The Impossibility of Certain Types of Carmichael Numbers

Thomas Wright

Abstract

This paper proves that if a Carmichael number is composed of primes $p_i$, then the LCM of the $p_i - 1$'s can never be of the form $2^k$ and can be of the form $2^k \cdot P$ for only four prime values of $P \leq 127$. Moreover, if the LCM of a Carmichael number is $2^k \cdot P$ and a Carmichael number $m$ has all of its Fermat prime factors among the five known Fermat primes, then $P$ must be one of the four possibilities mentioned above, and $m$ can take one of only eight possible values.

1 Introduction

The study of Carmichael numbers began in In 1640, Fermat, in a letter to Frenicle, stated his now-famous "Little Theorem":

Fermat's Little Theorem: Let $p$ be a prime and $a \in \mathbb{N}$. Then $p|a^p - a$.

Fermat actually speculated further, claiming that the converse was true, i.e. if $p|a^p - a \forall a \in \mathbb{N}$ then $p$ is a prime. However, this assertion was incorrect, though it was not shown to be so until R.D. Carmichael computed the first counterexamples in 1910. Counterexamples to this conjecture thus bear the name of Carmichael, and are defined as follows:

Definition: Let $m \in \mathbb{N}$. If $m|a^m - a \forall a \in \mathbb{N}$ and $m$ is not prime, then $m$ is a Carmichael Number.
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 [Ko]:

**Korselt’s criterion:** $m$ divides $a^m - a \forall a \in \mathbb{Z}$ iff $m$ is squarefree and $p - 1 | m - 1$ for all primes $p$ which divide $m$.

Now, let us write this square-free $m$ as a product of distinct primes: $m = p_1p_2...p_n$. An equivalent formulation of Korselt’s criterion could be written as follows:

**Korselt’s criterion (revised):** $m$ divides $a^m - a \forall a \in \mathbb{Z}$ iff $L = LCM[p_1 - 1, p_2 - 1, ..., p_n - 1]$ divides $m - 1$.

It was Erdős who realized how this new formulation could be beneficial to the search for Carmichael numbers. He noted that instead of merely searching for a number which fit the original Korselt’s criterion, one should search for an integer $L$ with a sizeable number of factors. If enough of these factors were of the form $p - 1$ for a prime $p$, one could show that some product $p_1...p_n$ of these primes was $\equiv 1 \pmod{L}$ and thus must be a Carmichael number (since $L | p_1...p_n - 1$).

Erdős used this to give the first heuristic argument that there were infinitely many Carmichael numbers. This idea for $L$ was later used by Alfred, Granville, and Pomerance in their proof of the infinitude of Carmichael numbers, as they showed that the set of $L$’s which exhibited this behavior is infinite [Al].

Since others have studied $L$’s for which Carmichael numbers must exist, we turn our attention to $L$’s for which Carmichael numbers cannot exist. This paper examines two of the possible forms for $L$: $2^k$ and $2^k * P$. 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 the smallest Carmichael number, 561, has $L = 2^4 * 5$. In the former case, we use Section 1 to prove the following:
Theorem 1: If \( m \) is a Carmichael number and \( k \in \mathbb{N} \) then \( L \) cannot be of the form \( 2^k \). In particular, no Carmichael number \( m \) can be of the form \( 2^s + 1 \) for any \( s \in \mathbb{N} \).

The latter case is slightly trickier. Eventually, we prove general theorems about \( L = 2^k \cdot P \) for \( P \leq 127 \):

Theorem 2: Let \( P \leq 127 \). Then \( P = 3, 5, 7, \) or \( 127 \) and \( m \) is one of the following:

\[
\begin{align*}
  m &= 5 \cdot 13 \cdot 17, \\
  m &= 5 \cdot 13 \cdot 193 \cdot 257, \\
  m &= 5 \cdot 13 \cdot 193 \cdot 257 \cdot 769 \\
  m &= 3 \cdot 11 \cdot 17, \\
  m &= 5 \cdot 17 \cdot 29, \\
  m &= 5 \cdot 17 \cdot 29 \cdot 113, \\
  m &= 5 \cdot 29 \cdot 113 \cdot 65537 \cdot 114689, \\
  m &= 5 \cdot 17 \cdot 257 \cdot 509.
\end{align*}
\]

Additionally, these are the only Carmichael numbers with \( L = 2^k \cdot P \) where all of the Fermat prime divisors are among the known Fermat primes.

The proof of this requires us to have a handy method for bounding the size of these Carmichael numbers. In sections 2-4, we develop an algorithm which finds bounds for the prime factors of Carmichael numbers. This is used repeatedly, and with some cleverness about congruences, we use this to prove the above theorem. We examine separately the cases of \( P \equiv 1, 2, \) and \( 0 \) modulo 3 (where the last is clearly when \( P = 3 \)). It is interesting to note that all of the methods used are completely elementary and require very little background in number theory.

1.1 Notation

Throughout this paper, let \( m \) denote a Carmichael number, where for primes \( p_1, p_2, ..., p_n \), we have
\( m = p_1 p_2 \cdots p_n, \)
\( L = LCM[p_1 - 1, p_2 - 1, \ldots, p_n - 1]. \)

In all cases, \( L \) will either be of the form \( 2^k \) or \( 2^k \cdot P \), where \( P \) will always denote an odd prime. It is well known that \( m \) is always odd and square-free and \( n \) must be \( \geq 3 \).

