On Carmichael numbers with three distinct prime factors

A thesis presented to the faculty of
San Francisco State University
In partial fulfillment of
The requirements for
The degree

Master of Arts
In
Mathematics

by

James Phillips

San Francisco, California

May 2011

CERTIFICATION OF APPROVAL

I certify that I have read *On Carmichael numbers with three distinct prime factors* by James Phillips and that in my opinion this work meets the criteria for approving a thesis submitted in partial fulfillment of the requirements for the degree: Master of Arts in Mathematics at San Francisco State University.

Neville Robbins
Professor of Mathematics

Eric Hayashi
Professor of Mathematics

Samuel Wagstaff
Professor of Computer Science, Purdue University

On Carmichael numbers with three distinct prime factors

James Phillips
San Francisco State University
2011

A Carmichael number is a composite number, n, such that $b^{n-1} \equiv 1 (\text{mod } n)$ for all integers b such that $\gcd(b, n) = 1$. A Carmichael number may also be called an *absolute pseudoprime*. Such numbers are of interest in computational number theory. It has been known since 1994 that there exist infinitely many Carmichael numbers. (See [1]). However, little has been established concerning Carmichael numbers with a fixed or limited number of distinct prime factors. Let a Carmichael number with exactly k prime factors be called a $k-$Carmichael number. A recent conjecture of Granville and Pomerance implies the existence of infinitely many $k-$Carmichael numbers for each $k \geq 3$. (See [7].) We are able to prove that (i) of the 78497 odd primes below 10^6, all but 543 of them are the least prime factor of a 3-Carmichael number; (ii) 53 of these exceptional primes are the second or third prime factor of a 3-Carmichael number, or the least prime factor of a 4-Carmichael number. Thus all but possibly 490 of the primes below 10^6 occur as factors of Carmichael numbers.

I certify that the Abstract is a correct representation of the content of this thesis.

Chair, Thesis Committee Date

ACKNOWLEDGMENTS

I would like to thank Dr. Robbins for giving me a problem to work on and helping me work on it. I would like to thank Dr. Wagstaff for offering suggestions which led to several of the observations in this thesis. I would like to thank Dr. Hayashi and Dr. Arsuaga for offering suggestions and comments. I would like to thank Will Galway for sending me a version of the algorithm used to find the 4-Carmichael numbers in Table 3.1. Finally, I would like to thank Kit Fitzpatrick for helping me rewrite some of the algorithms into different programming languages and I would like to thank Heather for her support.

TABLE OF CONTENTS

LIST OF TABLES

Chapter 1

Introduction

Before talking about Carmichael numbers, we will examine prime numbers and then we will understand why Carmichael numbers are interesting. Let's consider a transaction with an online marketplace such as amazon.com. Most people have probably used amazon.com in the past, and have had to use a credit card to do so. For most people this is no concern at all. You just click on the "add credit card information" button, enter your credit card number, expiration date, and card security code and then click on the "submit" button. You certainly wouldn't trust a stranger with this information, so why would you enter this information online and submit it through the internet, when there are billions of people with internet access? It turns out we can trust organizations such as amazon.com because their data security systems are based on the RSA algorithm, which relies on properties of prime numbers. In particular, breaking a code requires the factorization of a composite number that is

the product of two large primes, which is not computationally feasible. The RSA algorithm requires the availability of large primes (100-digits and upwards). The contrapositive of Fermat's Little Theorem is an excellent test for compositeness: If b is an integer such that $\gcd(b, n) = 1$ and b^{n-1} is not congruent to $1 (\mathrm{mod}\ n)$, then n is composite. It would be nice if the converse of Fermat's Little Theorem provided a test for primality. This converse would say: If n is a large odd integer and there is an integer b such that $\gcd(b, n) = 1$ and $b^{n-1} \equiv 1 (\mathrm{mod}\ n)$, then n is prime. However, this statement is false, as shown by the example $n = 341 = 11 \cdot 31$ and $b = 2$. But the statement is true for most large odd n and most b. Given b, the composite integers n for which the statement holds are called *pseudoprimes to the base b*. It is known that, for each b, pseudoprimes to the base b are rarer than primes. One might hope that if the statement holds for fixed n and several b, then one could be more confident that n is prime. But this hope is dashed by the existence of *Carmichael numbers*, which are pseudoprimes to every base b with $\gcd(n, b) = 1$. This ability of Carmichael numbers to masquerade as primes makes them an interesting object of study.

1.1 Definitions

Throughout this thesis, we will use the well known facts that a Carmichael number must be odd, square-free, and have at least 3 distinct prime factors. We will also use Korselt's Criterion, which we give below.

