_1 + \varepsilon_2)$. Now, $\left(\frac{D}{n}\right) = -1$, so either $\varepsilon_1 = -1, \varepsilon_2 = 1$ or $\varepsilon_1 = 1, \varepsilon_2 = -1$.

In the former case, $n = (2^{k_1}q_1 - 1)(2^{k_1+1}q_1 + 1)$. Clearly the latter factor is larger. So if $n = (2k+1)(6k+1)$ for some odd k, then $6k+1 = 2^{k_1+1}q_1 + 1$. If $6k+1 = 2^{k_1+1}q_1 + 1$ though, then as k is odd, $v_2(2^{k_1+1}q_1) = v_2(6k) = 1$. Then $k_1 = 0$. But then the smaller prime factor of n is $2^{k_1}q_1 - 1 = q_1 - 1$. But q_1 is odd, so $2^{k_1}q_1 - 1 = q_1 - 1$ is even. But it also has form $2k+1$ for some k. Alternatively, if $n = (2k+1)(4k+1)$ for some k, then $4k = 2^{k_1+1}q_1$, $2k+1 = 2^{k_1}q_1 - 1$. So, as q_1 is odd, $v_2(k) = k_1 - 1$. Then, $v_2(2k) = k_1$. But note that $2k+2 = 2^{k_1}q_1$, so $v_2(2k+2) = k_1$. However, $2k, 2k+2$ are both odd, so one of them is $2 \pmod 4$ and one of them is $0 \pmod 4$— they certainly cannot have equal 2-adic valuations.

In the latter case, $n = (2^{k_1}q_1 + 1)(2^{k_1+1}q_1 - 1)$. Suppose that $n = (2k+1)(6k+1)$, for k odd. We still have that the first factors are both the smaller ones, so $6k+1 = 2^{k_1+1}q_1 - 1$, $2k+1 = 2^{k_1}q_1 + 1$. Then $2k = 2^{k_1}q_1$, so as k is odd, $k_1 = 1, k = q_1$. So $6q_1 + 1 = 6k+1 = 2^{k_1+1}q_1 - 1 = 4q_1 - 1$. So $q_1 = 1$. Then $n = 3 \cdot 7$, and we certainly have $n < 81$, so n is not problematic. Finally, suppose that $n = (2k+1)(4k+1)$. Then, $4k+1 = 2^{k_1+1}q_1 - 1$, $2k+1 = 2^{k_1}q_1 + 1$. So $v_2(2k) = k_1$. Then $v_2(4k) = k_1 + 1$. But $4k+2 = 2^{k_1+1}q_1$, so $v_2(4k+2) = k_1 + 1$. □

So, we look only at the case where n has three prime factors. In this case, it has a large number of Miller-Rabin nonwitnesses, so it must be a Carmichael number with $v_2(p_1 - 1) = v_2(p_2 - 1) = v_2(p_3 - 1)$. Furthermore, since it has a large number of Lucas nonwitnesses it is a Lucas-Carmichael number, with $v_2(p_1 - \varepsilon_1) = v_2(p_2 - \varepsilon_2) = v_2(p_3 - \varepsilon_3)$. Using some of these characteristics, we prove the following lemma.

Lemma. *If n has three distinct prime factors, where $p_i = 2^{k_1}q_i + \varepsilon_i$ (so $v_2(p_1 - \varepsilon_1) = v_2(p_2 - \varepsilon_2) = v_2(p_3 - \varepsilon_3)$), and $v_2(p_1 - 1) = v_2(p_2 - 1) = v_2(p_3 - 1)$, then $\left(\frac{D}{n}\right) = \left(\frac{D}{p_i}\right)$ for $1 \le i \le 3$, where $\left(\frac{a}{b}\right)$ denotes the Jacobi symbol.*