### 1.2 The Minimal Powers Theorem

First, we need a theorem about the relationship between the powers of two for the various \( p_i - 1 \)'s. Let \( m \) be a square-free composite integer of the form

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

where \( n \geq 3 \), \( D_i \) is an odd positive integer \( \forall \ i \), and \( k_1 \leq k_2 \leq \ldots \leq k_n \).

**Theorem 1:** If \( m \) is a Carmichael number and \( 2^{k_1+1} \mid L \) then \( k_1 = k_2 \).

**Proof:** Assume \( k_1 < k_2 \). Then

\[
m = \prod_{i=1}^{n} (2^{k_i}D_i + 1)
= (2^{k_1}D_1 + 1) \prod_{i=2}^{n} (2^{k_i}D_i + 1)
\equiv 2^{k_1}D_1 + 1 \pmod{2^{k_1+1}}
\]

since \( k_i \geq k_1 + 1 \ \forall \ i > 1 \). Since \( 2^{k_1+1} \mid L \) and \( L \mid m - 1 \) by Korselt’s criterion, \( m \equiv 1 \pmod{2^{k_1+1}} \). Hence

\[
2^{k_1}D_1 + 1 \equiv 1 \pmod{2^{k_1+1}}
\]

contradicting that \( D_1 \) is odd. \( \square \)

This theorem will be used many times in this paper. It will be referred to as the *Minimal Powers Argument*, and this \( k_1 \) referred to as the *minimal power of two*. In general,
1.3 \( L \neq 2^k \) and \( m \neq 2^s + 1 \)

As a result of Theorem 1, we can immediately prove the nonexistence of Carmichael numbers with \( L \) of the form \( 2^k \).

**Theorem 1.1:** If \( m \) is a Carmichael number and \( k \in \mathbb{N} \) then \( L \) cannot be of the form \( 2^k \). In particular, no Carmichael number \( m \) can be of the form \( 2^s + 1 \) for any \( s \in \mathbb{N} \).

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

2 The Case of \( L = 2^k * P \)

2.1 General Properties of Carmichael Numbers with \( L = 2^k * P \)

In this section, we use the minimal powers argument to describe the characterize the various prime factors of a Carmichael number with \( L = 2^k * P \).

We begin by noting that in order for \( L \) to have the form \( 2^k * P \), the prime factors of a Carmichael number 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 \( 2^{k_i} + 1 \) are of Type 1 and primes of the form \( 2^{l_j} * P + 1 \) are of Type 2. Since a Carmichael number is square-free, it follows from Theorem 1 that a Carmichael number with \( L = 2^k * P \) 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 \( l_1 < l_2 < ... \)). Then we have the following lemma:

**Lemma 2.1.1:** If \( m \) is a Carmichael number with \( L = \)
$2^k \cdot P$ for some odd prime $P$, then $k_1 = l_1$.

**Proof:** Follows from Theorem 1. ⊞

**Corollary 2.1.2:** If $P \equiv 2 \pmod{3}$, then $3|m$ and $k_1 = l_1 = 1$. In particular, $2 \cdot P + 1$ must be prime.

**Proof:** If $l_1$ is odd and greater than 1 then $p_1$ is not prime. Similarly, since $P \equiv 2 \pmod{3}$, if $k_1$ is even then $3|q_1$ and $3 \neq q_1$. Thus, $k_1 = l_1 = 1$. ⊞

**Lemma 2.1.3:** If $L = 2^k \cdot P$ then

$$\prod_i (2^{k_i} + 1) \equiv 1 \pmod{P}.$$

**Proof:** Since $P|L$ and $L|m - 1$,

$$m = \prod_i (2^{k_i} + 1) \prod_j (2^{l_j} P + 1) \equiv 1 \pmod{P}$$

The latter product is clearly $\equiv 1 \pmod{P}$, so the former must be as well. ⊞

**Corollary 2.1.4:** If $m$ is a Carmichael number with $L$ of the form $2^k \cdot P$ for an odd prime $P$ then $m$ must have at least two Type 1 primes as divisors.

**Proof:** We already know that $m$ must have at least one prime divisor of each type. If there is only one Fermat prime divisor $2^{k_1} + 1$ of $m$ then $2^{k_1} + 1 \equiv 1 \pmod{P}$ by Lemma 2.1.3, which means that the odd prime $P$ divides $2^{k_i}$, a clear contradiction. ⊞

### 3 $P \equiv 2 \pmod{3}$

#### 3.1 An Algorithm for the Minimal Powers Argument

Here, we present an algorithm which, given a minimal power $r$, bounds the maximal power of two (the bound
will be denoted by \( B \). The algorithm applies in cases where \( 2^t + 1 \) and \( 2^t \cdot P + 1 \) for \( t \neq 1 \); this is clearly true whenever \( P \equiv 2 \pmod{3} \).

1.) Let \( B = r \) and \( h = (2^r + 1)(2^r \cdot P + 1) \)
2.) Let \( t \) be the maximal power of two such that \( 2^t|h - 1 \)
3.) If \( 2^t \cdot P + 1 \) and \( 2^t + 1 \) are not prime, define \( B \) as this \( t \) and stop.
4.) Follow one of the following steps:
   A.) If \( 2^t \cdot P + 1 \) is prime, then multiply \( h \) by \( 2^t \cdot P + 1 \) and define this new product to be \( h \).
   B.) If \( 2^t + 1 \) is prime, multiply \( h \) by \( 2^t + 1 \) and define this new product to be \( h \).
5.) Go back to step 2.

