#A31 INTEGERS 12 (2012)

THE IMPOSSIBILITY OF CERTAIN TYPES OF CARMICHAEL NUMBERS

Thomas Wright[1]
Department of Mathematics, Wofford College, Spartanburg, South Carolina
wrighttj@wofford.edu

Received: 4/2/11, Revised: 1/24/12, Accepted: 4/5/12, Published: 4/18/12

Abstract

The proof of the existence of infinitely many Carmichael numbers depends heavily upon the study of the Carmichael lambda function λ. In this paper, we study which types of forms this quantity can and cannot take. In particular, for a Carmichael number m, we prove that this $\lambda(m)$ can never be of the form 2^k. Moreover, we prove that if this $\lambda(m)$ is of the form $2^k \cdot P$ then either $P = 3, 5, 7$ or 127 and m is one of just eight possible values or else m is divisible by a Fermat Prime that is not currently among the known Fermat Primes.

1. Introduction

Let us begin by defining a Carmichael number:

Definition 1. Let $m \in \mathbb{N}$. If $m|a^m - a$ for every $a \in \mathbb{Z}$ and m is composite then m is a *Carmichael number*.

Such numbers, which answer in the negative the question of whether the converse of Fermat's Little Theorem is true, were first discovered by R.D. Carmichael in 1910 and thus bear his name.

The search for Carmichael numbers typically involves the study of the Carmichael function λ, which is defined as follows. For any prime power p^α, $\alpha \geq 1$, one has:

$$\lambda(p^\alpha) = \begin{cases} p^{\alpha-1}(p-1) & \text{if } p \text{ is odd or } \alpha \leq 2, \\ 2^{\alpha-2} & \text{if } p = 2 \text{ and } \alpha \geq 3. \end{cases}$$

For arbitrary $m \geq 2$ with prime factorization $m = p_1^{\alpha_1}...p_k^{\alpha_k}$, one has

$$\lambda(m) = LCM[\lambda(p_1^{a_1}), ..., \lambda(p_k^{\alpha_k})].$$

[1] I would like to thank Lazlo Hethelyi for helping start this research and Wells Johnson for all of his direction. I would also like to thank the referee for many helpful comments and suggestions.

Finally, $\lambda(1) = 1$. In the case that m is a Carmichael number, it is well known that m is square-free; hence, $m = p_1....p_k$, and thus,

$$\lambda(m) = LCM[p_1 - 1, ..., p_k - 1].$$

In 1994, it was proven by Alford, Granville, and Pomerance [1] that there are infinitely many Carmichael numbers, thereby resolving a conjecture that had been open for almost 100 years. This proof, which builds on ideas originally suggested by Erdős [3], yields Carmichael numbers m for which $\lambda(m)$ has many distinct prime factors. It is worth noting, however, that some of our most famous examples of Carmichael numbers have very simple λ's; for instance, the first Carmichael number, 561, has $\lambda(m) = 2^4 \cdot 5$, while the taxicab number, 1729, is a Carmichael number with $\lambda(m) = 2^2 \cdot 3^2$. It is in this spirit that we ask the following question:

Motivating Question. What can we say about Carmichael numbers if we restrict the possibilities for λ?

This paper examines the most basic cases: those cases for which $\lambda(m) = 2^k$ and $\lambda(m) = 2^k P$ for a prime P. The former has an obvious relation to Fermat (a Carmichael number of this form would be composed entirely of Fermat primes), while the latter is interesting because, as was stated earlier, the smallest Carmichael number, 561, has λ of this form.

In section 3, we prove the following:

Main Theorem 1. *Let m be a Carmichael number. Then $\lambda(m)$ can never be a power of two.*

There are two easy corollaries of this theorem: a Carmichael number cannot be entirely composed of Fermat primes, and a Carmichael number cannot be of the form $m = 2^l + 1$.

Since $\lambda(m) = 2^k$ is impossible, the next most elementary case is the case of $\lambda(m) = 2^k P$ for a prime P. In order to make a statement about Carmichael numbers with such $\lambda(m)$, we will need some information about Fermat primes. To this end, we recall the following widely held conjecture:

Fermat Primes Conjecture. The primes 3, 5, 17, 257, and 65537 are the only primes of the form $2^a + 1$ with $a \geq 1$.

It will be shown that if $\lambda(m) = 2^k P$ then m must have a Fermat prime divisor (in fact, it must have two). We then find the following theorem about Carmichael numbers involving known Fermat primes.

