8-1991

Carmichael numbers

David C. Burwell

To the Graduate Council:

I am submitting herewith a thesis written by David C. Burwell entitled "Carmichael numbers." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Mathematics.

R. M. McConnel, Major Professor

We have read this thesis and recommend its acceptance:

David Anderson, Ed Clark

Accepted for the Council:
Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

To the Graduate Council:

I am submitting herewith a thesis written by David C. Burwell entitled "Carmichael Numbers." I have examined the final copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Mathematics.

R. M. McConnel, Major Professor

We have read this thesis
and recommend its acceptance:

Accepted for the Council:

Associate Vice Chancellor
and Dean of The Graduate School

STATEMENT OF PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a Master of Science degree at the University of Tennessee, Knoxville, I agree the Library shall make it available to borrowers under rules of the Library. Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgement of the source is made.

Permission for extensive quotation from or reproduction of this thesis may be granted by my major professor, or in his absence, by the Head of Interlibrary Services when, in the opinion of either, the proposed use of the material is for scholarly purposes. Any copying or use of the material in this thesis for financial gain shall not be allowed without my written permission.

Signature ________________

Date 7-16-91

CARMICHAEL NUMBERS

A Thesis

Presented for the

Master of Science

Degree

The University of Tennessee, Knoxville

David C. Burwell

August 1991

ACKNOWLEDGEMENTS

I would like to thank my major professor, Dr. Robert McConnel, for his enthusiasm, and guidance, in every stage of preparing this thesis. I am indebted to my committee members, Dr. David Anderson and Dr. Ed Clark, for their advice, criticism and patience.

Special thanks to my wife, Elisabeth, for her encouragement and understanding.

ABSTRACT

This paper begins with a short description of Carmichael numbers, and the characterization of Carmichael numbers due to Chernick and the proof of this characterization. This along with Carmichael's original work leads naturally into a discussion of some bounds on Carmichael numbers in terms of the primes in their decomposition. Some bounds are presented and some examples given that show Carmichael numbers that attain these bounds. Next, Chernick's universal forms are examined, and a general universal form with an arbitrary number of linear factors is established. Some heuristic evidence is presented that supports the conjecture of the existence of infinitely many Carmichael numbers.

TABLE OF CONTENTS

Section **Page**

SECTION 1

INTRODUCTION

It is well known that Fermat's little theorem,

(1) $$a^{p-1} \equiv 1 \bmod(p),$$

for all a such that $(a,p) = 1$, is true for all primes p. If the converse were true, then it would provide a convenient test for primality of integers. There exist integers however, that are not prime that satisfy (1), as Carmichael [1] showed. If these composite integers could be classified by some means, listed for example, then (1) together with this classification could still be used as a test for primality.

Listing all composite integers of this form would only be possible if there were finitely many. But there is no proof yet that there are finitely or infinitely many of these composite integers, called Carmichael numbers after R. D. Carmichael their discoverer.

As to classification, Carmichael [2] and later Chernick [3] each gave proofs that for a positive integer C to be a Carmichael number it is necessary and sufficient that C be a square free odd composite integer with at least three prime factors, such that

$$C-1 \equiv 0 \bmod(p_i-1)$$

for all p_i that divide C. Chernick [3] went on to show a method for producing larger Carmichael numbers from a given Carmichael number. He also introduced universal forms with the question of infinitely many Carmichael numbers in mind.

Erdos [4] established an analytic bound on the number of Carmichael numbers less than a given integer, and established some heuristic evidence that there are indeed infinitely many. Pomerance, Selfridge and Wagstaff [5] improved on this bound and also suggested that infinitely many Carmichael numbers exist. In fact Yorinaga [10], [11] has produced impressive lists of Carmichael numbers, and Wagstaff [7] gives an example of a very large Carmichael number with 101 digits, which was improved upon when Woods and Huenemann [9] found a 432 digit Carmichael number.

Other papers (Wagstaff [8], Pomerance [6]) give more heuristic evidence that there are infinitely many Carmichael numbers.

This paper will look at some of the earlier work, in an algebraic rather than analytic manner. The desire here is to clarify, extend, and better understand the results on Carmichael numbers.

SECTION 2

CARMICHAEL NUMBERS

Before any investigation, some basic definitions and well known facts about Carmichael numbers are in order.

As the introduction implied, Carmichael numbers are positive composite integers that satisfy Fermat's little theorem. That is, C is a Carmichael number if

$$a^C \equiv a \bmod(C)$$

for all $a \in Z^+$. Since $a^C \equiv a \bmod(C)$ for some a and with C composite is the definition of a pseudoprime to the base a, then Carmichael numbers are pseudoprimes to every base.

These conditions on Carmichael numbers lead to a characterization of Carmichael numbers due to Chernick [3], that states:

C is a Carmichael number if and only if

$$C = p_1p_2...p_n, \qquad (n>2)$$

where p_i are distinct odd primes such that

$$C-1 \equiv 0 \bmod(p_i-1)$$

for each $p_i \mid C$.

The proof is as follows :

Suppose first that $C = p_1p_2...p_n$, $(n>2)$, p_i's distinct primes, each p_i odd, and $p_i-1 \mid C-1$ for $i = 1,2,...,n$. Then by Fermat's little theorem, for each p_i

$$a^{pi-1} \equiv 1 \bmod(p_i)$$

for all a such that $(a,p_i) = 1$, so that

$$a^{C-1} \equiv 1^{C-1/pi-1} \equiv 1 \bmod(p_i)$$

for each p_i. Since $(p_i,p_j) = 1$ for $i \neq j$ implies that the least common multiple of the p_i's is C, then

$$a^{C-1} \equiv 1 \bmod(p_i)$$

for each p_i implies

$$a^C \equiv a \bmod(p_i)$$

for each p_i, and for all a, or

$$a^C \equiv a \bmod(C)$$

for all a, and C is a Carmichael number.

Suppose on the other hand that C is a Carmichael number. Then from the definition of Carmichael numbers

$$a^C \equiv a \bmod(C)$$

for all a, and C is composite. Since C is composite let $C = 2^d p_1^{d1} \ldots p_n^{dn}$ where p_i are distinct odd primes, $d_i \in Z^+$. Define σ, as Carmichael [1] did, such that

$$\sigma(1) = 1$$

$$\sigma(2^d) = 2^{d-1} \text{ if } d = 1,2$$

$$\sigma(2^d) = 2^{d-2} \text{ if } d > 2$$

$$\sigma(p_i^{di}) = p_i^{di-1}(p_i-1)$$

if p_i is an odd prime; and if M composite

$$\sigma(M) = \sigma(2^d p_1^{d1} \ldots p_n^{dn})$$

so define $\sigma(M)$ as the Least Common Multiple (LCM) of

$$\{1, p_1^{d1-1}(p_1-1), \ldots, p_n^{dn-1}(p_n-1)\}$$

if $d = 0$,

$$\mathrm{LCM}\{2^{d-1}, p_1^{d1-1}(p_1-1), \ldots, p_n^{dn-1}(p_n-1)\}$$

if d = 1,2, and

$$\sigma(M) = \sigma(2^d p_1^{d1} \ldots p_n^{dn})$$
$$= \mathrm{LCM}\{2^{d-2}, p_1^{d1-1}(p_1-1), \ldots, p_n^{dn-1}(p_n-1)\}$$

if $d > 2$. With this definition of σ, Carmichael [1] states that for any $M \in Z^+$, $a^{\sigma(M)} \equiv 1 \bmod(M)$ for all a such that $(a,M) = 1$, and in fact $\sigma(M)$ is the least such integer.