The following Theorem will be proven in Section NUMBER:

**Theorem 2.2.5:** Let \( m \) be a Carmichael number with \( L = 2^k \cdot P \) for some prime \( P \). If the algorithm terminates for some minimal power \( r \), then \( k < B \).

In our case, we have \( r = 1 \). We use this theorem now to resolve the case where \( P \equiv 2 \pmod{3} \).

### 3.2 The Case \( P \equiv 2 \pmod{3} \) with Known Fermat Prime Divisors

Here, we apply Theorem 2.2.5 to the case where \( P \equiv 2 \pmod{3} \), \( r = 1 \). We consider separately the cases where \( P = 5 \) and \( P > 5 \). We deal with the latter first:

**Theorem 2.2.6:** If \( m \) is a Carmichael number with \( L = 2^k \cdot P \), where the prime \( P > 5 \) and \( P \equiv 2 \pmod{3} \) then \( m \) is divisible by some Fermat prime larger than any of the five known Fermat primes.

**Proof:** By Lemma 2.1.3,

\[
\prod (2^{k_i} + 1) \equiv 1 \pmod{P}.
\]

7
Additionally, by Corollary 2.1.4, $m$ must have at least two Fermat prime divisors, and by Corollary 2.1.2, one of them must be 3. So we examine all possible combinations. Further, $3|m$ by Corollary 2.1.2. So we examine all square-free combinations of the known Fermat primes (3, 5, 17, 257, and 65537) which include 3, and we find $P$’s which are $\equiv 2 \pmod{3}$ and satisfy

$$P \mid 3 \prod_{i \neq 1} (2^{k_i} + 1) - 1.$$  

From the data (Table 1), there exist only five such $P$: 5, 11, 41, 47, and 19661.

Case 1: $P = 11$.

The only possible combination of known Fermat primes whose product $R$ is such that $11 | R - 1$ is $R = 3 \times 257$. So if $L = 2^k \times 11$ then $3, 23 | m$ and $k \geq 8$. In particular, $5 \not| m$, so all other prime factors have power of 2 greater than 2. So $m = 3 \times 23 \times $ (primes w/ powers of 2 greater than 2). But since $3 \times 23 = 1 + 2^2 \times 17$, this means that $\exists$ a minimal power of 2 less than $k$, contradicting Theorem 1. Thus, $P \not= 11$.

Case 2: $P = 41$.

The only possible product $R$ of known Fermat primes where $41 | R - 1$ is $R = 3 \times 5 \times 257$. Since $257 = 2^8 + 1$, $k \geq 8$. But by the algorithm, $B = 3$, and $3 < 8$. Thus, $P \not= 41$.

Case 3: $P = 47$.

$2 \times 47 + 1 = 95$ is not prime, contradicting Corollary 2.1.2.

Case 4: $P = 19661$.

The only possible product $R$ of known Fermat primes where $19661 | R - 1$ is $R = 3 \times 65537$. Now, $65537 = 2^{16} + 1$, so $k \geq 16$. But $B = 5$, and, of course, $5 < 16$.

Case 5: $P = 5$.  

8
In this case, $B = 6$ from the algorithm. So, in examining Table 1, we restrict ourselves to those products of Fermat primes where the maximal prime has power of 2 less than 6. There is only one such product $R$ where $5|R - 1$, specifically, $R = 3 \times 17$. Additionally, there are only two primes of the form $2^t \times 5 + 1$ with $t \leq 6$: 11 and 41. Since $3 \times 17 \times 41$ and $3 \times 11 \times 17 \times 41$ fail the modified Korselt’s criterion, we are left only with $3 \times 11 \times 17$, which is known to be a Carmichael number.

**Theorem 2.2.7**: If $m$ is a Carmichael number such that $P$ is an odd prime, $P \equiv 2 \pmod{3}$, $P < 127$, and $L = 2^k \times P$ then $m = 561$, $P = 5$.

**Proof**: Having already dealt with $P = 5$ in the previous theorem, we assume $P \geq 7$. By Theorem 2.2.6, if $P \equiv 2 \pmod{3}$ and $P \geq 7$ then at least one of the Fermat primes is not among the known Fermat primes. So $k \geq 32$, since any unknown Fermat prime has power of 2 equal to $2^N$ and must be greater than $65537 = 2^{16} + 1$. So if $B < 32$ for a given $P$ then there exist no Carmichael numbers with $L = 2^k \times P$. But Table 2 shows that for all prime $P \equiv 2 \pmod{3}$ where $7 < P < 127$, we have $B < 32$.

4 $P \equiv 1 \pmod{3}$: Setup

Because the case of $P \equiv 1 \pmod{3}$ is slightly more difficult, we must generalize the algorithm from the previous section.

4.1 A More General Algorithm

Since the above algorithm does not apply to all odd primes $P$, the next step is to generalize the algorithm. Recall that in the earlier case, for any $t$ there exists at most one possible prime of the right form. In this case, there can exist many primes or products of primes with power of two equal to $t$, any of which can be multiplied with the $h$. For this general version of the algorithm, it is useful
to think of the path the algorithm takes as a tree, where the tree branches any time the algorithm encounters a $t$ with multiple possible primes or products of primes. Once the algorithm is completed for each of the branches, the algorithm terminates and $B$ is defined to be the value of the largest $t$ attained on any of the branches.