Proof. Suppose without loss of generality that for two of our prime factors, p_1 and p_2, $\left(\frac{D}{p_1}\right) \neq \left(\frac{D}{p_2}\right)$, where $\left(\frac{D}{p_1}\right) = 1, \left(\frac{D}{p_2}\right) = -1$. Then, $p_1 - 1 = 2^{k_1}q_1$, so $v_2(p_1) = k_1$. Meanwhile, $p_2 = 2^{k_1}q_2 - 1$, so $p_2 - 1 = 2^{k_1}q_2 - 2$. But as $v_2(p_1 - 1) = v_2(p_2 - 1)$, we thus get that $v_2(2^{k_1}q_2 - 2) = k_1$. So, in particular, $2^{k_1} | 2^{k_1}q_2 - 2$. So $2^{k_1} | 2$. So $k_1 = 1$. But then, $p_2 - 1 = 2q_2 - 2 = 2(q_2 - 1)$. But since q_2 is odd, $2 | (q_2 - 1)$, so $v_2(p_2) \neq k$. So, for any two prime factors, $\left(\frac{D}{p_i}\right) = \left(\frac{D}{p_j}\right)$. But we know that $\left(\frac{D}{n}\right) = \left(\frac{D}{p_1}\right)\left(\frac{D}{p_2}\right)\left(\frac{D}{p_3}\right)$, by

the properties of the Jacobi symbol. So, $\left(\frac{D}{n}\right) = \left(\frac{D}{p_1}\right)^3 = \left(\frac{D}{p_1}\right)$, as desired. □

The following corollary is immediate.

Corollary 1. *All problematic numbers with three prime factors satisfy* $\left(\frac{D}{n}\right) = \left(\frac{D}{p_i}\right)$.

So, we only have two different cases to consider— when $\left(\frac{D}{n}\right) = 1$ and when $\left(\frac{D}{n}\right) = -1$. However, note that in general, we are able to chose the value of $\left(\frac{D}{n}\right)$ based on our choice of D. In fact, we want to choose $\left(\frac{D}{n}\right) = -1$; if $\left(\frac{D}{n}\right) = 1$, then we have more problematic numbers, since the constraints on n are not all independent.

Lemma. *If n is a Carmichael number with three prime factors, and* $v_2(p_1-1) = v_2(p_2-1) = v_2(p_3-1)$, $v_2(p_1-\varepsilon_1) = v_2(p_2-\varepsilon_2) = v_2(p_3-\varepsilon_3)$, *and* $\left(\frac{D}{n}\right) = 1$, *then n is a Lucas-Carmichael number.*

Proof. By Corollary 1, we have that $\left(\frac{D}{p_i}\right) = \left(\frac{D}{n}\right) = 1$ for all p_i. Now, we earlier set $n-\varepsilon = 2^k q$, where $\varepsilon = \left(\frac{D}{n}\right) = 1$. So, as ε_i is just $\left(\frac{D}{p_i}\right)$, and $p_i - 1 | n-1$, by Korselt's Criterion (since n is a Carmichael number), we have $2^{k_1} q_i | 2^k q$. So $q_i | 2^k q$. But as q_i is odd, it is relatively prime to 2^k. So $q_i | q$ for all i. Then as $v_2(p_1-\varepsilon_1) = v_2(p_2-\varepsilon_2) = v_2(p_3-\varepsilon_3)$, by our earlier lemma, n is a Lucas-Carmichael number. □

Indeed, [BW00] also notes that want $\left(\frac{D}{n}\right) = -1$, or the Miller-Rabin and Lucas tests are not as independent, though their justification is different. They show how if $\left(\frac{D}{n}\right) = 1$, and n is a strong pseudoprime to some as for the Miller-Rabin test, then n must be a pseudoprime to certain pairs (P,Q) as well. So, we now assume all are Lucas tests are performed where $\left(\frac{D}{n}\right) = -1$, and when searching for problematic numbers with three prime factors, we only look at n where $\left(\frac{D}{n}\right) = \left(\frac{D}{p_i}\right) = -1$.