Korselt's Criterion: The positive, composite integer n is called a Carmichael number if and only if n is square-free, and for all primes p such that p divides n, it is also true that $p-1$ divides $n-1$.

These properties of Carmichael numbers can be found in many papers, such as [11] and [8]. The following definitions will also be useful:

Definition 1.1. A *k-Carmichael number* is a Carmichael number with exactly k distinct prime factors, where $k \geq 3$.

Definition 1.2. If x is a positive real number, let $C(x)$ denote the number of Carmichael numbers below x.

1.2 A Brief History of Carmichael Numbers

The first person to write about what we now call Carmichael numbers was Korselt, who defined them in a paper he wrote in 1899 (See [10]). Although he wrote about these numbers, he was unable to actually give an example of one. In fact, Robert Carmichael was the first person to discover a Carmichael number (which is why they are called Carmichael numbers) and wrote about them in a paper in 1912 (See [2]). In 1939, Chernick discovered what he called *universal forms*, which are terms in arithmetic progressions, whose products are Carmichael numbers provided that each factor is a prime. The simplest example of a universal form is $(6n+1)(12n+1)(18n+1)$, which gives the Carmichael number $561 = 7 \cdot 13 \cdot 19$ when $n = 1$ (See

[3]). It was suspected that there were infinitely many Carmichael numbers, but this was not easy to prove. In 1956, Erdős found an upper bound for $C(x)$ and conjectured that a lower bound for $C(x)$ implies that $C(x) \to \infty$ as $x \to \infty$ (See [5]). It was finally proved in 1994 by Alford, Granville, and Pomerance, that there are infinitely many Carmichael numbers (See [1]). Although numerous papers have been written concerning Carmichael numbers, few researchers have obtained results concerning Carmichael numbers with a fixed or limited number of prime factors. The theorem of Alford, Granville and Pomerance does not prove that there are infinitely many k-Carmichael numbers for any particular k. In fact, most of the literature on Carmichael numbers is concerned with finding all of the Carmichael numbers up to a given bound, or finding very large Carmichael numbers. Our approach differs from past research in that we are only concerned with $k-$Carmichael numbers whose prime factors are lower than a given bound.

1.3 Extending the Research of Carmichael Numbers

In this thesis, we make several observations concerning the prime factors of $k-$Carmichael numbers where $k = 3$ or 4. Using several algorithms (listed below), we have created tables that list 3-Carmichael numbers as well as their prime factors: p_1, p_2, p_3 where $p_1 < p_2 < p_3$ and $p_1 < 10^6$. When examining these tables we notice the absence of certain primes. We then examine these primes and make several conjectures concerning Carmichael numbers in Chapter 4. Finally, we examine the

3-Carmichael numbers found in the context of a more recent paper by Granville and Pomerance [7].

One reason why we focus on the *least* prime factors and on Carmichael numbers having only 3 or 4 prime factors is that reasonable algorithms exist for finding these numbers, but there are no fast algorithms for studying the perhaps more natural question of the prime factors of arbitrary Carmichael numbers.

Chapter 2

3-Carmichael Numbers

As previously mentioned, most papers about Carmichael numbers don't explore the different factors of Carmichael numbers. However, it has been mentioned in several papers such as [9], that the number 11 can *never* be the least factor of a 3-Carmichael number. How many primes share this property with 11? In this thesis we answer this question for all odd prime numbers $p < 10^6$. To do this we need a way to find all of the 3-Carmichael numbers such that each factor is less than 1 million. Thankfully, Pinch has already come up with an algorithm in [11] which is of much use to solve this problem. In this algorithm, you input a prime, p_1, and the algorithm outputs every 3-Carmichael number of the form $p_1 \cdot p_2 \cdot p_3$ where $p_1 < p_2 < p_3$. Furthermore, because of the relationship $p_1 < p_2 < p_3$, we are guaranteed that we will find all of the primes p_2 and p_3 under 10^6 which are factors of 3-Carmichael numbers. It should be mentioned that this method is not necessarily

the fastest way to solve our problem, but it does provide *all* of the 3-Carmichael numbers with $p_1, p_2, p_3 < 10^6$. This is helpful when we examine our newly-found Carmichael numbers to determine which are primitive and which are imprimitive, as suggested in [7]. (Primitive Carmichael numbers are defined in Section 3.3 below.) We also had enough computational resources and time to proceed with this method (See Appendix A).