We index a node of the tree by $t$, and we index the paths from a given node by $(t, z)$, where $t$ is the node and $z$ is a possible path at that node. Further, we let $C_{t,z}$ denote the prime or product of primes with power of two equal to $t$ which causes the algorithm to travel path $t, z$. More formally, for a given $t$, define $C_{t,z}$ by

$$C_{t,z} = \prod_{i=1}^{n}(2^{k_i} \times P + 1) \prod_{j=1}^{w}(2^{l_j} + 1)$$

where $r \leq k_i \leq t$ and $r \leq l_j \leq t \quad \forall \ i \text{ and } j$, $2^{k_i} \times P + 1$ and $2^{l_j} + 1$ are primes, and $C_{t,z} = 2^t \times D_{t,z} + 1$ for some odd $D_{t,z}$. Note that one of the products may be empty. Let $S_t$ be the set of $C_{t,z}$’s for a given $t$. Again, we let $r$ be the minimal power of two for prime divisors of $m$.

1.) Let $B = r$ and $h = (2^r + 1)(2^r \times P + 1)$
2.) Let $t$ be the maximal power of two such that $2^t | h - 1$
3.) If the set $S_t$ is non-empty and $\exists$ at least one $C_{t,z} \in S_t$ which is relatively prime to $h$, choose the $C_{t,z}$ with the smallest value of $z$ (i.e the smallest index) where $(C_{t,z}, h) = 1$ and $C_{t,z}$ has not been chosen previously at this node of the tree. We say that at this node the algorithm travels down branch $z$. Multiply $h$ by this $C_{t,z}$ and go back to step 2.
4.) If the set $S_t$ is empty, if $(C_{t,z}, h) \neq 1 \forall C_{t,z} \in S_t$, or if all $C_{t,z}$ have been chosen previously at this node of the tree, then define $B$ as $\max\{B, t\}$.
5.) Go back to the most recent node on the tree on the current path where $\exists$ multiple branches and not all of the branches have been traveled. If such a node does not exist then stop. Otherwise, let $t$ and $h$ be as they were when the algorithm arrived at this node.
6.) Go back to step 3.
4.2 Bounds for Maximal Powers of Two for Prime Factors of Carmichael Numbers

The proof that the algorithm actually generates a bound on maximal powers of 2 for prime divisors of Carmichael numbers depends upon the fact that the $C_{t,z}$’s are made up of primes whose powers of 2 are less than or equal to $t$. Lemma 2.2.3 and Corollary 2.2.4 demonstrate why we can make this assumption.

**Lemma 2.2.3:** Suppose the product

$$\prod_{i=1}^{u}(2^{k_i} \cdot D_i + 1) = 2^t \cdot D + 1$$

for some odd $D_1, D_2, ..., D_u, D$. If $k_u > t$ then

$$\prod_{i=1}^{u-1}(2^{k_i} \cdot D_i + 1) = 2^{t'} \cdot D' + 1$$

for some odd $D'$.

**Proof:** Write the product

$$\prod_{i=1}^{u-1}(2^{k_i} \cdot D_i + 1) = 2^{t'} \cdot D' + 1$$

for some odd $D'$. Then

$$(2^{t'} \cdot D' + 1)(2^{k_u} \cdot D_u + 1) = 2^t \cdot D + 1$$

But since $k_u > t$,

$$2^{t'} \cdot D' + 1 \equiv 2^t \cdot D + 1 \pmod{2^{t+1}}$$

which means that $t' = t$. ⊥

**Corollary 2.2.4:** Let
\[ E_t = 2^t \cdot D_t' + 1 = \prod_{i=1}^{u} (2^{k_i} \cdot D_i + 1) \]

where \( k_1 \leq k_2 \leq \ldots \leq k_u \). Then \( \exists E'_t, D''_t \) such that
\[
E'_t = 2^t \cdot D''_t + 1 = \left( \prod_{i=1}^{v} 2^{k_i} D_i + 1 \right)
\]

where \( v \leq u, k_v \leq t \).

**Proof:** If \( k_u > t \), we can rewrite this expression as the product of the first \( u - 1 \) terms by Lemma 2.2.3. This argument can be iterated until the maximal power of two is less than \( t \). ⊞

Using these results, we can show that if the algorithm terminates, then it finds an upper bound for the powers of 2 in the prime factors of Carmichael numbers.

**Theorem 2.2.5:** Let \( m \) be a Carmichael number with \( L = 2^k \cdot P \) for some prime \( P \). If the algorithm terminates for some minimal power \( r \), then \( k < B \).

**Proof:** If \( k = B \) then both \( 2^k + 1 \) and \( 2^k \cdot P + 1 \) are not prime (or else \( S_k \), the set of \( C_{t,z} \)'s for node \( k \), contains an element which is relatively prime to \( h_k \), contradicting the termination of the algorithm). But as in Lemma 2.2.3, this is impossible.