Since C is a Carmichael number $a^{C-1} \equiv 1 \bmod(C)$ for all a such that $(a,C) = 1$, and, from the definition of σ,

$$a^{\sigma(C)} \equiv 1 \bmod(C)$$

for all a such that $(a,C) = 1$. This implies,

$$a^{C-1} \equiv a^{\sigma(C)} \equiv 1 \bmod(C)$$

and, since $\sigma(C)$ is the smallest such integer C-1 must be a multiple of $\sigma(C)$,

$$C-1 \equiv 0 \bmod(\sigma(C)).$$

Therefore

$$C-1 \equiv 0 \bmod(\mathrm{LCM}\{1, p_1^{d1-1}(p_1-1), \ldots, p_n^{dn-1}(p_n-1)\})$$

if d = 0,

$$C-1 \equiv 0 \bmod(\mathrm{LCM}\{2^{d-1}, p_1^{d1-1}(p_1-1), \ldots, p_n^{dn-1}(p_n-1)\})$$

if d = 1,2,

or

$$C-1 \equiv 0 \bmod(\mathrm{LCM}\{2^{d-2}, p_1^{d1-1}(p_1-1), \ldots, p_n^{dn-1}(p_n-1)\})$$

if $d > 2$.

Now suppose C is even, that is $d \neq 0$, then $C-1 = 2q-1$ for some $q \in Z^+$. Clearly

$$\mathrm{LCM}\{2^{d-1}, p_1^{d1-1}(p_1-1), \ldots, p_n^{dn-1}(p_n-1)\}$$

has at least one factor of 2, thus, since 2 divides $\sigma(C)$ and 2 divides 0 and C is even,

$$C-1 \equiv 0 \bmod(\sigma(C))$$

implies that 1/2 is an integer, which is false. Therefore, C is never even, and thus $C = p_1^{d1}\ldots p_n^{dn}$, where the p_i's are distinct odd primes.

Suppose similarly that $d_j > 1$ for some j. Then

$$p_j^{dj-1} \mid \mathrm{LCM}\{p_1^{d1-1}(p_1-1),\ldots,p_n^{dn-1}(p_n-1)\}$$

and thus

$$C-1 = p_1^{d1}\ldots p_j^{dj}\ldots p_n^{dn}-1$$

$$\equiv 0 \bmod(\mathrm{LCM}\{p_1^{d1-1}(p_1-1),\ldots,p_n^{dn-1}(p_n-1)\}).$$

But this implies

$$p_1^{d1}\ldots p_j^{dj}\ldots p_n^{dn}-1 \equiv 0 \bmod(p_j^{dj-1}),$$

which is true if and only if $1/p_j^{dj-1}$ is an integer, that is only when $d_j-1 = 0$. This contradicts $d_j > 1$, therefore none of the d_j's is greater than one. This leaves

$$C = p_1\ldots p_n$$

where the p_i are distinct odd primes and

$$C-1 \equiv 0 \bmod(\mathrm{LCM}\{(p_1-1),\ldots,(p_n-1)\})$$

which is true if and only if

$$C-1 \equiv 0 \bmod(p_i-1)$$

for all $p_i \mid C$.

Finally suppose C is the product of exactly two prime factors, say $C = p_1p_2$, and, without loss of generality, let $p_1 < p_2$. Then

$$C-1 \equiv 0 \bmod(p_i-1)$$

for all $p_i \mid C$, implies

$$C-1 \equiv 0 \mod(p_2-1).$$

But

$$C-1 = p_1p_2-1,$$

so that

$$p_1p_2-1 \equiv 0 \mod(p_2-1);$$

however

$$p_1p_2-1= p_1(p_2-1) + p_1-1,$$

which leaves

$$p_1-1 \equiv 0 \mod(p_2-1),$$

which implies $p_2-1 \leq p_1-1$ or $p_2 \leq p_1$, which contradicts $p_1 < p_2$. Thus C must have at least three distinct prime factors, that is n must be greater than two. This completes the proof.

With this characterization of Carmichael numbers, considering the size of Carmichael numbers in terms of some subset of the primes in their decomposition, seems like the next logical step in determining if there are infinitely many Carmichael numbers. To this end, the next section considers some bounds on Carmichael numbers.

SECTION 3

SOME BOUNDS ON CARMICHAEL NUMBERS

It was shown earlier that the necessary and sufficient conditions for C to be a Carmichael number are

$$C-1 \equiv 0 \bmod (p_i-1)$$

for all i = 1,2,...n, n > 2, where the p_i are the distinct odd prime factors of C.

Let C denote a positive integer with n distinct odd prime factors, and let $p_1<p_2<\ldots<p_n$. Then, since

$$C-1 = p_1\ldots p_n-1$$

and

$$(p_1\ldots p_n-1)/(p_i-1)$$

$$= (p_1\ldots p_{i-1}p_{i+1}\ldots p_n) + (p_1\ldots p_{i-1}p_{i+1}\ldots p_n-1)/(p_i-1)$$

for C to be a Carmichael number it is both necessary and sufficient that

$$p_1\ldots p_{i-1}p_{i+1}\ldots p_n-1 \equiv 0 \bmod (p_i-1)$$

for all i=1,2,...,n, as Carmichael [2] showed. This implies that

$$p_1\ldots p_{i-1}p_{i+1}\ldots p_n \geq p_i$$

for all i. In particular:

<u>LEMMA 1</u> If $p_1\ldots p_n = C$, a Carmichael number, where $p_1<\ldots<p_n$, then $(p_1\ldots p_{n-1}-1)/(p_n-1) = m \in Z^+$, and $m < p_1\ldots p_{n-2}$.

Proof of Lemma:

By the choice of index on the p_i's and the fact that all the primes are distinct, then $p_n-1 > p_{n-1}$ which implies

$$(p_1\cdots p_{n-1}-1)/(p_n-1) < (p_1\cdots p_{n-1}-1)/p_{n-1}$$

$$= p_1\cdots p_{n-2} - (1/p_{n-1})$$

and since $0 < 1/p_{n-1}$,

$$(p_1\cdots p_{n-1}-1)/(p_n-1) < p_1\cdots p_{n-2}.$$

Therefore

$$m = (p_1\cdots p_{n-1}-1)/(p_n-1) < p_1\cdots p_{n-2}.$$

This provides an upper bound on m.