2.4 Results of Searching

We began by testing the Carmichael numbers less than 2^{30} which have three prime factors such that $v_2(p_1-1) = v_2(p_2-1) = v_2(p_3-1)$. In this search, no problematic numbers were found. Indeed, we present the following result:

Theorem. *There are no problematic numbers.*

To prove this, we first show the following lemmas

Lemma. *If* $\left(\frac{D}{n}\right) = -1$*, and n is both a Carmichael number and a Lucas-Carmichael number, then* $\left(\frac{D}{p_i}\right) = -1$ *for every prime* $p_i|n$*.*

Proof. Suppose otherwise— that for some p_i, $\left(\frac{D}{p_i}\right) = 1$. Then, $p_i - \varepsilon_i | n - \varepsilon$, where $\varepsilon = -1$, $\varepsilon_i = 1$, so $p_i - 1 | n + 1$. But n is also a Carmichael number, so $p_i - 1 | n - 1$. Then, $p_i - 1 | 2$. So as p_i is a prime, $p_i = 3$.

Then, $\left(\frac{D}{n}\right) = -1$, so there is some prime $p_j | n$ where $\varepsilon_j = -1$. Then $p_j - 1 | n - 1$, $p_j + 1 | n + 1$ But $p_j \not\equiv 1 \pmod 3$, or $3 | p_j - 1$, implying that $3 | n - 1$, and similarly, $p_j \not\equiv 2 \pmod 3$, or $3 | p_j + 1$, so $3 | n + 1$— these two are impossible, since $3 | n$. But also, $p_j \not\equiv 3$, unless $p_j = 3$, contradicting its distinctness. So, there is no p_i with $\varepsilon i = 1$. Thus, for every $p_i | n$, $\varepsilon_i = \left(\frac{D}{p_i}\right) = -1$, as desired. □

Corollary. *If* $\left(\frac{D}{n}\right) = -1$*, then there are no numbers with an even number of prime factors that are both Carmichael numbers and Lucas-Carmichael numbers.*

Proof. Suppose n has k prime factors. Then, $-1 = \left(\frac{D}{n}\right) = (-1)^k$ by Lemma 2.4. So k must be odd. □

Lemma. *If n is both a Carmichael and a Lucas-Carmichael number, then for every prime* $p|n$*,* $n \equiv p \pmod{\frac{p^2-1}{2}}$.

Proof. As $p|n$, we can write $n = ap$ for some integer a. Then, $p - 1 | n - 1$ by Korselt's Criterion, so $p - 1 | ap - 1 = ap - a + a - 1 = a(p-1) + a - 1$. So $p - 1 | a - 1$. Meanwhile, from our last lemma, $\left(\frac{D}{p}\right) = -1$, so from the analog of Korselt's Criterion for Lucas-Carmichael numbers, we get $p + 1 | n + 1$. Then, $n + 1 = ap + 1 = ap + a - a + 1 = a(p + 1) - a + 1$, so $p + 1 | -a + 1$, or $p + 1 | a - 1$. Now, consider $\gcd(p-1, p+1)$. Certainly, this is either 2 or 1— as p is an odd prime though, $2 | p - 1$, $2 | p + 1$. So $\gcd(p-1, p+1) = 2$. Now, we know $p^2 - 1 = (p+1)(p-1) = \operatorname{lcm}(p+1, p-1) \cdot \gcd(p+1, p-1) = 2 \cdot \operatorname{lcm}(p+1, p-1)$. So $\operatorname{lcm}(p+1, p-1) = \frac{p^2-1}{2}$. Then, as $p - 1 | a - 1$, $p + 1 | a - 1$, we have $\operatorname{lcm}(p+1, p-1) | a - 1$. So $\frac{p^2-1}{2} | a - 1$, or equivalently, $a \equiv 1 \pmod{\frac{p^2-1}{2}}$.