Main Theorem 2. *Let m be a Carmichael number such that $\lambda(m) = 2^k P$ for a prime P. If the Fermat Primes Conjecture is true then P must be either 3, 5, 7,* *or 127 and m must be one of the following eight Carmichael numbers:*

$$\begin{gathered}5 \cdot 13 \cdot 17, \\ 5 \cdot 13 \cdot 193 \cdot 257, \\ 5 \cdot 13 \cdot 193 \cdot 257 \cdot 769, \\ 3 \cdot 11 \cdot 17, \\ 5 \cdot 17 \cdot 29, \\ 5 \cdot 17 \cdot 29 \cdot 113, \\ 5 \cdot 29 \cdot 113 \cdot 65537 \cdot 114689, \\ 5 \cdot 17 \cdot 257 \cdot 509.\end{gathered}$$

If any other m exists with $\lambda(m) = 2^k P$ then m is divisible by a heretofore unknown Fermat prime.

To prove the theorem above, section 3 will present a theorem that allows us to narrow the size of the factors of a Carmichael number with given $\lambda(m)$, while section 4 and 5 narrow the list of candidates for P. The remainder of the paper systematically goes through each remaining candidate and determines the Carmichael numbers resulting from each P.

2. Korselt's Criterion

Carmichael's task of finding such a number was aided by an earlier discovery of A. Korselt, who, in 1899, devised a test to determine whether a number was a Carmichael number [6]. This criterion (and subsequent reformulations) is known as Korselt's Criterion:

Korselt's Criterion. *m divides $a^m - a$ for all $a \in \mathbb{Z}$ if and only if $\lambda(m)|m - 1$.*

In this paper, we will use Korselt's Criterion to create a criterion of our own (which we will call the *Minimal Powers Argument*) that we will use repeatedly. This new criterion is outlined in the next section.

3. Minimal Power of Two

In order to discuss our criterion, we note first that since the computation of $\lambda(m)$ prominently involves the quantity $p_i - 1$, it will be useful for us to write p_i as a number plus one. To this end, we will write primes (and, often, odd integers in general) in the form $2^{k_i} D_i + 1$ (for odd D_i) and then study the power of two. Doing so affords us the following theorem:

Theorem 2. *Let m be a Carmichael number. Write*

$$m = \prod_{i=1}^{n} (2^{k_i} D_i + 1),$$

where the D_i are odd, $n \geq 2$, and $k_1 \leq k_2 \leq ... \leq k_n$. If $2^{k_1+1} | \lambda(m)$ then $k_1 = k_2$.

Proof. Assume $k_1 < k_2$. Then

$$m = \prod_{i=1}^{n} (2^{k_i} D_i + 1) \equiv 2^{k_1} D_1 + 1 \ (mod\ 2^{k_1+1}).$$

As $2^{k_1+1} | \lambda(m)$ by assumption and $\lambda(m) | m - 1$ by Korselt's criterion,

$$m \equiv 1 \ (mod\ 2^{k_1+1}).$$

Hence

$$2^{k_1} D_1 + 1 \equiv 1 \ (mod\ 2^{k_1+1}),$$

contradicting that D_1 is odd. □

This theorem will be referred to as the *Minimal Powers Argument*, and this k_1 referred to as the *minimal power of two*. We note that although the motivation was given in terms of $p - 1$, there is no requirement that the $2^{k_i} D_i + 1$'s are prime.

As an immediate consequence to Theorem 2, we have the following theorem:

Main Theorem 1. *If m is a Carmichael number and $k \in \mathbb{N}$ then $\lambda(m)$ cannot be of the form 2^k. In particular, no Carmichael number m can be of the form $2^s + 1$.*

Proof. If $\lambda(m) = 2^k$ then each prime p_i dividing m is of the form $p_i = 2^{k_i} + 1$. Since m is square-free, one of the k_i's must be minimal and unique, contradicting Theorem 2. Further, if m is of the form $2^s + 1$ then $\lambda(m) | 2^s$ by Korselt's criterion, and hence $\lambda(m) = 2^k$. □

4. $\lambda(m) = 2^k P$: Prelude

Now, we move on to the case where m is a Carmichael number with $\lambda(m) = 2^k P$ for a prime P. The remainder of the paper will be devoted to proving Main Theorem 2.