In the case where there are only three prime factors $p_1 < p_2 < p_3$ in the Carmichael number then Lemma 1 states that

$$m = (p_1p_2-1)/(p_3-1) < p_1.$$

For a lower bound on m consider:

LEMMA 2 If $p_1\cdots p_n = C$, a Carmichael number, where $p_1<\cdots<p_n$ then $(p_1\cdots p_{n-1}-1)/(p_n-1) = m \in Z^+$ and $m > 1$.

Proof of Lemma :

From lemma 1, $m \in Z^+$. Suppose $m = 1$. Then

$$m = (p_1\cdots p_{n-1}-1)/(p_n-1) = 1$$

which implies

$$(p_1\cdots p_{n-1}-1) = (p_n-1),$$

thus

$$p_1\cdots p_{n-1} = p_n,$$

which contradicts the fact that p_n is prime. Therefore $m > 1$ which completes the proof.

Now that m is bounded from above and below, bounds on Carmichael numbers come readily. The following theorem shows some of these bounds.

<u>THEOREM 1</u> If $C_n = p_1 \ldots p_n$ is a Carmichael number with n prime factors, $n > 2$, such that $p_1 < \ldots < p_n$, then

$$2p_n^2 - p_n \leq C_n, \text{ and}$$

$$C_n \leq \{(p_1 \ldots p_{n-2}[(p_1 \ldots p_{n-2}-1)(2p_1 \ldots p_{n-2}-1)+1])^2 + p_1 \ldots p_{n-2}[(p_1 \ldots p_{n-2}-1)(2p_1 \ldots p_{n-2}-1)+1]\}/2.$$

Proof of Theorem 1 :

Let $(p_1 \ldots p_{n-1}-1)/(p_n-1) = m$. From lemma 2, $m > 1$, thus

$$2 \leq (p_1 \ldots p_{n-1}-1)/(p_n-1)$$

which implies

$$2(p_n-1) \leq p_1 \ldots p_{n-1}-1,$$

or that

$$2p_n-1 \leq p_1 \ldots p_{n-1}.$$

Multiplying by p_n gives

$$2p_n^2-p_n \leq p_1 \ldots p_n = C_n$$

which completes the first part of theorem 1. For the second part of theorem 1, let $(p_1 \ldots p_{n-1}-1)/(p_n-1) = m$ and solve for p_n, hence

$$p_n = (p_1 \ldots p_{n-1}-1+m)/m.$$

But

$$(p_1 \ldots p_{n-2}p_n-1) \equiv 0 \bmod (p_{n-1}-1)$$

and hence, eliminating p_n,

$$(p_1 \ldots p_{n-2}(p_1 \ldots p_{n-1}-1+m)/m)-1 \equiv 0 \bmod (p_{n-1}-1)$$

or

$$(p_1 \ldots p_{n-2}(p_1 \ldots p_{n-1}-1+m)-m)/m \equiv 0 \bmod (p_{n-1}-1).$$

This implies

$$p_1 \cdots p_{n-2}((p_{n-1}-1)p_1 \cdots p_{n-2}+p_1 \cdots p_{n-2}-1+m)-m \equiv 0 \bmod(p_{n-1}-1)$$

and hence

$$(p_1 \cdots p_{n-2}+m)(p_1 \cdots p_{n-2}-1) \equiv 0 \bmod(p_{n-1}-1).$$

This implies that

$$p_{n-1}-1 \mid (p_1 \cdots p_{n-2}-1)(p_1 \cdots p_{n-2}+m)$$

and hence

$$p_{n-1}-1 \le (p_1 \cdots p_{n-2}-1)(p_1 \cdots p_{n-2}+m).$$

But Lemma 1 states that $m \le p_1 \cdots p_{n-2}-1$; hence

$$p_{n-1} \le (p_1 \cdots p_{n-2}-1)(2p_1 \cdots p_{n-2}-1)+1.$$

From the first part of the theorem $2p_n-1 \le p_1 \cdots p_{n-1}$ so that,

$$p_n \le (p_1 \cdots p_{n-1}+1)/2.$$

Substituting the upper bound for p_{n-1} in terms of $p_1 \cdots p_{n-2}$ leaves

$$p_n \le (p_1 \cdots p_{n-2}[(p_1 \cdots p_{n-2}-1)(2p_1 \cdots p_{n-2}-1)+1]+1)/2$$

as an upper bound for p_n. Therefore an upper bound for C_n is given by

(2) $$C_n \le (p_1 \cdots p_{n-2}[(p_1 \cdots p_{n-2}-1)(2p_1 \cdots p_{n-2}-1)+1]) \times (p_1 \cdots p_{n-2}[(p_1 \cdots p_{n-2}-1)(2p_1 \cdots p_{n-2}-1)+1]+1)/2.$$

Therefore

$$2p_n^2-p_n \le C_n,$$

$$C_n \le \{(p_1 \cdots p_{n-2}[(p_1 \cdots p_{n-2}-1)(2p_1 \cdots p_{n-2}-1)+1])^2 + p_1 \cdots p_{n-2}[(p_1 \cdots p_{n-2}-1)(2p_1 \cdots p_{n-2}-1)+1]\}/2$$

which completes the proof.

In the case when $n = 3$, the theorem states

$$2p_3^2-p_3 \le C_3 \le \{(p_1[(p_1-1)(2p_1-1)+1])^2 + p_1[(p_1-1)(2p_1-1)+1]\}/2$$

and in fact some Carmichael numbers do attain these bounds. For example, consider the smallest Carmichael number, namely $561 = 3 \cdot 11 \cdot 17$. In the above notation $p_1 = 3$, $p_2 = 11$, $p_3 = 17$, so the lower bound $2p_3^2 - p_3 \le C_3$ becomes

$$2 \cdot 17^2 - 17 = 561$$

and the upper bound

$$C_3 \le \{(p_1[(p_1-1)(2p_1-1)+1])^2 + p_1[(p_1-1)(2p_1-1)+1]\}/2$$

becomes

$$\begin{aligned} C_3 &\le \{(3[(3-1)(2 \cdot 3-1)+1])^2 + 3[(3-1)(2 \cdot 3-1)+1]\}/2 \\ &= \{(3[11])^2 + 3[11]\}/2 \\ &= \{33^2 + 33\}/2 \\ &= \{1089 + 33\}/2 \\ &= 561. \end{aligned}$$

Thus 561 is a Carmichael number that attains both the upper and lower bound.