Then, p is certainly relatively prime to $\frac{p^2-1}{2}$, so we can multiply by p to get $n = ap \equiv p \pmod{\frac{p^2-1}{2}}$, as desired. □

Theorem 6. *There are no composites with three prime factors that are both Carmichael Numbers and Lucas-Carmichael numbers.*

Proof. Let $n = pqr$ be a Lucas-Carmichael number, and a Carmichael number. Then, without loss of generality, suppose $p < q < r$. From our previous lemma, we get that $pq \equiv 1 \pmod{\frac{r^2-1}{2}}$. So, $pq = 1 + x \cdot \frac{r^2-1}{2}$, for some integer x. Now, if $x \geq 2$, then we get $pq \geq r^2$, contradicting that $p < q < r$. Furthermore, we clearly know that $x \not\leq 0$. So, $x = 1$, and $pq = 1 + \frac{r^2-1}{2}$. Note that $1 + \frac{r^2-1}{2} = \frac{r^2+1}{2}$. So $r^2 + 1 = 2pq$. In particular, $r < \sqrt{2pq}$.

Note that $3 < q$. So, $9(3-2\sqrt{2}) < q^2(3-2\sqrt{2})$. In particular, $1 < 9(3-2\sqrt{2})$. Then $1 < q^2(3-2\sqrt{2}) = 3q^2 - 2\sqrt{2}q^2$. So, $2\sqrt{2}q^2 - 2 < 3q^2 - 3$. As the right hand side is positive, $\frac{2(\sqrt{2}q^2-1)}{q^2-1} < 3$, and as $p < q$, $p\sqrt{2pq} < \sqrt{2}q^2$. Since $r < \sqrt{2pq}$, $\frac{2(pr-1)}{q^2-1} < 3$. Then $\frac{pr-1}{(\frac{q^2-1}{2})} < 3$.

By lemma 7, $pqr \equiv q \pmod{\frac{q^2-1}{2}}$. So $\frac{q^2-1}{2} | pr - 1$. Then, $\frac{pr-1}{(\frac{q^2-1}{2})}$ is an integer, so it must be 1 or 2. But if $\frac{pr-1}{(\frac{q^2-1}{2})} = 2$, then $pr = q^2$, a contradiction. So $\frac{pr-1}{(\frac{q^2-1}{2})} = 1$. Note that $1 = \frac{pq-1}{(\frac{r^2-1}{2})} < \frac{pr-1}{(\frac{q^2-1}{2})} = 1$. □

After showing the above, we became aware of an equivalent result by [Wil77], using an alternative proof.

Theorem 7. *There are no problematic numbers.*

Proof. Follows immediately from Lemma 1 and Theorem 6, since problematic numbers with three prime factors must be both Carmichael numbers and Lucas-Carmichael numbers. □

3 Numbers that are Carmichael and Lucas-Carmichael

In general, Carmichael and Lucas-Carmichael numbers tend to have many nonwitnesses for the Miller-Rabin and Lucas Probable Prime tests. Indeed, this fact is evident from the

formulas for the number of nonwitnesses stated in [Arn97]. Thus, numbers that are both Carmichael and Lucas-Carmichael become of interest.

3.1 Searching for Carmichael and Lucas-Carmichael Numbers

In showing there were no problematic numbers, we were able to prove that there were no numbers with either an even number of prime factors, or three prime factors, that were both Carmichael and Lucas-Carmichael. So, one might expect that there are, in general, no numbers that are both Carmichael and Lucas-Carmichael numbers. Indeed, after examining all Carmichael numbers less than 10^{16}, we found no Lucas-Carmichael numbers ([Pin]). However, despite having already shown several lemmas about numbers that are both Carmichael and Lucas-Carmichael numbers, trying to generalize the result to other odd numbers of factors proves much more difficult.

The following lemma provides a useful starting point:

Lemma. *If n is both a Carmichael number and a Lucas-Carmichael number, then all primes dividing n are equivalent mod* 12*.*

Proof. Clearly, n must have multiple prime factors. If $2|n$, there is another odd prime $p|n$, so $n-1$ is odd, but divisible by an even number. Similarly, if $3|n$, but there is either another odd prime $p|n, p \equiv 1 \pmod 3$, in which case $p-1|n-1 \implies 3|n-1$, or there is an odd prime $p|n, p \equiv 2 \pmod 3$, so as $p+1|n+1$ since n is a Lucas-Carmichael number, $3|n+1$. Either way, we reach a contradiction. So, $\gcd(n,6) = 1$.