Now, assume that \( k > B \). Since \( r \) is a minimal power, \( 2^r + 1 \) and \( (2^r \cdot P + 1) | m \). So
\[
m = (2^r + 1)(2^r \cdot P + 1) \prod_{i \neq x} (2^{k_i} + 1) \prod_{j \neq y} (2^{l_j} \cdot P + 1)
\]
\[
= (2^t \cdot D_t + 1) \prod_{i \neq x} (2^{k_i} + 1) \prod_{j \neq y} (2^{l_j} \cdot P + 1)
\]

Clearly, \( t < B \) since \( t \) appears on one of the paths in our algorithm. Now, there must exist some combination of Type 1 and Type 2 primes such that the power of 2 for their product is \( t \); otherwise we multiply all remaining primes together to find that
for some odd integer \( D' \) and some integer \( t' \), where either \( t < t' \) and \( t < k \), or \( t' < t < k \), both of which contradict the minimal powers argument. So by Corollary 3.2.2 there exists a combination of Type 1 and Type 2 primes whose powers of two are greater than or equal to \( r \) and less than or equal to \( t \) such that their product has power of 2 equal to \( t \). So we multiply \( 2^t * D_t + 1 \) by this combination of Type 1 and 2 primes, giving us a new \( t \) where

\[
m = (2^t * D_t + 1)(2^{t'} * D' + 1)
\]

Now, since \( k > B > t \), we know that the set of remaining Type 1 and Type 2 primes is nonempty. So we can repeat this argument until we have a term with a power of 2 that caused the algorithm to terminate; call this power \( B' \). Clearly, \( B' < B \). So

\[
m = (2^{B'} * D_{B'} + 1) \cdot \prod_{\text{remaining } i's} (2^{k_i} + 1) \cdot \prod_{\text{remaining } j's} (2^{l_j} * P + 1)
\]

By the fact that the algorithm terminates, we know that there does not exist any combination of Type 1 and Type 2 primes such that the power of 2 of the product is \( B' \). Further, since we have only grouped terms whose powers of 2 are less than \( B' \) to this point and there must exist a Type 1 or Type 2 prime whose power of 2 is greater than \( B' \) (since \( k > B \geq B' \)), we know that the set of remaining Type 1 and Type 2 primes is nonempty. So we can multiply all remaining Type 1 and 2 primes together to find that

\[
m = (2^{B'} * D_{B'} + 1)(2^{t'} * D' + 1)
\]

for some odd integer \( D' \) and some integer \( t' \). Since \( B' \neq t' \), we know that either \( B' < t' \) and \( B' \leq B < k \) or \( t' < B' < k \), both of which contradict the minimal powers argument. Thus, \( k \) must be less than \( B \). \( \square \)
5 Carmichael Numbers with $L$ of the form $2^k \cdot P$ for $P \equiv 1 \pmod{3}$

Throughout this section, $P + 1$ will be expressed as $2^n \cdot q$ for some odd $q$ and some integer $n \geq 1$.

5.1 The Case $n$ is Odd

First, we establish a property about the powers of 2 associated with prime factors of $m$ if $P \equiv 1 \pmod{3}$.

Lemma 2.3.1: If $p = 2^f \cdot P + 1$ is prime for some $P \equiv 1 \pmod{3}$ then $f$ is even.

Proof: If $f$ is odd then

$$p = 2^f \cdot P + 1 \equiv 2 \cdot P + 1 \equiv 0 \pmod{3}.$$  

This result can be used to bound $r$, the minimal power of 2 for a prime factor of $m$:

Theorem 2.3.2: Let $m$ be a Carmichael number with $L = 2^k \cdot P$, where the prime $P \equiv 1 \pmod{3}$ and $P + 1 = 2^n \cdot q$. If $n$ is odd then $r < n$.

Proof: Assume that $n$ is odd and $r \geq n$. Clearly, $r \neq n$ since $2^n \cdot P + 1$ is not prime by the previous lemma. So $r > n$. Note that

$$(2^r + 1)(2^r \cdot P + 1) = (1 + 2^r)(1 - 2^r + 2^n r q)$$  

$$\equiv 1 + 2^{n+r} q \pmod{2^{n+r+1}}$$  

So

$$m = (2^{n+r+1}(q') + 2^{n+r} q + 1) \prod_i (2^{k_i} + 1) \prod_j (2^{l_j} P + 1)$$

where $q'$ is a positive integer and it is possible that one of the products is just 1.

Now, if $k_i, l_j > r + n \ \forall \ i, j$ then $r + n$ is a minimal
power of 2 which appears uniquely in the expression and \( r + n < k \), contradicting Theorem 1. Further, \( k_i, l_j \neq n + r \) \( \forall i, j \) since \( n + r \) is odd and greater than 2, implying that \( 3|2^{n+r} \times P + 1 \) (by Lemma 2.3.1) and \( 3|2^{n+r} + 1 \). So \( \exists k_i \) or \( l_j \) which is less than \( r + n \).

Since \( 2^r + 1 \) is prime, \( r \) is a power of 2. So \( r < k_i < r + n \) implies that \( r < k_i < 2r \), which means that \( k_i \) cannot be a power of 2, and hence \( 2^{ki} + 1 \) is not prime. So \( \exists \) minimal \( l_j \), denoted \( l_x \), such that \( r < l_x < r + n \). This gives us a minimal power of 2, which is a contradiction unless \( l_x \) is also the maximal power of 2. So \( m = (2^r + 1)(2^r \times P + 1)(2^k \times P + 1) \), which contradicts Corollary 2.1.4. Thus, \( r \) cannot be greater than \( n \).

**Corollary 2.3.3:** \( n \neq 1 \)

**Proof:** If \( n = 1 \) then \( r = 0 \), which means that \( 2^0 \times P + 1 = P + 1 \) must be prime. But this is a contradiction, since \( P + 1 \) is even and greater than 2.

**Corollary 2.3.4:** If \( P \equiv 1 \pmod{3} \) then \( P \equiv 3 \pmod{4} \) and hence \( P \equiv 7 \pmod{12} \).

**Proof:** If \( P \equiv 1 \pmod{4} \), then \( 2^n \times q = P + 1 = 2 \pmod{4} \), so that \( n = 1 \), which is impossible by Corollary 2.3.3.