2.1 The Least Factor of 3-Carmichael Numbers

To find the primes which are not the least factor of a 3-Carmichael number we first used Pinch's algorithm mentioned above to generate a list of 3-Carmichael numbers such that the first factor, p_1, is less than 10^6. After we obtained this list of 3-Carmichael numbers, it was easy to write an algorithm in Matlab to compare our list of p_1's with a list of all of the primes p up to 10^6, and have this algorithm output a list of primes p, such that p is not the least factor of a 3-Carmichael number. We call such primes *exceptional*. Our list contains 543 primes, and is given below.

Table 2.1: Prime Numbers up to One Million which are not the Least Factor of a 3-Carmichael Number

11, 197, 1223, 1487, 4007, 4547, 7823, 9833, 9839, 10259, 11483, 11807, 11909, 13259, 13967, 14207, 15629, 15803, 16139, 16889, 18287, 19583, 22367, 23039, 23879, 24359, 25349, 29339, 30707, 32027, 33343, 34883, 36929, 38747, 39113, 39119, 42787, 43223, 44207, 46829, 47189, 48779, 49003, 49019, 49157, 53093, 56267, 56909, 57119, 58043, 59399, 61463, 61547, 63377, 63737, 64019, 65867, 66467, 68219, 70019, 71411, 73847, 75743, 75767, 78137, 78809, 78839, 79279, 84977, 86579, 90527, 92899, 93059, 93287, 93719, 94463, 95561, 97103, 97883, 97967, 99377, 100847, 101429, 102077, 103919, 104207, 108287, 109199, 111533, 112403, 113453, 115553, 117959, 119039, 120677, 121379, 122099, 122399, 122579, 123269, 123983, 127691, 128923, 132527, 136139, 139739, 144569, 146057, 147347, 147377, 148139, 150533, 151303, 152519, 153191, 153563, 154619, 156683, 157877, 160967, 162119, 162263, 167249, 167267, 169019, 170603, 171947, 172829, 174299, 175277, 178187, 180023, 181283, 183479, 184727, 184967, 185267, 186119, 186653, 187463, 191123, 191783, 192923, 193577, 195863, 197837, 199247, 205817, 205823, 206627, 211067, 212117, 212867, 212903, 213791, 216803, 220931, 221069, 221087, 221603, 222107, 225749, 227993, 228479, 228847, 229819, 231131, 231719, 232007, 232049, 233939, 235043, 240743, 242927, 247607, 253469, 254699, 256889, 260543, 260747, 263573, 264179, 266129, 266177, 267959, 268733, 269783, 270563, 270797, 271367, 273359, 274739, 275987, 277331, 279143, 282389, 283079, 284759, 284783, 285119, 285343, 287159, 287219, 288683, 289607, 290327, 290399, 294023, 295079, 295283, 295439, 297683, 297989, 299723, 300719, 307253, 309503, 311447, 312979, 315223, 316067, 316469, 320339, 321017, 323467, 323903, 325883, 328883, 336109, 336829, 336863, 341333, 342299, 345707, 346187, 347987, 349199, 349379, 349499, 350699, 353687, 353939, 356999, 359147, 360023, 361799, 364607, 365699, 365759, 365903, 377717, 379439, 381323, 386017, 391247, 397799, 399263, 400859, 401057, 402947, 405143, 408263, 411119, 411947, 414539, 416147, 419303, 420149, 422627, 424433, 425387, 427283, 428579, 429719, 430819, 432527, 438203, 438983, 440159, 440333,

440339, 440807, 441011, 442979, 442997, 443117, 443879, 443999, 445307, 446477, 448139, 448387, 449963, 450803, 456167, 462653, 463247, 463889, 463993, 467123, 468239, 470243, 470399, 470579, 473723, 475379, 477727, 478169, 478483, 480527, 483167, 484259, 486323, 489743, 490493, 492083, 492893, 495017, 497719, 499067, 499211, 500693, 500699, 508727, 515477, 516359, 517373, 520067, 522059, 522659, 526139, 526759, 526937, 527159, 532307, 534707, 539447, 539663, 539993, 546067, 547663, 549587, 550763, 551963, 553667, 556883, 558287, 562361, 564407, 565259, 566639, 566723, 569927, 571199, 571679, 573317, 579053, 580079, 580163, 589409, 595313, 598127, 599003, 604613, 605167, 606539, 607319, 607703, 612719, 614543, 616997, 617429, 619007, 622613, 626009, 630719, 631487, 633599, 637163, 641387, 643403, 647099, 647477, 649379, 651803, 660503, 660659, 663539, 664667, 665207, 667699, 669359, 670487, 672059, 672227, 673019, 673567, 675539, 675827, 676733, 679607, 681449, 681839, 682511, 684599, 684869, 688379, 688999, 691037, 691709, 694367, 695099, 695327, 695687, 699383, 702503, 703643, 703673, 706403, 708479, 708839, 709433, 709799, 711839, 713477, 713747, 713939, 714947, 715739, 715889, 717719, 718007, 730727, 732959, 733277, 735419, 736469, 737327, 739337, 739829, 742619, 744539, 745727, 753707, 755333, 759359, 759959, 762479, 766439, 767279, 767633, 773447, 778847, 779159, 779699, 779707, 784583, 785459, 793439, 794579, 795239, 798179, 798737, 799223, 799739, 803669, 809903, 811919, 819899, 820559, 823997, 828833, 829457, 831323, 831583, 831707, 836387, 836663, 837059, 838043, 838667, 841889, 844553, 852959, 855419, 855719, 855983, 856139, 863867, 864803, 865247, 865577, 869039, 869879, 870679, 872129, 872393, 877043, 882263, 882863, 885967, 898439, 901547, 902963, 904067, 904907, 905683, 911663, 913637, 915947, 916583, 918539, 919883, 921959, 922463, 923591, 928883, 929627, 931067, 936407, 938573, 940259, 940727, 946997, 947783, 948749, 950927, 951943, 954539, 954719, 956357, 958487, 962789, 963659, 973283, 974063, 975599, 978749, 981263, 982211, 984167, 992723, 992843