The behavior of 561 is atypical of Carmichael numbers in general. In fact for a Carmichael with three prime factors to attain its upper bound it is necessary that

$$C_3 = \{(p_1[(p_1-1)(2p_1-1)+1])^2 + p_1[(p_1-1)(2p_1-1)+1]\}/2.$$

But equation (2) implies

$$p_1p_2p_3 = (p_1[(p_1-1)(2p_1-1)+1]) \text{ x } (p_1[(p_1-1)(2p_1-1)+1]+1)/2$$

and the second factor is an integer. Dividing by p_1 leaves

$$p_2p_3 = ((p_1-1)(2p_1-1)+1) \text{ x } (p_1[(p_1-1)(2p_1-1)+1]+1)/2,$$

so, since $(p_1[(p_1-1)(2p_1-1)+1]+1)/2$ is an integer and $p_1/2 > 1$, then the product on the right is a product of two distinct positive integers both greater than 1. Hence, from the ordering of the p_i's,

$$p_2 = ((p_1-1)(2p_1-1)+1)$$

or

$$p_2-1 = (p_1-1)(2p_1-1)$$

and

$$p_3 = (p_1[(p_1-1)(2p_1-1)+1]+1)/2 = (p_1[(p_2-1)+1]+1)/2.$$

But C_3 is a Carmichael number so that

$$p_1p_3-1 \equiv 0 \bmod(p_2-1).$$

Hence, substituting for p_3

$$p_1((p_1[(p_2-1)+1]+1)/2)-1 \equiv 0 \bmod(p_2-1)$$

or

$$p_1(p_1[(p_2-1)+1]+1)-2 \equiv 0 \bmod(p_2-1)$$

so that

$$p_1(p_1+1)-2 \equiv 0 \bmod(p_2-1)$$

which implies

$$p_1(p_1+1)-2 \geq p_2-1.$$

Since

$$(p_1-1)(2p_1-1) = p_2-1$$

then

$$p_1(p_1+1)-2 \geq (p_1-1)(2p_1-1)$$

or

$$p_1^2+p_1-2 \geq 2p_1^2-3p_1+1.$$

so that

$$4p_1 \geq p_1^2+3$$

or

$$4p_1 > p_1^2,$$

so

$$4 > p_1,$$

and since p_1 is an odd prime less than four, $p_1 = 3$. Therefore no Carmichael number with three prime factors other than 561 attains its upper bound, as 561 is the only Carmichael number with three prime factors that is divisible by three.

Carmichael numbers with more than three prime factors also do not attain their upper bound. The proof is similar to the preceding one.

For a Carmichael with n prime factors to attain its upper bound it is necessary that,

$$C_n = \{(p_1\cdots p_{n-2}[(p_1\cdots p_{n-2}-1)(2p_1\cdots p_{n-2}-1)+1])^2 + p_1\cdots p_{n-2}[(p_1\cdots p_{n-2}-1)(2p_1\cdots p_{n-2}-1)+1]\}/2.$$

But equation (2) implies

$$p_1\cdots p_n = (p_1\cdots p_{n-2}[(p_1\cdots p_{n-2}-1)(2p_1\cdots p_{n-2}-1)+1]) \times (p_1\cdots p_{n-2}[(p_1\cdots p_{n-2}-1)(2p_1\cdots p_{n-2}-1)+1]+1)/2.$$

Dividing by $p_1\cdots p_{n-2}$ leaves

$$p_{n-1}p_n = ((p_1\cdots p_{n-2}-1)(2p_1\cdots p_{n-2}-1)+1) \times (p_1\cdots p_{n-2}[(p_1\cdots p_{n-2}-1)(2p_1\cdots p_{n-2}-1)+1]+1)/2,$$

where the two factors on the right are again distinct positive integers each greater than one, hence

$$p_n = (p_1\cdots p_{n-2}[(p_1\cdots p_{n-2}-1)(2p_1\cdots p_{n-2}-1)+1]+1)/2$$

and

$$p_{n-1}-1 = (p_1\cdots p_{n-2}-1)(2p_1\cdots p_{n-2}-1);$$

so

$$p_n = (p_1 \cdots p_{n-2}[(p_{n-1}-1)+1]+1)/2.$$

But C_n is a Carmichael number so that

$$p_1 \cdots p_{n-2} p_n - 1 \equiv 0 \bmod (p_{n-1}-1).$$

Hence, substituting for p_n,

$$(p_1 \cdots p_{n-2}(p_1 \cdots p_{n-2}[(p_{n-1}-1)+1]+1)/2)-1 \equiv 0 \bmod (p_{n-1}-1),$$

thus

$$p_1 \cdots p_{n-2}(p_1 \cdots p_{n-2}+1)-2 \equiv 0 \bmod (p_{n-1}-1)$$

which implies

$$p_1 \cdots p_{n-2}(p_1 \cdots p_{n-2}+1)-2 \geq p_{n-1}-1.$$

Since

$$(p_1 \cdots p_{n-2}-1)(2p_1 \cdots p_{n-2}-1) = p_{n-1}-1,$$

then

$$p_1 \cdots p_{n-2}(p_1 \cdots p_{n-2}+1)-2 \geq (p_1 \cdots p_{n-2}-1)(2p_1 \cdots p_{n-2}-1)$$

or

$$(p_1 \cdots p_{n-2})^2+p_1 \cdots p_{n-2}-2 \geq 2(p_1 \cdots p_{n-2})^2-3p_1 \cdots p_{n-2}+1,$$

so that

$$4p_1 \cdots p_{n-2} \geq (p_1 \cdots p_{n-2})^2+3$$

or

$$4p_1 \cdots p_{n-2} > (p_1 \cdots p_{n-2})^2$$

so

$$4 > p_1 \cdots p_{n-2},$$

which implies $n = 3$ and $p_1 = 3$. Therefore no Carmichael number except 561 attains its upper bound.

Clearly, if there are several Carmichael numbers with three prime factors and the same smallest prime, each one has the same upper bound, and at most one of these will attain this upper bound. Consider, for example, 7 as the smallest prime in a Carmichael number with three prime factors. Yorinaga's [10] list of Carmichael numbers shows that there are only six Carmichael numbers that fit in this category, namely:

$$1729 = 7 \cdot 13 \cdot 19$$

$$2821 = 7 \cdot 13 \cdot 31$$

$$6601 = 7 \cdot 23 \cdot 41$$

$$8911 = 7 \cdot 19 \cdot 67$$

$$15841 = 7 \cdot 31 \cdot 73$$

$$52633 = 7 \cdot 73 \cdot 103.$$

A quick calculation of the upper bound gives $C_3 \leq 153181$, which is approximately three times as large as the largest Carmichael number shown.

This upper bound seems to get progressively worse as p_1 gets larger. When $p_1 = 31$, the upper bound is 3218349630 but the largest C_3 with 31 as the smallest prime factor is 471905281, approximately 1/8 the size. Looking at Carmichael numbers that have more than three prime factors, the first n-2 primes must be known to use the upper bound. For example consider $p_1 = 5$, $p_2 = 7$, then the upper bound for any Carmichael number with four prime factors with these two primes as the smallest prime factors is 6742134210. The largest C_4 that has 5 and 7 as the smallest primes in its factorization, according to Yorinaga's [10] list, is 170947105. This bound is more than 39 times too large.

Even though the upper bound seems to be of the order of $p_1p_2 \cdots p_{n-2}$ too large it still proves that:

<u>THEOREM 2</u> Given any n-2 positive ordered odd primes $p_1, p_2, \ldots, p_{n-2}$, there are finitely many Carmichael numbers C, with n prime factors, such that $p_1p_2 \ldots p_{n-2}$ divides C.