### 5.2 The Case \( n \) is Even

In this section, we prove a weaker bound on \( r \) in the case that \( n \) is even.

**Theorem 2.3.5:** Let \( m \) be a Carmichael number with \( L = 2^k \times P \), where \( P \equiv 1 \pmod{3} \) and \( P + 1 = 2^n \times q \). If \( n \) is even and \( q \equiv 3 \pmod{4} \), then \( r \leq n \).

**Proof:** Assume that \( r > n \). We multiply the smallest
Type 1 and Type 2 prime factors together to find that

\[(2^r + 1)(2^r * P + 1) = (2^r + 1)(2^r * (2^n * q - 1) + 1)\]
\[= 2^{n+2r}q - 2^{2r} + 2^{n+r}q + 1\]
\[≡ 2^{n+r}q + 1 \pmod{2^{n+r+2}}\]

since \(r\) must be even, meaning that \(r > n\) implies \(2r \geq n + r + 2\). Thus

\[m = (2^{n+r+2} * q' + 2^{n+r} * q + 1) \prod_i (2^{k_i} + 1) \prod_j (2^{l_j} P + 1)\]

for some positive integer \(q'\), where it is possible that one of the products is just 1.

By the same reasoning as in Theorem 2.3.2, we can see that not all \(k_i, l_j\) can be greater than \(r + n\). Further, since \(r\) is a power of 2, \(r < k_i < r + n < 2r\) implies that \(k_i\) is not a power of 2, meaning that \(2^{k_i} + 1\) is not prime. So \(\exists\) a minimal Type 2 prime, with power of 2 denoted as \(l_x\), such that \(r < l_x \leq r + n\). Now, if \(l_x < r + n\) then \(l_x\) is the minimal power of 2 in the remaining equation, which means (by same argument as Theorem 2.3.2) that \(m\) is the product of 3 primes, where \(l_x\) is the maximal power of 2. But then \(\exists\) only one Type 1 prime divisor of \(m\), contradicting Corollary 2.1.4. So \(l_x = r + n\).

Given our third prime divisor of \(m\), we multiply it by the first two to find that

\[(2^{n+r+2} * q' + 2^{n+r} * q + 1)(2^{r+n} * (2^n * q - 1) + 1)\]
\[≡ 2^{n+r} * (q - 1) + 1 \pmod{2^{n+r+2}}\]

If \(q \equiv 3 \pmod{4}\), this is congruent to \(2^{n+r+1} + 1 \pmod{2^{n+r+2}}\). By the same process as before, we know that not all remaining primes can have powers of 2 greater than \(2^{n+r+1}\), and the fact that \(n + r + 1\) is odd and greater than 2 implies that no primes can have a power of 2 equal to \(n + r + 1\). But we assumed before that \(l_x\) was the minimal power, so \(\exists\) no other prime with power of 2 less than or equal to \(r + n + 1\). So \(m\) must again be the product of 3 primes, where \(l_x\) is the maximal power of 2. But then \(\exists\) only one Type 1 prime divisor of \(m\), contradicting Corollary 2.1.4. 因此。
5.3 \hspace{1cm} P = 127

The previous theorem can be immediately applied to two important examples. The simpler one is the case where \( P = 127 \).

**Theorem 2.3.6:** The only Carmichael number \( m \) with \( L = 2^k \cdot 127 \) is \( m = 5 \cdot 17 \cdot 257 \cdot 509 \).

**Proof:** First, \( 127 + 1 = 2^7 \), which, implies that the smallest power of 2 for any Carmichael number must be less than 7 by Theorem 2.3.2. Since \( P = 127 \equiv 1 \pmod{3} \), this means that the minimal power must be either 2 or 4. However, \( 19 \mid 2^4 \cdot 127 + 1 \). So \( r = 2 \) and hence 5 and \( 4 \cdot 127 + 1 = 509 \) are prime divisors of \( m \).

We use the algorithm to find that \( B = 9 \). Since there are 3 Fermat primes with powers greater than or equal to 2 and less than 9, and \( 5 \mid m \), we have three possible combinations of Fermat primes:

\[
\begin{align*}
5 \cdot 17 & \equiv 85 \pmod{127} \\
5 \cdot 257 & \equiv 14 \pmod{127} \\
5 \cdot 17 \cdot 257 & \equiv 1 \pmod{127}
\end{align*}
\]

Thus, by Lemma 2.1.3, only the last combination is possible, and \( k \geq 8 \). So

\[
m = 5 \cdot 17 \cdot 257 \cdot 509 \cdot \text{other primes}
\]

\[
= (2^9 \cdot 21717 + 1) \cdot \text{other primes}
\]

But \( 13 \mid 2^8 \cdot 127 + 1 \) and \( 3 \mid 2^9 \cdot 127 + 1 \). So any other prime with power of 2 less than 8 causes a minimal power of 2 less than \( k \), and any other prime factor with power of 2 greater than 9 will cause a minimal power of 2 of 9, which would have to be less than \( k \). Thus, the only possible combination of primes is \( m = 5 \cdot 17 \cdot 257 \cdot 509 \), which is known to be a Carmichael number. \( \blacksquare \)
Theorem 2.3.7: There exist exactly three Carmichael numbers with \( L = 2^k \cdot 7 \), namely

\[
\begin{align*}
m &= 5 \cdot 17 \cdot 29, \\
m &= 5 \cdot 17 \cdot 29 \cdot 113, \\
m &= 5 \cdot 29 \cdot 113 \cdot 65537 \cdot 114689.
\end{align*}
\]

Proof: First, since \( 7+1 = 2^3 \), \( r < 3 \) by Theorem 2.3.2. So \( r = 2 \) by Lemma 2.3.1. Thus, \( 5, 29|m \), and \( 5 \cdot 29 = 145 = 2^4 \cdot 9 + 1 \), which means that \( m = (2^4 \cdot 9 + 1)(\text{other primes}) \). Moreover, for \( r = 2 \), the algorithm yields \( B = 17 \).