Table 2.1: Prime Numbers up to One Million which are not the Least Factor of a 3-Carmichael Number

2.2 The Second and Third Factor of 3-Carmichael Numbers

We already saw that there are 543 odd primes, $p < 10^6$, such that p is not the least factor of a 3-Carmichael number. The first such prime p is 11, which occurs as the *second* prime factor of the 3-Carmichael number $561 = 3 \cdot 11 \cdot 17$. So now it seems natural to ask the following question: Of the 78497 odd primes, $p < 10^6$, which of these are not the second or third factor of a 3-Carmichael number? To do this, we wrote an algorithm which examined the list of 3-Carmichael numbers obtained from Pinch's algorithm, and output lists of primes which were not the second or third factor of a 3-Carmichael number. Before we give the data obtained from this algorithm, we should note that since 11 is the least prime which occurs as a second factor of any 3-Carmichael number, we do not count any primes below 11 as a possible second factor for a 3-Carmichael number. That is, we do not include any primes less than 11 in the list of primes which are not the second factor of a 3-Carmichael number. Likewise, 17 is the least prime which occurs as a third factor of any 3-Carmichael number, so we do not count any primes lower than 17 as a possible third factor for a 3-Carmichael number.

2.3 The Data Obtained

Of the 78497 odd primes, $p < 10^6$, there are 543 primes (about 0.69% of primes) which are not the first factor of a 3-Carmichael number, 51104 primes (about 65%

of primes) which are not the second factor of a 3-Carmichael number, and 70479 (about 90% of primes) primes which are not the third factor of a 3-Carmichael number. And of the 543 primes which are not the first factor of a 3-Carmichael number, 500 of them are not the second factor of a 3-Carmichael number as well, and 535 of them are not the third factor of a 3-Carmichael number. Furthermore, there are 48678 primes which are not the second or third factor of a 3-Carmichael number. Finally, there are 495 primes (about 0.63% of primes) which do not occur as *any* of the factors of a 3-Carmichael number. These 495 primes are given below in Table 2.2

Table 2.2: Prime numbers up to one million which are not any factor of a 3-Carmichael number