The lower bound is better in some sense, in that, given any single odd prime p_n, if p_n is the largest prime factor of a Carmichael number C then,

$$2p_n^2 - p_n \le C$$

as was shown above. But, in fact, this bound holds regardless of the size of p_n compared to the other prime factors of C. Since $2p^2-p \le 2p_n^2-p_n \le C$ for any p that divides C. Then for any prime p that is a factor of C,

$$2p^2 - p \le C.$$

There are numerous examples of Carmichael numbers that attain this lower bound. This should be expected since the proof of the lower bound used the bound on

$$m = (p_1 \cdots p_{n-1} - 1)/(p_n - 1) > 1.$$

Clearly, for some m

$$m \cdot p_n(p_n - 1) + p_n = C_n$$

for any Carmichael number, and when m = 2 the lower bound is attained. Some examples from Yorinaga's [10] list are:

$$561 = 3 \cdot 11 \cdot 17$$

$$8911 = 7 \cdot 19 \cdot 67$$

$$10585 = 5 \cdot 29 \cdot 73$$

$$115921 = 13 \cdot 37 \cdot 241$$

$$314821 = 13 \cdot 61 \cdot 397$$

$$334153 = 19 \cdot 43 \cdot 409$$

$$6313681 = 11 \cdot 17 \cdot 19 \cdot 1777$$

$$8134561 = 37 \cdot 109 \cdot 2017.$$

For Carmichael numbers with three prime factors, and the bounds established above, then given any prime p if it occurs in the factorization it must be greater than or equal to the smallest prime factor, and less than or equal to the largest prime factor. Therefore all Carmichael numbers, with three prime factors, that contain that prime p are in the range

$$2p^2-p \le C_3 \le \{(p[(p-1)(2p-1)+1])^2 + p[(p-1)(2p-1)+1]\}/2.$$

In general, when dealing with Carmichael numbers with more than three prime factors, this is not true. The first n-2 primes must be specified. It is clear however, that for infinitely many Carmichael numbers to exist there must be some infinite set P of odd primes such that each prime in this set is a divisor of some Carmichael number. Thus some iterative process for creating Carmichael numbers out of other Carmichael numbers, or the primes in P would be useful. Since Chernick [3] used his universal forms to generate Carmichael numbers with more prime factors from a given Carmichael number, an investigation of universal forms could be enlightening.

SECTION 4

CHERNICK'S UNIVERSAL FORMS

Chernick [3] defines a universal form U_n as any product of n odd distinct linear factors a_iM+b_i, where $n > 2$, and such that

$$U_n \equiv 1 \bmod (a_iM+b_i-1)$$

for $i = 1,2,3,\ldots,n$, and for every integer value of M in some infinite set of positive integers S. For example, $(6M+1)(12M+1)(18M+1)$ is a U_3 as,

$$(6M+1)(12M+1)(18M+1) \equiv 1 \bmod(6M)$$

and

$$(6M+1)(12M+1)(18M+1) \equiv (6M+1)(18M+1)$$

$$108M^2 + 24M + 1 \equiv 1 \bmod(12M)$$

and

$$(6M+1)(12M+1)(18M+1) \equiv (6M+1)(12M+1)$$

$$72M^2 + 18M + 1 \equiv 1 \bmod(18M).$$

If each of the linear terms in a U_n are prime for some M in S, then there are at least 3 odd primes such that

$$p_1 \cdots p_n \equiv 1 \bmod(p_i-1)$$

for each p_i, which makes the U_n a Carmichael number for that particular M. In the example above, since any M in Z^+ satisfies the congruences, and for M = 1, all three linear factors are prime, then $7 \cdot 13 \cdot 19 = 1729$ is a Carmichael number.

One way to prove that there are infinitely many Carmichael numbers would be to find a universal form that could be extended to contain an arbitrary number of linear factors such that for some set of integers M all the linear factors were prime in any of the extensions. Another way would be to find a universal form such that all the linear factors were prime for each M in some infinite set S. Chernick [3] has shown that there are universal forms with arbitrarily many linear factors. First, however, some preliminary results due to Chernick [3] are necessary.

<u>LEMMA 3</u> Let $U_{n-1} = (a_1M+1)(a_2M+1)\ldots(a_{n-1}M+1)$ and q_{n-1} be the LCM of the a_iM, $i = 1,2,3,\ldots,(n-1)$. Define r_{n-1} to be equal to $(U_{n-1}-1)/q_{n-1}$. If $a_nM = q_{n-1}\cdot t_{n-1}$ where t_{n-1} is any divisor of r_{n-1}, and a_nM+1 is distinct from the a_iM+1, then $(a_1M+1)(a_2M+1)\ldots(a_{n-1}M+1)(a_nM+1)$ is a U_n.

Proof of Lemma :

Clearly M divides q_{n-1}, because the LCM of the a_iM, $i = 1,2,3,\ldots,(n-1)$ is $M\cdot LCM\{a_i\}$ $i = 1,2,3,\ldots,(n-1)$. Also from the definition of a universal form $r_{n-1} = (U_{n-1}-1)/q_{n-1}$ is an integer for every positive integer M. Thus from the definition of a universal form, it suffices to show that

$$U_n \equiv 1 \bmod(a_iM)$$

for $i = 1,2,\ldots,n$. But

$$U_n = U_{n-1}(a_nM+1) \equiv a_nM+1 \equiv 1 \bmod(q_{n-1})$$

because $U_{n-1} \equiv 1 \bmod(q_{n-1})$, and $a_nM = q_{n-1}\cdot t_{n-1}$ so that $a_nM \equiv 0 \bmod(q_{n-1})$. Also since $a_nM+1 \equiv 1 \bmod(q_{n-1})$ this implies

$$a_nM+1 \equiv 1 \bmod(\mathrm{LCM}(a_iM))$$

$i = 1,2,\ldots,(n-1)$, so that

$$a_nM+1 \equiv 1 \bmod(a_iM)$$

for each $i = 1,2,\ldots,(n-1)$. Thus since,

$$U_{n-1} \equiv 1 \bmod(a_iM)$$

for each $i = 1,2,\ldots,(n-1)$,

$$U_n = U_{n-1}(a_nM+1) \equiv 1\cdot 1 \equiv 1 \bmod(a_iM)$$

for each $i = 1,2,\ldots,(n-1)$.

It remains to show that

$$U_n \equiv 1 \bmod(a_nM).$$

But $a_nM = q_{n-1}\cdot t_{n-1}$ which divides $r_{n-1}\cdot q_{n-1} = U_{n-1}-1$, this implies a_nM divides $U_{n-1}-1$ so that

$$U_{n-1} \equiv 1 \bmod(a_nM)$$

and therefore

$$U_n = U_{n-1}(a_nM+1) \equiv U_{n-1} \equiv 1 \bmod(a_nM).$$

This completes the proof of the lemma.

With this lemma, a universal form with an arbitrary number of linear factors can be constructed. Consider Chernick's [3] example, letting

$$U_3 = (6M+1)(12M+1)(18M+1),$$

here $q_3 = 36M$, which implies

$$r_3 = (U_3-1)/q_3 = (36M+396M^2+1296M^3)/36M$$
$$= 1+11M+36M^2$$

so set $t_3 = 1$, and $t_3q_3 = 36M$, thus

$$U_4 = (6M+1)(12M+1)(18M+1)(36M+1)$$

is a U_4 for all positive integers M by lemma 3 and $q_4 = 36M$.