Now, by lemma 2.1.3, the product of all Type 1 primes must be 1 (mod 7). But there are only 4 Fermat primes with powers of 2 greater than or equal to 2 and less than 17, and 5 must be included in any such combination of Fermat primes. Since \( m \) requires at least two Fermat primes, there are seven possible combinations:

\[
\begin{align*}
5 \cdot 17 &\equiv 1 \pmod{7} \\
5 \cdot 257 &\equiv 4 \pmod{7} \\
5 \cdot 65537 &\equiv 1 \pmod{7} \\
5 \cdot 17 \cdot 257 &\equiv 5 \pmod{7} \\
5 \cdot 17 \cdot 65537 &\equiv 3 \pmod{7} \\
5 \cdot 257 \cdot 65537 &\equiv 5 \pmod{7} \\
5 \cdot 17 \cdot 257 \cdot 65537 &\equiv 1 \pmod{7}
\end{align*}
\]

Of these, we need only consider the three which are 1 (mod 7).

Case 1: Suppose \( 17|m \); this handles the first and last cases. So

\[
\begin{align*}
m &= 5 \cdot 17 \cdot 29 \cdot (\text{other primes}) \\
\quad &= 2^5 \cdot 77 + 1
\end{align*}
\]

If \( k \geq 5 \) then there exists a prime with power of two equal to 5. But \( 5|2^5 \cdot 7 + 1 \) and \( 3|2^5 + 1 \), so no such prime exists, meaning that \( k < 5 \) and the only other possible prime
factor is $2^4 \cdot 7 + 1 = 113$. Thus, exactly two possible combinations exist, $m = 5 \cdot 17 \cdot 29$ and $m = 5 \cdot 17 \cdot 29 \cdot 113$, both of which are known to be Carmichael numbers.

**Case 2:** Now, we consider the case where 5 and 65537 are the only Type 1 factors. So

$$m = 5 \cdot 29 \cdot 65537 \cdot (\text{other primes})$$
$$= (2^4 \cdot 9 + 1)(2^{16} + 1)(\text{other primes})$$

Since $k > 4$, there exists a prime factor of $m$ with power of two equal to four. Further, since 17 is not a factor, we know that $2^4 \cdot 7 + 1 = 113 | m$. So

$$m = 5 \cdot 29 \cdot 113 \cdot 65537 \cdot (\text{other primes})$$
$$= (2^{14} + 1)(2^{16} + 1)(\text{other primes})$$

Again, since $k > 14$, $m$ must have a prime factor with power of two equal to 14. So $2^{14} \cdot 7 + 1 = 114689 | m$, which implies that

$$m = 5 \cdot 29 \cdot 113 \cdot 114689 \cdot 65537 \cdot (\text{other primes})$$
$$= (2^{17} \cdot 14337 + 1)(2^{16} + 1)(\text{other primes}).$$

Now, $79 | 2^{16} \cdot 7 + 1$ and $11 | 2^8 \cdot 7 + 1$, so every power of two greater than 4 and less than 17 is unique (i.e. each prime factor of $m$ must have a different power of two). Thus, multiplying this expression by another prime with power of two less than 17 gives us a unique minimal power of two, contradicting Theorem 1. But we cannot have a power of two greater than or equal to $B = 17$ by Theorem 2.2.5. Moreover, $k \geq 16$ since $2^{16} + 1 = 65537 | m$. So $k = 16$ is the only option and hence the only possibility is $m = 5 \cdot 29 \cdot 113 \cdot 114689 \cdot 65537$, which is known to be a Carmichael number. $\Box$
6 The Special Case $P = 3$

6.1 A Bound on the Minimal Power

In order to deal with the case $P = 3$, we first find the minimal power of two for prime factors of the Carmichael number $m$ and then examine several special cases.

First, by examining prime factors modulo 7, we can eliminate the powers of 2 which are 1 modulo 3.

**Lemma 2.4.1**: If $p = 2f \times 3 + 1$ is prime and $f > 1$ then $f \not\equiv 1 \pmod{3}$.

**Proof**: Note that $2^3 \equiv 1 \pmod{7}$. So if $f \equiv 1 \pmod{3}$ then $2^f \equiv 2 \pmod{7}$, which means that $2^f \times 3 + 1 \equiv 2 \times 3 + 1 \equiv 0 \pmod{7}$.

But if $f > 1$ then $p > 7$ and $7|p$, so $p$ is not prime.  