1223, 1487, 4007, 4547, 7823, 9839, 10259, 11483, 11807, 11909, 13259, 13967, 14207, 15629, 15803, 16139, 16889, 18287, 19583, 23039, 23879, 24359, 25349, 29339, 30707, 32027, 34883, 36929, 38747, 39113, 39119, 42787, 43223, 44207, 46829, 47189, 49003, 49019, 49157, 53093, 56267, 56909, 57119, 58043, 59399, 61463, 61547, 63377, 64019, 65867, 66467, 68219, 70019, 73847, 75743, 75767, 78137, 78839, 79279, 84977, 86579, 90527, 93287, 93719, 94463, 95561, 97883, 97967, 99377, 100847, 101429, 103919, 104207, 108287, 109199, 111533, 112403, 117959, 119039, 120677, 121379, 122099, 122399, 122579, 123269, 123983, 127691, 128923, 136139, 139739, 144569, 146057, 147347, 147377, 148139, 150533, 151303, 152519, 153191, 153563, 154619, 156683, 157877, 160967, 162119, 162263, 167249, 167267, 169019, 170603, 171947, 172829, 174299, 175277, 178187, 180023, 181283, 183479, 184727, 184967, 185267, 186119, 186653, 187463, 191123, 191783, 192923, 193577, 195863, 197837, 199247, 205817, 205823, 211067, 212117, 212867, 212903, 216803, 220931, 221069, 221087, 221603, 222107, 225749, 229819, 231131, 231719, 232007, 232049, 233939, 235043, 240743, 242927, 247607, 253469, 254699, 260543, 260747, 263573, 264179, 266177, 267959, 268733, 270563, 270797, 271367, 273359, 274739, 275987, 277331, 279143, 282389, 283079, 284759, 284783, 285119, 285343, 287159, 287219, 288683, 290399, 294023, 295079, 295283, 297683, 297989, 299723, 300719, 307253, 309503, 311447, 312979, 315223, 316469, 320339, 321017, 323467, 323903, 325883, 328883, 336109, 336829, 336863, 341333, 342299, 345707, 346187, 347987, 349199, 349379, 349499, 350699, 353687, 353939, 356999, 359147, 361799, 364607, 365699, 365759, 377717, 379439, 381323, 391247, 397799, 399263, 400859, 401057, 402947, 405143, 408263, 411119, 411947, 414539, 416147, 420149, 422627, 424433, 427283, 428579, 429719, 430819, 432527, 438203, 438983, 440159, 440333, 440339, 440807, 441011,

442979, 442997, 443117, 443879, 443999, 445307, 446477, 448139, 448387, 449963, 456167, 462653, 463247, 463889, 463993, 467123, 468239, 470243, 470399, 470579, 473723, 475379, 477727, 478169, 478483, 480527, 483167, 484259, 486323, 489743, 490493, 492083, 492893, 495017, 499067, 499211, 500693, 500699, 508727, 516359, 517373, 520067, 522059, 522659, 526759, 526937, 527159, 532307, 534707, 539447, 539993, 546067, 547663, 549587, 550763, 551963, 553667, 556883, 558287, 564407, 565259, 566639, 566723, 569927, 571199, 571679, 573317, 579053, 580079, 595313, 598127, 599003, 604613, 605167, 606539, 607319, 607703, 612719, 616997, 617429, 619007, 622613, 626009, 630719, 631487, 633599, 637163, 641387, 643403, 647099, 647477, 649379, 651803, 660503, 660659, 663539, 664667, 665207, 667699, 669359, 670487, 672059, 672227, 673019, 673567, 675539, 675827, 676733, 679607, 681839, 682511, 684599, 684869, 688379, 688999, 691037, 691709, 694367, 695099, 695327, 695687, 702503, 703643, 703673, 706403, 708479, 708839, 709433, 709799, 711839, 713477, 713747, 713939, 714947, 715739, 717719, 718007, 730727, 732959, 733277, 735419, 736469, 737327, 739829, 742619, 744539, 745727, 753707, 755333, 759359, 759959, 762479, 766439, 767279, 767633, 773447, 778847, 779159, 779699, 779707, 784583, 785459, 793439, 794579, 795239, 798179, 798737, 799223, 799739, 803669, 809903, 811919, 819899, 820559, 823997, 828833, 829457, 831323, 831583, 831707, 836387, 836663, 837059, 838043, 838667, 841889, 844553, 852959, 855419, 855719, 855983, 856139, 863867, 864803, 865247, 865577, 869039, 869879, 870679, 872129, 872393, 877043, 882263, 882863, 885967, 898439, 901547, 902963, 904067, 904907, 905683, 911663, 913637, 915947, 916583, 918539, 919883, 921959, 922463, 923591, 928883, 929627, 931067, 936407, 938573, 940259, 946997, 947783, 948749, 950927, 951943, 954539, 954719, 958487, 962789, 963659, 973283, 974063, 975599, 978749, 981263, 982211, 984167, 992723, 992843

Table 2.2: Prime Numbers up to One Million which are not any Factor of a 3-Carmichael Number

Chapter 3

Further Observations Regarding Exceptional Primes

After finding this list of primes which are not the least factor of a 3-Carmichael number, we look to see if the primes are the least factor of other Carmichael numbers. We also make an observation regarding Sophie Germain primes as well as the residue classes of the primes from Tables 2.1 and 2.2.