In this section, we prove a couple of lemmas that limit the types of factors that can show up for each choice of P. These limitations allow us to completely remove all P's that are 1 mod 12.

We begin by noting that in order for $\lambda(m)$ to have the form $2^k P$, the prime factors of m must be of the form $p_i = 2^{k_i} + 1$ or $q_j = 2^{l_j} P + 1$. We say that primes of the form $p_i = 2^{k_i} + 1$ are of *Type 1* and primes of the form $q_j = 2^{l_j}P + 1$ are of *Type 2* (the former will be denoted as p's and the latter as q's; the powers of two appearing in the former will be denoted as k_i's, and those appearing in the latter will be l_j's). We note an easy lemma about the parity of these exponents:

Lemma 3. *Any k_i must itself be two to some power. Any l_j is even if $P \equiv 1$ (mod 3) or odd if $P \equiv 2$ (mod 3).*

Proof. The first statement follows from the definition of a Fermat prime, and the second follows from examination modulo 3. □

Since a Carmichael number is square-free, it follows from Theorem 2 that a Carmichael number with $\lambda(m) = 2^k P$ must be divisible by at least one prime of each type. Assume that $p_1 < p_2 < ...$ and $q_1 < q_2 < ...$ (or, equivalently, $k_1 < k_2 < ..$ and $l_1 < l_2 ...$). Again by Theorem 2, it is clear that $k_1 = l_1$.

Using the above, we can prove that P can never be 1 (mod 12):

Theorem 4. *Let $\lambda(m) = 2^k P$. If $P \equiv 1$ (mod 3) then $P \not\equiv 1$ (mod 4).*

Proof. Assume $P \equiv 1$ (mod 3). As noted above, any l_j is even while any k_i is 1 or even. Now, let

$$m = p_1 ... p_r q_1 ... q_s$$

where $r, s \geq 1$ and $r + s \geq 3$ (since it is known that any Carmichael number must be the product of at least three primes). We know that $k_1 = l_1 \geq 2$, which means that every k_i is even.

Next, let $P \equiv 1$ (mod 4). Then $P + 1 = 2D$ for some odd D. So

$$\begin{aligned} m =& (2^{k_1} + 1)(2^{l_1}P + 1)p_2 ... p_r q_2 ... q_s \\ &= (2^{k_1+1}(2^{k_1-1}P + D) + 1)p_2 ... p_r q_2 ... q_s, \end{aligned}$$

where it is possible that either $p_2 ... p_r$ or $q_2 ... q_s$ are empty. Since $r + s \geq 3$, we know that there must be another prime factor, and by Lemma 3, we know that k_2 or $l_2 \geq k_1 + 2$. So $2^{k_1+2} | \lambda(m)$ and 2^{k_1+1} is a unique smallest power of 2, thereby contradicting Theorem 2. □

Theorem 5. *Let $\lambda(m) = 2^k P$ with $P \equiv 2$ (mod 3). Then $5|m$ if and only if $P \equiv 3$ (mod 4).*

Proof. First, it is clear that $P + 1 = 2D$ for some integer D. Note that D is even if and only if $P \equiv 3$ (mod 4). Now, by Theorem 2 and Lemma 3, we see that $k_1 = l_1 = 1$. So

$$\begin{aligned} m &= 3(2P + 1)p_2 ... p_r q_2 ... q_s \\ &= (2^2(P + D) + 1)p_2 ... p_r q_2 ... q_s. \end{aligned}$$

Assume first that D is even. Clearly 2^2 is the smallest power of two in this expression. By Theorem 2, it must not be unique. So we must have $k_2 = 2$ or $l_2 = 2$, the latter of which is impossible by Lemma 3.

Now assume that D is odd. Then $2^3 | 2^2(P+D)$, which means (again by Theorem 2) that $k_2 \neq 2$. □

5. Fermat Primes

Now, we can drastically limit the number of permissible P's by proving the following lemma about Fermat prime divisors of a Carmichael number.