Iterating this process, since $q_4 = 36M$ implies

$$r_4 = (U_4-1)/q_4 = (72M+1692M^2+15552M^3+46656M^4)/36M$$
$$= 2+47M+432M^2+1296M^3$$

if M is restricted to even integers, that is S is the set of all even positive integers, then two divides r_4 and one divides r_4. But choosing $t_4 = 1$ would repeat the linear factor (36M+1), and the lemma demands that the factors be distinct. Thus choose $t_4 = 2$, and

$$t_4q_4 = 72M.$$

Hence

$$U_5 = (6M+1)(12M+1)(18M+1)(36M+1)(72M+1)$$

is a U_5 for all positive integers M that are divisible by 2, and $q_5 = 72M$, which implies

$$r_5 = (U_5-1)/q_5 = 2 + (191/2)M + KM^2$$

where K is some polynomial in M with integer coefficients. Since M is even

$$r_5 = 2 + (191/2)M + KM^2 \equiv M/2 \bmod(2),$$

so to guarantee divisibility by 2, M must be restricted to integers divisible by four. Choosing $t_5 = 2$, then $t_5q_5 = 144M$, and

$$U_6 = (6M+1)(12M+1)(18M+1)(36M+1)(72M+1)(144M+1)$$

is a U_6 for all positive integers M that are divisible by 4, and the pattern seems clear. Thus let

$$U_n = (6M+1)(12M+1)(18M+1)(36M+1)\ldots(2^{n-2}9M+1)$$

be a universal form with n linear factors. Assume $n > 3$ and

$S = \{ M \text{ in } Z^+ : M \equiv 0 \bmod(2^{n-4}) \}$. Then $q_n = 2^{n-2}9M$ which implies

$$r_n = (U_n-1)/q_n$$

$$= ((6M+1)(12M+1)(18M+1)(36M+1)\ldots(2^{n-2}9M+1)-1)/2^{n-2}9M$$

which is an integer for all M in S. It is easy to show that,

$$(6M+12M+18M+36M+\ldots+2^{n-2}9M)/2^{n-2}9M = 2,$$

because

$$6M+12M+18M+36M+\ldots+2^{n-2}9M$$

$$= 18M(1+1+2+2^2+\ldots+2^{n-3})$$

$$= 18M(1+2^{n-2}-1)$$

$$= 18M(2^{n-2})$$

so that,

$$(6M+12M+18M+36M+\ldots+2^{n-2}9M)/2^{n-2}9M = 18M(2^{n-2})/2^{n-2}9M = 2.$$

Also the coefficient of M in r_n is the sum of the product of the a_iM in pairs divided by $2^{n-2}9M$, that is,

$$6M(12M+18M+36M+\ldots+2^{n-2}9M) + 12M(18M+36M+\ldots+2^{n-2}9M) +$$

$$\sum_{i=3}^{n} 2^{i-2}\cdot 9M \sum_{k=i+1}^{n} 2^{k-2}\cdot 9M$$

divided by $2^{n-2}9M$. Which is

$$6M(12M+18M(2^{n-2}-1))+12M(18M(2^{n-2}-1))$$
$$+\frac{(18M(2^{n-2}-1))^2-\sum_{i=3}^{n}(2^{i-2}\cdot 9M)^2}{2}$$

divided by $2^{n-2}9M$. Which equals $(3\cdot 2^{2n-4}-1)M/2^{n-4}$, an integer for any M in S. Also since 2^{2n-4} divides M, 2^{4n-8} divides M^2, and since $2^4 9$ divides any product of a_i taken three or more at a time, then $2^{2n-4}9$ divides the remaining terms in r_n. Thus the remaining terms are even after division by $2^{n-2}9M$. Hence,

$$r_n = 2 + (3\cdot 2^{2n-4}-1)M/2^{n-4} + KM^2,$$

so restricting M to integers that are divisible by 2^{n-3}, then choosing $t_n = 2$, so that $t_n q_n = 2^{n-1}9M$ and,

$$U_{n+1} = (6M+1)(12M+1)(18M+1)(36M+1)\dots(2^{n-2}9M+1)(2^{n-1}9M+1)$$

then U_{n+1} is a universal form. Therefore, by induction on n and lemma 3, there exist a universal form, U_n, for any n greater than 2.

For a universal form to be a Carmichael number it was shown earlier that, for some M in S, all the linear factors must be prime. So even though there exist universal forms with an arbitrary number of linear factors, this does not imply the existence of Carmichael numbers with an arbitrary number of prime factors.

However, Chernick [3] also proved that given any Carmichael number, $C_n = p_1 \dots p_n$, then it is possible to construct a U_n from the Carmichael number C_n, and

$$U_n = ((p_1-1)RM/k+p_1)\dots((p_n-1)RM/k+p_n),$$

provided that if all the $(p_1-1)/k$ are odd then the set S that M ranges over be replaced with 2S. In the expression for U_n above, k is the greatest common divisor of the p_i-1, and R is the LCM of $(p_i-1)/k$, $i = 1,2,\ldots,n$. This fact suggest a general form for lemma 3, that is;

<u>LEMMA 4</u> Let $U_{n-1} = ((p_1-1)RM/k+p_1)\ldots((p_{n-1}-1)RM/k+p_{n-1})$, a universal form constructed from a Carmichael number, and q_{n-1} be the LCM of the $(p_i-1)RM/k+p_i-1$, $i = 1,\ldots,(n-1)$, where k is the greatest common divisor of the p_i-1, and R is the LCM of $(p_i-1)/k$, $i = 1,2,\ldots,n$. Define r_{n-1} to be equal to $(U_{n-1}-1)/q_{n-1}$. If

$$(p_n-1)RM/k+p_n-1 = q_{n-1}t_{n-1}$$

for some p_n, not necessarily prime, where t_{n-1} is any divisor of r_{n-1}, and $(p_n-1)RM/k+p_n$ is distinct from the $(p_i-1)RM/k+p_i$, then

$$((p_1-1)RM/k+p_1)\ldots((p_{n-1}-1)RM/k+p_{n-1})((p_n-1)RM/k+p_n)$$

is a U_n.