Furthermore, we cannot have $p,q|n$, $p \equiv 1 \pmod 4, q \equiv 3 \pmod 4$— $p-1|n-1$, so $4|n-1$, but $q+1|n+1$, so $4|n+1$, a contradiction. Similarly, we cannot have $p,q|n$, $p \equiv 1 \pmod 3, q \equiv 2 \pmod 3$ as $p-1|n-1 \implies 3|n-1$, and $q+1|n+1 \implies 3|n+1$. So, as any prime dividing n must be $\equiv 1,3 \pmod 4$, and $\equiv 1,2 \pmod 3$, we get that all primes dividing n are equivalent mod 12 from the Chinese Remainder Theorem. □

Now, if n is both a Carmichael and a Lucas-Carmichael number, when $\left(\frac{D}{n}\right) = -1$, then we have that $\operatorname{lcm}(p_1-1,\ldots,p_m-1)|n-1$ and $\operatorname{lcm}(p_1+1,\ldots,p_m+1)|n+1$. Furthermore, by definition

$$\operatorname{lcm}(p_1-1,\ldots,p_m-1)|(p_1-1)\cdots(p_m-1)$$

and

$$\operatorname{lcm}(p_1+1,\ldots,p_m+1)|(p_1+1)\cdots(p_m+1).$$

So both

$$\frac{(p_1-1)\cdots(p_m-1)}{\operatorname{lcm}(p_1-1,\ldots,p_m-1)} \text{ and } \frac{(p_1+1)\cdots(p_m+1)}{\operatorname{lcm}(p_1+1,\ldots,p_m+1)}$$

are integers—these numbers measure of much "overlap" there is between the different p_i-1s and p_i+1s respectively. The smaller these numbers are, the "stronger" the conditions $\operatorname{lcm}(p_1-1,\ldots,p_m-1)|n-1$ and $\operatorname{lcm}(p_1+1,\ldots,p_m+1)|n+1$ are, as more primes are required to divide $n-1$ or $n+1$.

3.2 Beginning to Generalize

We start developing techniques to generalize the results of Theorem 6 by examining the case where n has five prime factors, $n \equiv 11 \mod 12$ (by lemma 8, these two conditions imply that for every prime $p|n$, $p \equiv 11 \mod 12$), and $\frac{(p_1-1)\cdots(p_5-1)}{\operatorname{lcm}(p_1-1,\ldots,p_5-1)} = 16$. The last condition comes from the fact that 2^4 is the minimum possible value for the ratio—as $p_i \equiv 11 \mod 12$, 2 divides p_i-1 exactly once for all p_i, so 2 divides the numerator five times and the denominator once. So, the ratio must be a (positive integer) multiple of $2^4 = 16$.

In the special case we are looking at, we thus have that $\frac{(p_1-1)\cdots(p_5-1)}{16}|n-1$. So without loss of generality, there is some integer r such that $\frac{(p_1-1)\cdots(p_5-1)}{16}(16+r) = n-1$. As $(p_1-1)\cdots(p_5-1) < n-1$, r must even be positive. Now let $s_{a,b}$ denote the ath elementary symmetric polynomial in b variables. (For example, $s_{1,b}(x_1,\ldots,x_b) = \sum_{1\le i\le b} x_i$, $s_{2,b}(x_1,\ldots,x_b) = \sum_{1\le i<j\le b} x_i x_j$, and $s_{b,b} = x_1\cdots x_b$.) Then we can express $(p_1-1)\cdots(p_5-1)$ as $s_{5,5}-s_{4,5}+s_{3,5}-s_{2,5}+s_{1,5}-1$, and $n-1$ as $s_{5,5}-1$, where the argument for each of the symmetric functions is (p_1,p_2,p_3,p_4,p_5). So, substituting into $\frac{(p_1-1)\cdots(p_5-1)}{16}(16+r) = n-1$ and rearranging, we have have that $r(s_{5,5}-s_{4,5}+s_{3,5}-s_{2,5}+s_{1,5}-1)-16(s_{4,5}-s_{3,5}+s_{2,5}-s_{1,5}) = 0$. This motivates defining the function $f_r(x_1,x_2,x_3,x_4,x_5) = r(s_{5,5}-s_{4,5}+s_{3,5}-s_{2,5}+s_{1,5}-1)-16(s_{4,5}-s_{3,5}+s_{2,5}-s_{1,5})$ where here, each of the elementary symmetric polynomials has (x_1,x_2,x_3,x_4,x_5) as its argument. We can now employ calculus to show that f_r has no positive integer roots where for all i, $p_i \equiv 11 \mod 12$, thus showing that there are no numbers that are both Carmichael and Lucas-Carmichael with the specific properties mentioned earlier.