3.1 4-Carmichael Numbers

In this section we examine whether the primes from Tables 2.1 and 2.2 are the least factor of a 4-Carmichael number. We first start by using an algorithm provided by Jaeschke in [8]. In this algorithm you must input values p_1 and p_2. This algorithm

then outputs all of the 4-Carmichael numbers of the form $p_1 \cdot p_2 \cdot p_3 \cdot p_4$ where $p_1 < p_2 < p_3 < p_4$. Using this algorithm we try to compute 4-Carmichael numbers whose least factor is in Table 2.1. This algorithm provides 4-Carmichael numbers with 11 and 197 as the least factor, but takes too long to run for the next value in the list which is 1223. This is because the algorithm must go through many more loops when we increase our least prime by an order of magnitude since the algorithm has nested for loops which each have an upper limit dependent on the value of p_1 and p_2 entered (see the algorithms on page 385 and 386 in [8] for more details.) We also searched to see if there were any Extended Chernick 4-Carmichael numbers. An example of one of the forms we checked is the form $(6m+1)(12m+1)(18m+1)(36m+1)$ where $m \in \mathbb{N}$, with least factor from Table 2.1. There are 7 different Chernick forms for 4-Carmichael numbers (see the table on page 272 of [3] for a list). We checked each one and, when we did this, we discovered that no such numbers exist other than the 4-Carmichael number $75361 = 11 \cdot 13 \cdot 17 \cdot 31$, which is not from one of Chernick's forms, but which we knew from tables. We then turned to other approaches to solve this problem.

3.2 Tables

There have been relatively large tables of both Carmichael numbers and pseudoprimes computed and published by several mathematicians. Tables of pseudoprimes can help us, since a Carmichael number is an absolute pseudoprime. This published

data can help because the Carmichael numbers we are interested can be found from some of this data if the data is large enough. For example, the algorithm mentioned above has only been able to find a 4-Carmichael number for 2 of the 543 primes we are interested in, but using a table of pseudoprimes up to 2^{64}, given by Feitsma and Galway from [6], we were able to find a 4-Carmichael number for 7 of the 543 primes we are interested in. We were able to search this table of pseudoprimes very easily because every Carmichael number in this list was marked, and the factors of the Carmichael numbers were listed as well. Furthermore, we contacted Galway and he was kind enough to send us a version of the algorithm which was used to create this table. If a larger table of Carmichael numbers or pseudoprimes can be produced, then we may be able to find the data we need to construct the complete list of 4-Carmichael numbers from the table. For a list of the found 4-Carmichael numbers, see Table 3.1. Note that we were able to find many different 4-Carmichael numbers with the least factor given below in the table, but we only listed one 4-Carmichael number for each such prime, p_1.

p1	**p2**	**p3**	**p4**
11	13	17	31
197	421	463	491
1223	1483	1873	6917
1487	2273	6301	2907451
4007	72109	120181	244367
9833	17207	22123	103237
11909	14657	17863	59083

Table 3.1: 4-Carmichael Numbers whose Least Factor is an Exceptional Prime

3.3 Primitive Carmichael Numbers

In this section, we examine our results in the context of the paper [7]. In this section we will use the following definitions (obtained from [7]):

Definition 3.1. Let c be a Carmichael number. Then $c = \prod_{i=1}^{n} p_i$ where p_i is prime for $i = 1, \ldots, n$. Let $g = \gcd(p_1 - 1, \ldots, p_n - 1)$ and notice that for each $i = 1, \ldots, n$, $p_i - 1 = a_i g$ for some $a_i \in \mathbb{N}$. Now let $l = \text{lcm}(a_1, \ldots, a_n)$. Then c is called *primitive* if $g \leq l$.

Definition 3.2. A Carmichael number is called *imprimitive* if it is not primitive.

Definition 3.3. If x is a positive real number, let $C_3(x)$ denote the number of 3-Carmichael numbers below x.

Definition 3.4. If x is a positive real number, let $C_3^0(x)$ denote the number of imprimitive 3-Carmichael numbers below x.

We will first give a summary of some of the results from [7]. It is noted that there was a disagreement between Erdős and Shanks. Erdős conjectured that there are $x^{1-o(1)}$ Carmichael numbers up to x, whereas Shanks was skeptical as to whether one might even find an x up to which there are more than $\sqrt{x}$ Carmichael numbers. Then Granville and Pomerance mention that if Carmichael numbers are separated into the classes of primitive and imprimitive Carmichael numbers, that Shank's argument applies more appropriately to imprimitive Carmichael numbers, while

Erdős' argument applies more appropriately to primitive Carmichael numbers. It is then mentioned that the disagreement between Erdős and Shanks is probably because most Carmichael numbers are primitive, whereas most Carmichael numbers with a fixed number of prime factors, such as those found in computations, are imprimitive. The authors then go on to make the conjecture that $C_k^0(x) \sim C_k(x)$ as $x \to \infty$ for each $k \geq 3$. If this is correct, we should see that most of the numbers found in the computations in this thesis are primitive, but as we increase our bound on p_1 we should see a higher percentage of imprimitive Carmichael numbers. This is in fact what we see. However, it should be noted that the number of imprimitive Carmichael numbers increases at a much slower rate than expected. This data is in Table 3.2. Also, it should be mentioned that of the 7 4-Carmichael numbers found in Table 3.1, 6 of them are primitive, while only 1 is imprimitive. However, since this amount of data is so small, it may not be representative of more 4-Carmichael numbers.