Lemma 6. *Let $p_1, p_2, ..., p_r$ be the Type 1 prime divisors of m. Then*

$$p_1 ... p_n \equiv 1 \pmod{P}.$$

Proof. First, we know that $P | \lambda(m) | m - 1$. Moreover, for any Type 2 prime divisor q_i, it is clear that $q_i \equiv 1 \pmod{P}$. So

$$\begin{aligned} m =& p_1 ... p_r q_1 ... q_s \\ \equiv& p_1 ... p_r \pmod{P} \\ \equiv& 1 \pmod{P}. \end{aligned}$$

□

Corollary 7. *Any Carmichael number m with $\lambda(m) = 2^k P$ must be divisible by at least two Fermat primes.*

Proof. We know from before that m is divisible by at least one Fermat prime. If m is divisible by only one Fermat prime p_1 then by the previous lemma, $P | p_1 - 1$, contradicting the assumption that P is odd. □

From here, we may determine the Carmichael numbers with known Fermat primes by taking all possible products of two or more Fermat primes (call such a product R), finding the odd prime factors of $R - 1$, and using Theorem 2 to identify Carmichael numbers. Table 1 illustrates all of the possible combinations R of Fermat primes and the prime factorizations for the various $R - 1$, indicating in addition what k_1 would have to be if a Carmichael number were divisible by R.

Now, since $k_1 = l_1$, we can remove any possible P on the table for which $2^{k_1} P + 1$ is not prime; the numbers we remove from the table are all such that $2^{k_1} P + 1$ is divisible by 3, 5, 7, 11, 13, 19, or 103. By Theorem 4, we may also remove any $P \equiv 1 \pmod{12}$. Moreover, by Theorem 5, we may also remove $P = 11$ and 41. The removed P's and k_1's and explanations for their removal are given on Table 2, while the remaining candidates for P are given on Table 3.

Table 1: Products of Fermat primes

Combination of Primes (R)	Factorization of $R-1$	k_1
$3*5$	$2*7$	1
$3*17$	$2*5^2$	1
$3*257$	$2*5*7*11$	1
$3*65537$	$2*5*19661$	1
$3*5*17$	$2*127$	1
$3*5*257$	$2*41*47$	1
$3*17*257$	$2*6553$	1
$3*5*65537$	$2*491527$	1
$3*17*65537$	$2*127*13159$	1
$3*257*65537$	$2*25264513$	1
$3*5*17*257$	$2*7*31*151$	1
$3*5*257*65537$	$2*7*18046081$	1
$3*5*17*65537$	$2*8355967$	1
$3*17*257*65537$	$2*19*22605091$	1
$3*5*17*257*65537$	$2*2147483647$	1
$5*17$	2^2*3*7	2
$5*257$	$2^2*3*107$	2
$5*65537$	$2^2*3*7*47*83$	2
$17*257$	2^4*3^3*7*13	4
$17*65537$	2^4*3^3*2579	4
$257*65537$	$2^8*3*7*13*241$	8
$5*17*257$	$2^2*43*127$	2
$5*17*65537$	$2^2*131*10631$	2
$5*257*65537$	$2^2*467*45083$	2
$17*257*65537$	$2^4*29*43*113*127$	4
$5*17*257*65537$	$2^2*3*7*11*31*151*331$	2

This removal leaves us with just six possible values for P: 3, 5, 7, 43, 127, and 19661. In the next section, we will prove that two more of these can be removed.

6. The Impossible Cases: $P = 43, 19661$

The rest of the paper will go through the six remaining P's from the previous section and determine the Carmichael numbers associated to each P. We begin with the two P's above for which no Carmichael numbers exist: 43 and 19661. We will use essentially the same argument for each of these two cases.

Theorem 8. *$P \neq 43$.*

Table 2: Eliminated P and k_1

Condition	Pairs (P, k_1) Removed by Condition
$3 \vert 2^{k_1}P+1$	$(7,1)$, $(19,1)$, $(31,1)$, $(127,1)$, $(151,1)$, $(6553,1)$, $(13159,1)$, $(491527,1)$, $(18046081,1)$, $(25264513,1)$, $(8355961,1)$, $(22605091,1)$, $(2147483647,1)$ $(11,2)$, $(47,2)$, $(83,2)$, $(107,2)$, $(131,2)$, $(10631,2)$, $(29,4)$, $(113,4)$, $(2579,4)$,
$5 \vert 2^{k_1}P+1$	$(47,1)$, $(31,2)$, $(151,2)$, $(331,2)$
$11 \vert 2^{k_1}P+1$	$(7,8)$
$13 \vert 2^{k_1}P+1$	$(43,4)$
$19 \vert 2^{k_1}P+1$	$(127,4)$
$103 \vert 2^{k_1}P+1$	$(241,8)$
Theorem 4	$(13,4)$, $(13,8)$
Theorem 5	$(11,1)$, $(41,1)$