Lemma. *Consider a point in $\mathbb{R}^5$ given by $\boldsymbol{q} = (q_1,q_2,q_3,q_4,q_5)$, where $q_1 < q_2 < q_3 < q_4 < q_5$. Then if $f, \frac{\partial f_r}{\partial x_5}, \frac{\partial^2 f_r}{\partial x_4 \partial x_5}, \frac{\partial^3 f_r}{\partial x_3 \partial x_4 \partial x_5}, \frac{\partial^4 f_r}{\partial x_2 \partial x_3 \partial x_4 \partial x_5}$ are all positive at $\boldsymbol{q}$, then at*

any point $(q_1', q_2', q_3', q_4', q_5')$ where for all i, $q_i < q_i'$, f is also positive.

Proof. It is a well known fact that, for $a, b > 0$, $\dfrac{\partial s_{a,b}}{\partial x_b} = s_{a-1,b-1}$, where $s_{0,b} = 1$ for any b. Repeatably applying this rule with the linearity of the derivative, we get that $\dfrac{\partial^5 f_r}{\partial x_1 \partial x_2 \partial x_3 \partial x_4 \partial x_5} = r$. In particular, this function is always positive. Now, $\dfrac{\partial^4 f_r}{\partial x_2 \partial x_3 \partial x_4 \partial x_5}$ is only a function of x_1, so if its positive at q_1, then its positive at any $y_1 > q_1$ since its derivative is always positive. So $\dfrac{\partial^3 f_r}{\partial x_3 \partial x_4 \partial x_5}$ is positive at any pair (y_1, y_2) if there is a permutation π with $q_1 < y_{\pi(1)}, q_2 < y_{\pi(2)}$, since permuting the order of the arguments does not change the value of the function (as the function is a polynomial in terms of elementary symmetric polynomials and is thus symmetric), and the derivative is positive for the relevant values. Repeating this process, we find that when choosing any point $(y_1, y_2, y_3, y_4, y_5) \in \mathbb{R}^5$, where some permutation π of the y_is has $q_i < y_{\pi(i)}$, f is positive at that point. □

Using the lemma, we then verify the required conditions at $(63, 75, 87, 99, 111)$ for any positive integer r (one can easily show that increasing r only increases the function). So, as the five prime factors in a Carmichael number that is also a Lucas-Carmichael number must be unique, and differ by at least 12, we can rule out any numbers whose least prime factor is greater than 63, since f_r on the five prime factors cannot be 0. Now, since we are only looking at the case that is $11 \mod 12$, note that the smallest prime factor must then either be $11, 23, 47$, or 59. Checking around $(25, 37, 49, 61, 73)$, for $r \geq 2$, we find that the lemma is applicable. So for 47 and 59, if f_r has a root, we must have $r = 1$. Now, for 59, check that the lemma is applicable at $(59, 83, 107, 119, 131)$, so for any possible set of five primes, f_1 is too large if the second smallest prime is not 71. Then use $(59, 71, 107, 119, 131)$ to force the third smallest prime to be 83. Then use $(59, 71, 83, 119, 131)$ to force there to be 107. Finally its easy to check that for any prime greater than 119, f_1 has no zero. But we can explicitly check $f_1(59, 71, 83, 107, 119)$ to see that it is not 0. So there is no composite satisfying the required properties with least factor 59. One can use a similar series of tests to show that there are no numbers with the desired properties with least prime factor of $11, 23$, or 47, with the caveat that for 11 and 23, one first shows that f_r is negative if $r \leq 2, 1$ respectively, and always positive if $r \geq 4, 3$ respectively. Thus, there are no $n \equiv 11 \mod 12$, where $\dfrac{(p_1 - 1) \cdots (p_5 - 1)}{\operatorname{lcm}(p_1 - 1, \ldots, p_5 - 1)} = 16$, which are both Carmichael and Lucas-Carmichael numbers.