Proof of Lemma :

From the definition of universal form it suffices to show that

$$U_n \equiv 1 \bmod((p_i-1)RM/k+p_i-1)$$

for all $i = 1,2,\ldots,n$. But,

$$U_n = U_{n-1}((p_n-1)RM/k+p_n) \equiv (p_n-1)RM/k+p_n \equiv 1 \bmod(q_{n-1})$$

because U_{n-1} is a universal form and hence

$$U_{n-1} \equiv 1 \bmod(q_{n-1});$$

also

$$(p_n-1)RM/k+p_n-1 = q_{n-1}t_{n-1} \equiv 0 \mod(q_{n-1})$$

which implies

$$(p_n-1)RM/k+p_n \equiv 1 \mod(q_{n-1}).$$

Therefore $U_n \equiv 1 \mod(q_{n-1})$, and since q_{n-1} is the LCM of the $(p_i-1)RM/k+p_i-1$, $i = 1,\ldots,(n-1)$,

$$U_n \equiv 1 \mod((p_i-1)RM/k+p_i-1),\ \text{for } i = 1,\ldots,(n-1),$$

and it remains to show that

$$U_n \equiv 1 \mod((p_n-1)RM/k+p_n-1).$$

Since

$$(p_n-1)RM/k+p_n-1 = q_{n-1}t_{n-1}$$

and

$$(U_{n-1}-1) = q_{n-1}r_{n-1}$$

and t_{n-1} is a divisor of r_{n-1}, this implies

$$(p_n-1)RM/k+p_n-1 \mid U_{n-1}-1$$

or that

$$U_{n-1} \equiv 1 \mod((p_n-1)RM/k+p_n-1)$$

but

$$U_n = U_{n-1}((p_n-1)RM/k+p_n)$$

so that

$$U_n \equiv ((p_n-1)RM/k+p_n) \equiv 1 \mod((p_n-1)RM/k+p_n-1).$$

That the $(p_n-1)RM/k+p_n$ is distinct from the $(p_i-1)RM/k+p_i$, $i = 1,\ldots,(n-1)$ is clear provided none of the $(p_i-1)RM/k+p_i-1$ happen to be equal to q_{n-1}, in which case choose $t_{n-1} = 1$, and if

$$(p_i-1)RM/k+p_i-1 = q_{n-1}$$

for some i, then $(p_n-1)RM/k+p_n$ will be distinct provided t_{n-1} does not equal one. But the constant term in

$$U_{n-1} = ((p_1-1)RM/k+p_1)\ldots((p_{n-1}-1)RM/k+p_{n-1}),$$

considered as a polynomial in M, is $p_1p_2\ldots p_{n-1}$ which implies that the constant term in

$$r_{n-1} = (U_{n-1}-1)/q_{n-1}$$

is $(p_1p_2\ldots p_{n-1}-1)/Rk$, an integer, because C_{n-1} is a Carmichael number. Also $q_{n-1} = LCM\{(p_i-1)RM/k+p_i-1\}$

$$= (RM+k)LCM\{(p_i-1)/k\}$$

$$= R(RM+k)$$

thus

$$U_{n-1}-1 \equiv 0 \bmod(R^2M+Rk)$$

for all positive integers M in some infinite set S, so that r_{n-1} is a polynomial with rational coefficients. Since $(p_1p_2\ldots p_{n-1}-1)/Rk$ is an integer greater than 1, by restricting S to non-negative integers divisible by the $(LCM\{b_i\})(p_1p_2\ldots p_{n-1}-1)/Rk$, where the b_i are the denominators of the coefficients of r_{n-1}, considered as a polynomial in M, and choosing

$$t_{n-1} = (p_1p_2\ldots p_{n-1}-1)/Rk$$

for example, would guarantee that $(p_n-1)RM/k+p_n$ is distinct, which completes the proof.

Combining lemma 4 with Chernick's [3] method of creating universal forms from given Carmichael numbers, results in;

<u>THEOREM 3</u> Given any Carmichael number $C_n = p_1 \ldots p_n$ there exists a universal form

$$U_n = ((p_1-1)RM/k+p_1)\ldots((p_n-1)RM/k+p_n)$$

and this form can be extended to contain an arbitrary number of linear factors.

Proof of Theorem; From Chernick's theorem on the construction of universal forms from Carmichael numbers, the first part of the theorem is clear. For the extension, applying lemma 4 to

$$U_n = ((p_1-1)RM/k+p_1)\ldots((p_n-1)RM/k+p_n)$$

gives the $\mathrm{LCM}\{(p_i-1)RM/k+p_i-1\} = \mathrm{LCM}\{((p_i-1)/k)(RM+k)\}$, $i = 1,2,\ldots,n$, which is $R(RM+k) = q_n$. Also

$$r_n = (((p_1-1)RM/k+p_1)\ldots((p_n-1)RM/k+p_n)-1)/R(RM+k)$$

so letting $t_n = (p_1p_2\ldots p_n-1)/Rk$ and restricting M to non-negative integers divisible by $(\mathrm{LCM}\{b_i\})(p_1p_2\ldots p_n-1)/Rk$ where the b_i are the denominators of the coefficients of r_n, implies,

$$q_nt_n = (RM+k)(p_1p_2\ldots p_n-1)/k$$

and

$$U_{n+1} = ((p_1-1)RM/k+p_1)\ldots((p_n-1)RM/k+p_n)$$
$$\times\ ((p_1p_2\ldots p_n-1)RM/k+p_1p_2\ldots p_n)$$

is a universal form, with constant term $(p_1p_2\ldots p_n)^2$.

Iterating this process,

$$q_{n+1} = (p_1p_2\ldots p_n-1)RM/k+p_1p_2\ldots p_n-1$$

and

$$r_{n+1} = (U_{n+1}-1)/((p_1p_2\ldots p_n-1)RM/k+p_1p_2\ldots p_n-1)$$

with constant term

$$((p_1p_2...p_n)^2-1)/(p_1p_2...p_n-1) = p_1p_2...p_n+1$$

which is divisible by $(p_1p_2...p_n+1)$ so choose

$$t_{n+1} = (p_1p_2...p_n+1).$$

Other choices are possible for t_{n+1}, since any divisor of r_{n+1} that is larger than one is sufficient, $t_{n+1} = 2$ would be a valid choice for t_{n+1}, because $p_1p_2...p_n+1$ is even. With $t_{n+1} = (p_1p_2...p_n+1)$, and restricting M to positive integers divisible by

$$(LCM\{b_i\})((p_1p_2...p_n-1)/Rk)(p_1p_2...p_n+1)$$
$$= (LCM\{b_i\})((p_1p_2...p_n)^2-1)/Rk,$$

where the b_i are the denominators of the coefficients of r_{n+1}, then,

$$U_{n+2} = ((p_1-1)RM/k+p_1)...((p_n-1)RM/k+p_n)$$
$$\times\ ((p_1p_2...p_n-1)RM/k+p_1p_2...p_n)$$
$$\times\ ((p_1p_2...p_n)^2-1)RM/k+(p_1p_2...p_n)^2.$$

This implies

$$q_{n+2} = ((p_1p_2...p_n)^2-1)RM/k+(p_1p_2...p_n)^2-1$$

and

$$r_{n+2} = (U_{n+2}-1)/(((p_1p_2...p_n)^2-1)RM/k+(p_1p_2...p_n)^2-1)$$

with constant term $(p_1p_2...p_n)^2+1$, so choosing

$$t_{n+2} = (p_1p_2...p_n)^2+1$$

and restricting M to positive integers divisible by $(LCM\{b_i\})((p_1p_2...p_n)^4-1)/Rk$, where the b_i are the denominators of the coefficients of r_{n+2}, implies,

$$U_{n+3} = ((p_1-1)RM/k+p_1)\ldots((p_n-1)RM/k+p_n)$$
$$\times\ ((p_1p_2\ldots p_n-1)RM/k+p_1p_2\ldots p_n)$$
$$\times\ (((p_1p_2\ldots p_n)^2-1)RM/k+(p_1p_2\ldots p_n)^2)$$
$$\times\ (((p_1p_2\ldots p_n)^4-1)RM/k+(p_1p_2\ldots p_n)^4)$$

is a universal form.