Table 3: Carmichael Candidates

Combination of Primes (R)	Permissible Factors of $R-1$	k_1
$3 * 17$	5	1
$3 * 257$	5	1
$3 * 65537$	5,19661	1
$5 * 17$	3,7	2
5*257	3	2
$5 * 65537$	3,7	2
$5 * 17 * 257$	43,127	2
$5 * 17 * 257 * 65537$	3,7	2

Proof. From Table 3, if m is a Carmichael number with $P = 43$,

$$m = 5 \cdot 17 \cdot 257 \cdot \Pi_{i=1}^{s} q_i,$$

where the q_i are Type 2 primes. Now, by Theorem 2, $l_1 = 2$. Plugging this in for l_1 and multiplying gives

$$m = (2^5 \cdot 27 + 1) \cdot (2^4 + 1) \cdot 257 \cdot \Pi_{i=2}^{s} q_i.$$

Note that $13 \vert 2^4(43) + 1$. Since $2^8 \vert \lambda(m)$, 2^4 is clearly a minimal power of two, contradicting Theorem 2. □

Theorem 9. $P \neq 19661$.

Proof. This theorem is nearly identical to the case of $P = 43$. In this case,

$$m = 3 \cdot 65537 \cdot \Pi_{i=1}^{s} q_i.$$

Plugging in q_1 with $l_1 = 1$,

$$m = (2^4(7373) + 1) \cdot 65537 \cdot \Pi_{i=2}^{s} q_i.$$

Note that $11|2^3(19661)+1$ and $3|2^l(19661)+1$ for any even l. Here $2^{16}|\lambda(m)$, which means that 2^4 is the minimal power of two that contradicts Theorem 2. □

7. The Cases of $P = 7$ and $P = 127$

Since we have finally removed all of the cases where there are no Carmichael numbers, we now turn our attention to the cases for which Carmichael numbers exist. In this section, we deal with the two P's that are 1 modulo 3 for which there exist Carmichael numbers with $\lambda(m) = 2^k P$.

Theorem 10. *Let m be a Carmichael number with $\lambda(m) = 2^k \cdot 7$ where all Fermat prime factors are among the known Fermat primes. Then m is one of the following three Carmichael numbers:*

$$5 \cdot 17 \cdot 29,$$
$$5 \cdot 17 \cdot 29 \cdot 113,$$
$$5 \cdot 29 \cdot 113 \cdot 65537 \cdot 114689.$$

Proof. From the chart, if $P = 7$ then $l_1 = 2$. Thus, if $P = 7$ then $p_1 = 5$. Moreover, again from the chart, there are two possible cases for p_2: 17 and 65537.

Case 1. $p_2 = 17$.

Let us consider first the case where $p_2 = 17$. Then

$$m = 5 \cdot 17(2^2 \cdot 7 + 1) \prod_{j=2}^{s} q_j = (2^5 \cdot 77 + 1) \prod_{j=2}^{s} q_j,$$

where the remaining product may be empty.

Now, if the product is empty then $\lambda(m) = 2^4 \cdot 7|m - 1$, which means that $m = 5 \cdot 17 \cdot 29$ is a Carmichael number.

If the product is non-empty then $l_2 \leq 5$. This is only possible if $l_2 = 4$ (i.e., $q_2 = 113$), since q_2 would not be prime for $l_2 = 3$ or 5. In this case, we have

$$m = (2^5 \cdot 77 + 1)(2^4 \cdot 7 + 1) \prod_{j=3}^{s} q_j$$

where the product may again be empty. If the product is non-empty then 2^4 is the minimal power of two and $2^6|\lambda(m)$ (since $l_3 \geq 6$). If the product is empty then $\lambda(m) = 2^4 \cdot 7$ divides $m - 1$, and hence $m = 5 \cdot 17 \cdot 29 \cdot 113$ is a Carmichael number.

Case 2. $p_2 = 65537$.