Upper Bound on p_1	$C_3(x)$	$C_3^0(x)$	**%age**
10^4	8639	2157	25
10^6	71951	20159	28

Table 3.2: The Number of Imprimitive Carmichael Numbers found

3.4 The Factorization of $p - 1$

In this section we take each prime, p, from Table 2.2 and factor the value $p - 1$. We also do this for the primes in Table 2.1 as well as 495 random primes below 10^6. When we do this, we notice that the factors from Tables 2.2 and 2.1 are mostly large primes. However, when we look at the factors of $p - 1$ for the 495 random primes, we see that there are a lot of small factors such as 2, 3, and 5, which occur many times. This data leads to an observation regarding Sophie Germain primes.

Definition 3.5. A *Sophie Germain prime* is a prime number, q, such that the value $2q + 1$ is also a prime.

Definition 3.6. A *Sophie Germain pair* is a pair of prime numbers of the form $(q, 2q + 1)$.

Of the 495 primes from Table 2.2, we can see that 169 of them (about 34%) are the larger value of a Sophie Germain pair. Put another way, for these 169 primes, p, $p - 1$ could be factored as 2 and one other large prime. However, for the list of random primes, there were 26 (about 5%) which could also be characterized in the same way. This leads to the observation that the larger prime $2q + 1$ of a Sophie Germain pair is less likely to be a factor of any 3-Carmichael number than is a random prime of the same size.

3.5 The Residue Classes of the Primes from Our Tables

If we examine the number of primes in each residue class for a fixed prime, p, we find that there are very few primes from our lists which belong to the residue class 1. This suggests that a prime number is more likely to be a factor of a 3-Carmichael number if it belongs to the residue class 1 for multiple primes p. We examine this data for all primes up to 100 but only include primes up to 13 in Table 3.3. It should also be mentioned that this tendency for the primes to avoid the residue class 1 for a prime p seems to decrease as p gets larger. Specifically, when $p > 37$ this tendency decreases. Note that in this table we examine the primes from Table 2.2, Table 2.1, and 495 random primes below 10^6.

The data in Table 3.3 and 3.4 are consistent with the observations about the prime factors of $p - 1$ made in Section 3.4.

Table 3.3: The number of primes from Table 2.2, Table 2.1, and 495 random primes which are congruent to n modulo p for $p = 3, 5, 7, 8$

p	n	Primes from Table 2.2	Primes from Table 2.1	Random Primes
3	1	30	35	250
	2	465	508	245
5	1	11	15	121
	2	154	170	137
	3	136	151	119
	4	194	207	118
7	1	9	12	86
	2	94	102	80
	3	101	116	82
	4	105	115	86
	5	86	90	74
	6	100	108	87
8	1	38	51	127
	3	192	203	113
	5	67	72	130
	7	198	217	125

Table 3.4: The number of primes from Table 2.2, Table 2.1, and 495 random primes which are congruent to n modulo p for $p = 11, 13$

p	n	Primes from Table 2.2	Primes from Table 2.1	Random Primes
11	1	16	19	51
	2	55	57	43
	3	52	57	41
	4	60	65	43
	5	52	57	42
	6	47	55	56
	7	42	45	62
	8	58	61	58
	9	52	56	48
	10	61	70	51
13	1	23	14	48
	2	40	34	46
	3	50	47	40
	4	43	42	29
	5	57	51	33
	6	39	35	51
	7	52	47	43
	8	27	24	43
	9	61	58	44
	10	39	39	40
	11	50	45	39
	12	62	59	39

Chapter 4

Some Conjectures Concerning Carmichael Numbers

Throughout this thesis, we have made several observations regarding Carmichael numbers. In this chapter, we make several conjectures based on these observations. Recall that of the 78497 odd primes below 10^6, only 543 of them (about 0.69% of primes) are not the least prime factor of a 3-Carmichael number. We also find that only 495 odd primes below 10^6 (about 0.63% of primes) are not *any* factor of a 3-Carmichael number. This shows that more than 99% of the odd primes below 10^6 occur as factors of 3-Carmichael numbers. This leads to the following conjecture:

Conjecture 4.1. *There are infinitely many 3-Carmichael numbers.*

Conjecture 4.1 follows from Dickson's (See [4]) prime k-tuples conjecture which,

in a slightly simplified form, says that if $a_1, \ldots, a_k$ are distinct even positive integers, then there are infinitely many positive integers n so that all k numbers $a_1n+1, \ldots, a_kn+1$ are prime. With $k = 3$, this conjecture would imply that there are infinitely many positive integers n for which each factor in Chernick's form $(6n + 1)(12n + 1)(18n + 1)$ is prime, so that the value of the form is a Carmichael number.