4 Future Plans

Now that we have begun to develop techniques for showing the nonexistence of composites that are both Carmichael and Lucas-Carmichael numbers, these techniques could be generalized to show that there are no numbers that are both Carmichael and Lucas-Carmichael numbers. In particular, we conjecture that there is an explicit bound for the two ratios $\frac{(p_1-1)\cdots(p_m-1)}{\text{lcm}(p_1-1,\ldots,p_m-1)}$ and $\frac{(p_1+1)\cdots(p_m+1)}{\text{lcm}(p_1+1,\ldots,p_m+1)}$, and are currently working to find such a bound. Then, this would enable us to use a more general form of the techniques from Section 3 to show that there cannot be numbers that are both Carmichael and Lucas-Carmichael numbers in general. Furthermore, the Baillie-PSW test is a well known probabilistic primality test that derives its strength from the independence of the Miller-Rabin and Lucas tests. However, as there are no known composites that pass the test, there is not much insight into how to effectively turn it into a deterministic test (unfortunately, heuristics suggest that some composites do pass the test). Our results could be used to develop a modified form of the Baillie-PSW algorithm where the composites that pass the test are easily characterized, opening the way for a faster provably deterministic primality testing algorithm. After all, the Miller-Rabin and Lucas Probable Prime tests are far faster than the current fastest deterministic tests.

5 Acknowledgements

We would foremost like to thank the PRIMES program and faculty for making this research possible, particularly Program Director Dr. Slava Gerovitch, Chief Research Adviser Professor Pavel Etingof, and head mentor Dr. Tanya Khovanova. We also would like to express our utmost gratitude to our mentor, David Corwin, for guiding us through the research process. In addition, we recognize Stefan Wehmeir, from Mathworks, for suggesting the project.

References

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Ann. of Math. (2)*, 160(2):782–793, 2004.

[Ami15] David Amirault. Better Bounds on the Rate of Non-Witnesses of Lucas Pseudoprimes. 2015. http://math.mit.edu/research/highschool/primes/materials/2015/Amirault.pdf.

[Arn97] F. Arnault. The Rabin-Monier theorem for Lucas pseudoprimes. *Math. Comp.*, 66(218):869–881, 1997.

[BW00] David Bressoud and Stan Wagon. *A course in computational number theory.* Key College Publishing, Emeryville, CA; in cooperation with Springer-Verlag, New York, 2000.

[Con] Keith Conrad. Carmichael Numbers and Korselt's Criterion. http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/carmichaelkorselt.pdf.

[CSE11] How can I use asymmetric encryption, such as RSA, to encrypt an arbitrary length of plaintext?, 2011. Accessed September 2016. http://crypto.stackexchange.com/questions/14/how-can-i-use-asymmetric-encryption-such-as-rsa-to-encrypt-an-arbitrary-length.

[EMC16] Dell EMC. Public-Key Cryptography Standards, 2016. Accessed September 2016. http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm.

[Nar14] Shyam Narayanan. Improving the Speed and Accuracy of the Miller-Rabin Primality Test. 2014. http://math.mit.edu/research/highschool/primes/materials/2014/Narayanan.pdf.

[Pin] Richard G.E. Pinch. Tables relating to Carmichael numbers. Accessed July 2016. http://www.s369624816.websitehome.co.uk/rgep/cartable.html.

[Wil77] H. C. Williams. On numbers analogous to the Carmichael numbers. *Canad. Math. Bull.*, 20(1):133–143, 1977.