In the case of $p_2 = 65537$, we again have $l_2 = 2$, giving us

$$m = (2^4 \cdot 9 + 1) \cdot (2^{16} + 1) \prod_{j=2}^{s} q_j.$$

Obviously, $2^{16} | \lambda(m)$. So there must be another prime factor with power of two less than or equal to 4, else 2^4 is the minimal power of two. So $l_2 = 4$ (i.e., $q_2 = 113$), which means that

$$m = (2^{14} + 1) \cdot (2^{16} + 1) \prod_{j=3}^{s} q_j.$$

There must be still another factor with power of two less than or equal to 14, else 2^{14} is the minimal power. Moreover, if $l_3 < 14$ then l_3 would be the unique minimal power of two. So $l_3 = 14$ (i.e., $q_2 = 114689$) and hence

$$\begin{aligned} m =& (2^{17}(2^{11} \cdot 7 + 1) + 1) \cdot (2^{16} + 1) \prod_{j=4}^{s} q_j \\ =& (2^{16}(268458277 \cdot 7) + 1) \prod_{j=4}^{s} q_j \end{aligned}$$

Now, if there were another prime factor q_4 then $l_4 \geq 18$, since $l_3 = 14$ and q_4 would not be prime with l_4 odd (by Lemma 3) or with $l_4 = 16$ (since $79 | 2^{16} \cdot 7 + 1$). So the remaining product is empty. Clearly, $\lambda(m) = 2^{16} \cdot 7$ divides $m - 1$ for the m above. So $m = 5 \cdot 29 \cdot 113 \cdot 65537 \cdot 114689$ is a Carmichael number.

Since all cases have been exhausted, these are the only possible Carmichael numbers with known Fermat primes and $\lambda(m) = 2^k \cdot 7$. □

Theorem 11. *Let m be a Carmichael number with $\lambda(m) = 2^k \cdot 127$ where all Fermat prime factors are among the known Fermat primes. Then*

$$m = 5 \cdot 17 \cdot 257 \cdot 509.$$

Proof. From the chart, we see that if $P = 127$ then $k_1 = l_1 = 2$ (i.e., $q_1 = 509$) and the Type 1 primes are 5, 17, and 257. Plugging this information in and manipulating the arithmetic, we have

$$m = (2^9(127 \cdot 171) + 1) \prod_{j=2}^{s} q_j$$

where the product may be empty.

Now, assume the product is non-empty. It is clear that $p_3 - 1 = 2^8 | \lambda(m)$. So if there exists a q_2 with $l_2 < 8$ then l_2 would be the minimal power of two, contradicting Theorem 2. Moreover, if there exists q_2 with $l_2 \geq 10$ then $2^{l_2}|\lambda(m)$, which means that 2^9 would be the minimal power of two that contradicts Theorem 2. So $l_2 = 8$ or 9, which is impossible since neither would be prime ($13|2^8 \cdot 127 + 1$ and $3|2^9 \cdot 127 + 1$). Thus, the remaining product must be empty.

Note that if the remaining product is empty then $\lambda(m) = 2^8 \cdot 127|m - 1$. So $m = 5 \cdot 17 \cdot 257 \cdot 509$ is a Carmichael number; in fact, it is the only one with known Fermat primes and $P = 127$. □

8. The Case of $P = 5$

In this section, we consider the case of $P = 5$. This case is interesting for two reasons: it is the only case with $P \equiv 2 \pmod 3$, and the first Carmichael number, 561, is an example of this case. In this section, we show that 561 is in fact the only Carmichael number with $P = 5$ and known Fermat prime divisors.

Theorem 12. *Let m be a Carmichael number with $\lambda(m) = 2^k \cdot 5$ where all Fermat prime factors are among the known Fermat primes. Then*

$$m = 3 \cdot 11 \cdot 17.$$

Proof. From Table 2, we see that $p_1 = 3$, $p_2 = 17$, and $k_1 = l_1 = 1$ (i.e., $q_1 = 11$). Combining this information, we have

$$m = (2^4(35) + 1) \prod_{j=2}^{s} q_j$$

where the product may be empty.

Assume the product is non-empty, i.e., there exist q_2 and l_2. Note that $2^4|\lambda(m)$. Since $l_2 \neq 4$ by Lemma 3, either $l_2 = 3$ or $l_2 \geq 5$. In the former case, 2^3 is the minimal power of two contradicting Theorem 2, while in the latter case, $2^5|\lambda(m)$, which then means that 2^4 is the minimal power of two which causes the contradiction.