Furthermore, of the 543 primes which are not the least factor of a 3-Carmichael number, we find that some of them are the second or third factor of a 3-Carmichael number, and some are the least prime factor of a 4-Carmichael number. This leads to the following conjecture:

Conjecture 4.2. *Every odd prime occurs as some factor of a Carmichael number.*

It should be noted that both Conjectures 4.1 and 4.2 are stronger statements than the much-heralded results in [1].

Chapter 5

Conclusion

In this thesis we extended the research done on Carmichael numbers. We mainly examined the factors of 3-Carmichael numbers which led to some interesting observations. These observations led to some very strong conjectures. Thus, we have paved the way for someone to prove these conjectures and continue research on Carmichael numbers.

Appendix A: Information about the Computer and Software used

The computer used for these calculations is a custom built PC, which was custom built by James, with the following components:

Processor: Intel i-7 870 (4 cpu cores, each with hyperthreading for 8 total cpu threads)

Memory: 8 GB of Corsair XMS 3 DDR3 1600

Operating System: Microsoft Windows 7 (64-bit)

Software: Mathematica 7 for Students (64-bit), MATLAB R2008b Student (32-bit)

When we first approached this problem, we were only interested in the first factor of 3-Carmichael numbers. So, we used a slightly different version of Pinch's algorithm. The only difference was that this version of the algorithm only outputs one Carmichael number for each value of p_1 entered, or none if no such Carmichael number exists. It took about 10 straight days of computations with this altered

algorithm to create the tables of 3-Carmichael numbers with $p_1 < 10^6$ using Mathematica. Then, when we decided to compute *all* of the 3-Carmichael numbers with $p_1 < 10^6$, it took significantly longer. In fact, it took about 2 months to get this data. It could have been possible to do this in about half the time, however, it was only possible to run 2 instances of Mathematica on this computer because this version of Mathematica was the student version, otherwise this computer would have been able to run 4 instances with hyperthreading. Furthermore, we could have used cloud computing for even faster results, but this would have cost us money.

Most of the algorithms used in this paper were run in Mathematica because Mathematica is very powerful for calculations involving integers, whereas Matlab seemed to have problems when multiplying large numbers together. However, Matlab was used for comparing lists of numbers because it was very friendly for comparing and ordering lists of numbers. Because of this, Matlab was used to analyze most of the data that came from the algorithms in Mathematica.

Bibliography

[1] W. R. Alford, Andrew Granville, and Carl Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), no. 3, 703–722. MR 1283874 (95k:11114)

[2] R. D. Carmichael, *On composite numbers p which satisfy the Fermat congruence* $a^{P-1} \equiv 1 \bmod p$, The American Mathematical Monthly **19**, no. 2, pp. 22–27.

[3] Jack Chernick, *On Fermat's simple theorem*, Bull. Amer. Math. Soc. **45** (1939), no. 4, 269–274. MR 1563964

[4] L. Dickson, *A new extension of Dirichlet's theorem on prime numbers*, Messenger of Math. **33** (1904), 155–161.

[5] P. Erdős, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1956), 201–206. MR 0079031 (18,18e)

[6] Jan Feitsma and Will Galway, *Tables of pseudoprimes and related data*, `http://www.cecm.sfu.ca/Pseudoprimes/index-2-to-64.html`, February 2010.

[7] Andrew Granville and Carl Pomerance, *Two contradictory conjectures concerning Carmichael numbers*, Math. Comp. **71** (2002), no. 238, 883–908 (electronic). MR 1885636 (2003d:11148)

[8] Gerhard Jaeschke, *The Carmichael numbers to* 10^{12}, Math. Comp. **55** (1990), no. 191, 383–389. MR 1023763 (90m:11018)

[9] G.J.O. Jameson, *Carmichael numbers with three prime factors*, `http://www.maths.lancs.ac.uk/~jameson/3car.pdf`.

[10] A. Korselt, *Problème chinois*, L'intermédiare des mathématiciens **6** (1899), 142–143.

[11] R. G. E. Pinch, *The Carmichael numbers up to* 10^{15}, Math. Comp. **61** (1993), no. 203, 381–391. MR 1202611 (93m:11137)