Assuming

$$U_{n+m} = ((p_1-1)RM/k+p_1)\ldots((p_n-1)RM/k+p_n)\ldots$$
$$(((p_1p_2\ldots p_n)^{2exp(m-1)}-1)RM/k+(p_1p_2\ldots p_n)^{2exp(m-1)})$$

is a universal form for M divisible by

$$(LCM\{b_i\})(p_1p_2\ldots p_n)^{2exp(m-1)}/Rk.$$

Then

$$q_{n+m} = ((p_1p_2\ldots p_n)^{2exp(m-1)}-1)RM/k+(p_1p_2\ldots p_n)^{2(exp(m-1)}-1$$

and

$$r_{n+m} = (U_{n+m}-1)$$
$$\div\ (((p_1p_2\ldots p_n)^{2exp(m-1)}-1)RM/k+(p_1p_2\ldots p_n)^{2exp(m-1}-1)$$

with constant term

$$(p_1p_2\ldots p_n)^{2(exp(m-1)}+1,$$

so choosing

$$t_{n+m} = (p_1p_2\ldots p_n)^{2exp(m-1)}+1$$

and restricting M to non-negative integers divisible by $(LCM\{b_i\})((p_1p_2\ldots p_n)^{2exp(m)}-1)/Rk$, where the b_i are the denominators of the coefficients of r_{n+m}, implies,

$$U_{n+m+1} = ((p_1-1)RM/k+p_1)\ldots((p_n-1)RM/k+p_n)\ldots$$
$$(((p_1p_2\ldots p_n)^{2exp(m)}-1)RM/k+(p_1p_2\ldots p_n)^{2exp(m)})$$

is a universal form. Therefore by induction, any universal form constructed from a Carmichael number can be extended to contain an arbitrary number of linear factors, and the theorem holds.

An example, at this point, will clarify much of the above notation. Choose $8911 = 7 \cdot 19 \cdot 67$, a Carmichael number, for this example. Then from Chernick's theorem,

$$R = 33, \ k = 6$$

and since all the $(p_i-1)/k$ are odd,

$$(66M+7)(198M+19)(726M+67)$$

is a universal form with three linear factors, where M ranges over all non-negative integers. So

$$q = 33(66M+6) \text{ and } r = 4356M^2+886M+45$$

and hence restricting M to integers that are divisible by 45 and choosing $t = 45$, then

$$qt = 1485(66M+6) = 98010M+8910$$

and

$$(66M+7)(198M+19)(726M+67)(98010M+8911)$$

is a universal form, for $M \equiv 0 \bmod(45)$, and M is non-negative.

The construction has the same limitation as Chernick's universal form of arbitrary length, in that it is sufficient that all linear factors be prime, for some M, to produce a Carmichael number.

SECTION 5

DISCUSSION

Applying the bounds of section 2 to the linear factors of universal forms instead of the prime factors of a Carmichael number changes the proof little. The bounds in fact are the same with p_i replaced with a_iM+b_i. More interesting is the observation that for Chernick's example of a universal form with an arbitrary number of linear factors, namely,

$$(6M+1)(12M+1)(18M+1)\ldots(2^{n-2}\cdot 9M+1),$$

that $(6M+1)^2 > (2^{n-2}\cdot 9M+1)$ for all admissible M. This is due to the fact that 2^{n-4} divides M, and thus $M \geq 2^{n-4}$. This implies that for any Carmichael number, obtained from some M, such that all the linear factors in the universal form are prime, then all the primes lie between the smallest prime p and p^2 inclusive. But as M gets arbitrarily large the number of primes between p and p^2 becomes unbounded. Although this does not prove that there are Carmichael numbers with arbitrarily many prime factors, it does suggest that this could be the case.

Alternatively, in the proof of the existence of a universal form with an arbitrary number of linear factors, it was necessary to restrict S repeatedly as factors were added to the universal form. This suggest that there is no fixed Carmichael number that can be used to obtain Carmichael numbers with an arbitrary number of prime factors.

Also, in the construction of a universal form with an arbitrary number of linear factors, r_n was determined to be a polynomial in M with rational coefficients. It seems that r_n has integer coefficients when U_n is first constructed out of a Carmichael number, but not necessarily for any other step in the construction, that is, not for any r_{n+m}. If it could be shown that r_{n+m} has integer coefficients, then the LCM$\{b_i\}$ would be 1, and choices for M could be found without finding r_{n+m} explicitly.

Since one method of showing that there are infinitely many Carmichael numbers is to show that a fixed Carmichael number can be used to create Carmichael numbers with an arbitrary number of prime factors. The conjecture above, that states this is unlikely, must be shown to be false. Whereas, even with the weaker conclusion for universal forms, showing the conjecture to be false seems difficult.

LIST OF REFERENCES

LIST OF REFERENCES

[1] R. D. Carmichael: Note on a new number theory function. Bull. Amer. Math. Soc., **19** (1910), 232-238

[2] R. D. Carmichael: On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$. Amer. Math. Monthly, **19** (1912), 22-27

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

[4] P. Erdos: On pseudoprimes and Carmichael numbers. Publ. Math. Debrecen, **4** (1956), 201-206

[5] C. Pomerance, J. L. Selfridge and S. Wagstaff, Jr.: The pseudoprimes to $25 \cdot 10^9$. Math. Comp., **35** (1980), 1003-1026

[6] C. Pomerance: On the distribution of pseudoprimes. Math. Comp., **37** (1981), 587-593

[7] S. Wagstaff, Jr.: Large Carmichael numbers. Math. J. Okayama Univ., **22** (1980), 33-41

[8] S. Wagstaff, Jr.: Pseudoprimes and a generalization of Artin's conjecture. Acta Arith., **41** (1982), 141-150

[9] D. Woods and J. Huenemann: Larger Carmichael numbers. Comp. & Maths. with Appls., **8** (1982), 215-216

[10] M. Yorinaga: Numerical computation of Carmichael numbers. Math. J. Okayama Univ., **21** (1979), 183-205

[11] M. Yorinaga: Carmichael numbers with many prime factors. Math. J. Okayama Univ., **22** (1980), 169-184

VITA

David C. Burwell received a Bachelor of Science in Mathematics, with Physics emphasis, from Central State University, Edmond, Oklahoma in May 1989. In the fall of 1989 he entered the University of Tennessee, Knoxville, and began study toward a Master of Science degree in Mathematics. During the 1989-90, 1990-91 academic years he worked as a teaching assistant for the Mathematics Department at the University of Tennessee. A Master of Science degree was awarded in August 1991.

The author is a member of the American Mathematical Society, The Mathematical Association of America, and the Alpha Chi national honor society.