On the other hand, if the product is empty then $m = 3 \cdot 11 \cdot 17$, which is clearly a Carmichael number with $\lambda(m) = 2^4 \cdot 5$. □

9. The Special Case $P = 3$

The final case is that of $P = 3$. This is the most complicated case, both because there are several possible combinations of Type 1 primes and because we do not have the usual restriction that the l_i must be either all odd or all even. The best we can do to limit the possible l_i's is the following:

Lemma 13. *If $2^l \cdot 3 + 1$ is prime and $l \geq 2$ then $l \not\equiv 1$ (mod 3), 3 (mod 4), or 9 (mod 28).*

Proof. The first statement follows from examination mod 7, the second from examination mod 5, and the third from examination mod 29. □

Theorem 14. *Let m be a Carmichael number with $\lambda(m) = 2^k \cdot 3$ where all Fermat prime factors are among the known Fermat primes. Then m is one of the following three Carmichael numbers:*

$$5 \cdot 13 \cdot 17,$$
$$5 \cdot 13 \cdot 193 \cdot 257,$$
$$5 \cdot 13 \cdot 193 \cdot 257 \cdot 769.$$

Proof. We split this into three cases:

`Case 1.` $17|m$.

There are three possibilities for this on the table: either (5,17), (5,17,257) or (5,17,257,65537) are the Type 1 divisors of m. In all cases, $l_1 = 2$, which means that $q_1 = 13$. So

$$m = (2^4(69) + 1) \prod_{i=3}^{r} p_i \prod_{j=2}^{s} q_j,$$

where one or both of the products may be empty. Now, $2^4|\lambda(m)$. If there exist p_3 or q_2 then $k_3 > 4$ or $l_2 > 4$ (by Lemma 13), which would give 2^4 as the minimal power that contradicts Theorem 2. So both of these products must be empty, which means that $m = 5 \cdot 13 \cdot 17$, which is clearly a Carmichael number with $\lambda(m) = 2^4 \cdot 3$.

`Case 2.` The Type 1 primes divsors of m are 5 and 257.

In this case, $l_2 = 5$ and

$$m = (2^6 + 1)(2^8 + 1) \prod_{j=2}^{s} q_j.$$

Clearly, we have a problem with the minimal power of two (since $2^8|\lambda(m)$) unless we have another factor with 2^6. This can only be done if $l_2 = 6$, or $q_2 = 193$. Plugging this in for q_2, we have

$$m = (2^9(153) + 1) \prod_{j=3}^{s} q_j.$$

Now, if the product is empty then the remaining $m = 5 \cdot 13 \cdot 193 \cdot 257$ is a Carmichael number with $\lambda(m) = 2^8 \cdot 3$.

If the product is non-empty then $l_3 > 7$ (by Theorem 2) and $l_3 \leq 9$ (for the same reason). By Lemma 3, $l_3 \neq 9$. So $l_3 = 8$ (i.e., $q_3 = 769$), and hence

$$m = (2^9(153) + 1)(2^8 \cdot 3 + 1) \prod_{j=4}^{s} q_j.$$

Clearly, there can be no larger q_j (or else $2^9 | \lambda(m)$). So the remaining product is empty and $m = 5 \cdot 13 \cdot 193 \cdot 257 \cdot 769$ is a Carmichael number with $\lambda(m) = 2^8 \cdot 3$.

`Case 3.` The Type 1 primes divsors of m are 5 and 65537.

In this case, $l_1 = 2$. As such, we have

$$m = (2^6 + 1)(2^{16} + 1) \prod_{j=2}^{s} q_j.$$

To avoid contradicting Theorem 2, we must also have $l_2 = 6$, which gives us

$$m = (2^8(49) + 1)(2^{16} + 1) \prod_{j=3}^{s} q_j.$$

Again, to escape the ire of Theorem 2, we must multiply by a prime with $l_3 = 8$:

$$m = (2^9(49) + 1)(2^{16} + 1) \prod_{j=4}^{s} q_j.$$

Here again, Theorem 2 compels us to multiply by a prime with $l_4 = 9$. But this is impossible, since q_4 is then composite by Lemma 3. So there are no Carmichael numbers for Case 3. □

References

[1] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Mathematics, 140 (1994), 703-722.

[2] R. D. Carmichael, *Note on a new number theory function*, Bulletin of the American Mathematical Society, 16 (1910), 232-238.

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

[4] A. Granville, *Primality Testing and Carmichael Numbers*, Notices of the American Mathematical Society, 39 (September 1992), 696-700.

[5] A. Granville and C. Pomerance, *Two Contradictory Conjectures Concerning Carmichael Numbers*, Mathematics of Computation, 71 (2001), 883908.

[6] A. Korselt, *Problème chinois*, L'intermédinaire des mathématiciens 6 (1899), 142-143.