Using this, we can determine the value for $r$ when $P = 3$:

**Theorem 2.4.2**: Let $m$ be a Carmichael number with $L = 2^k \times 3$. Then $r = 2$, so that $5 \times 13|m$.

**Proof**: First, if $r = 1$ then $3|m$, contradicting the fact that that $L|m - 1$. Now, assume $r > 2$. Since $r$ must be the power of two for a Fermat prime, $r = 2^a$ for some $a$. This implies that $r \not\equiv 0 \pmod{3}$. Further, by Lemma 2.4.1, $r \not\equiv 1 \pmod{3}$. So $r \equiv 2 \pmod{3}$. So

$$m = (2^r + 1)(2^r \times 3 + 1) \prod (2^{ki} + 1) \prod (2^{lj} \times 3 + 1) = (2^{2r} \times 3 + 2^{r+2} + 1) \prod (2^{ki} + 1) \prod (2^{lj} \times 3 + 1).$$

By the minimal powers argument, we know that if $k > r+2$ then $\exists k_i$ or $l_j$ which equals $r+2$. Since we assume $r > 2$, and $r = 2^a$ for some $a > 1$, and thus $r + 2 \not= 2^b$ for any $b \in \mathbb{Z}$. So $k_i \not= r + 2 \forall i$, which means that $\exists l_j$ such that $l_j = r + 2$. But if $r \equiv 2 \pmod{3}$ then $r + 2 \equiv 1 \pmod{3}$, which means by Lemma 2.4.1 that $2^{l_j} \times 3 + 1$ is
not prime. Thus, \( k \leq r + 2 \). But by definition of \( r \), we know that all other prime factors must have powers of 2 greater than \( r \) and less than \( r+2 \). In particular, \( \exists \) only one possible Type 1 prime factor of \( m \), contradicting Lemma 2.1.3. Thus, \( r = 2 \), and hence 5 and 13|\( m \). □

### 6.2 Finding All Carmichael Numbers with \( L = 2^k \cdot 3 \)

We can now find all Carmichael numbers with \( L = 2^k \cdot 3 \); there are exactly three.

**Theorem 2.4.3:** Let \( m \) be a Carmichael number with \( L = 2^k \cdot 3 \). Then one of the following is true:

\[
\begin{align*}
m &= 5 \cdot 13 \cdot 17, \\
m &= 5 \cdot 13 \cdot 193 \cdot 257, \\
m &= 5 \cdot 13 \cdot 193 \cdot 257 \cdot 769.
\end{align*}
\]

**Proof:** Since \( r = 2 \) by Theorem 2.4.2, the minimal Type 1 prime must be 5. From the algorithm, \( B = 10 \). So we examine all combinations of Type 1 primes with powers of 2 greater than or equal to 2 and less than 10 which are congruent to 1 (mod 3); there are two such combinations, \( 5 \cdot 17 \) and \( 5 \cdot 257 \).

**Case 1:** If \( 17 \mid m \), then \( 5 \cdot 13 \cdot 17 = 2^4 \cdot 69 + 1 \), so that

\[
m = (2^4 \cdot 69 + 1) \cdot (\text{other primes}).
\]

But \( 5 \mid 2^4 \cdot 3 + 1 \) and \( 7 \mid 2^4 \cdot 3 + 1 \). So there any other Type 1 or 2 primes with powers of two \( \geq 2 \) and \( \leq 4 \). So 4 must be a unique minimal power of two. So \( k \leq 4 \). Since there exist no other possible prime factors with powers of \( \leq 4 \), \( m = 5 \cdot 13 \cdot 17 \) is the only possible combination and is, in fact, known to be a Carmichael number.

**Case 2:** If \( 257 \mid m \), then \( 5 \cdot 13 \cdot 257 = (2^6 + 1)(2^8 + 1) \), and \( k \geq 8 \). Again, we know that \( B = 10 \). Since \( 17 \nmid m \), \( \exists \) only
three other possible prime factors: $2^5 \cdot 3 + 1$, $2^6 \cdot 3 + 1$, and $2^8 \cdot 3 + 1$.

Now, $2^6 \cdot 261 + 1$ times either or both of the latter two factors will yield a product with power of two $\geq 6$. So if $2^5 \cdot 3 + 1 | m$ then

$$m = (2^6 \cdot 261 + 1)(2^5 \cdot 3 + 1)(\text{any combination of the remaining primes})$$

$$= (2^5 \cdot 3 + 1)(2^6 \cdot D_x + 1)$$

where $D_x \in \mathbb{Z}$. But then 5 is a minimal power of two and $5 < 8 \leq k$. So $2^5 \cdot 3 + 1 \nmid m$. Moreover,

$$5 \cdot 13 \cdot 257 = (2^6 + 1)(2^8 + 1)$$

and

$$5 \cdot 13 \cdot 257 \cdot 769 = (2^6 + 1)(2^8 + 1)(2^8 \cdot 3 + 1)$$

are not Carmichael numbers, since 6 is a unique minimal power and $k = 8$. So we are left with only two possible combinations of primes, $m = 5 \cdot 13 \cdot 193 \cdot 257$ and $m = 5 \cdot 13 \cdot 193 \cdot 257 \cdot 769$, both of which are known to be Carmichael numbers. □

7 General Results about $P$

7.1 $7 < P < 127$ Is Impossible

In a table of the first 150 Carmichael numbers, there are only a few Carmichael numbers where $L$ is of the form $2^k \cdot P$ for some odd prime $P$. Of those which do fit this form, however, all have $P \leq 7$ or $P = 127$. In fact, it can be proven that $7 < P < 127$ is impossible:

**Theorem 2.5.1:** Let $P$ be an odd prime such that $7 < P < 127$. Then there exist no Carmichael numbers with $L = 2^k \cdot P$.

**Proof:** By Corollary 2.2.7, this theorem is true for $P \equiv 2 \pmod{3}$, and from Corollary 2.3.4, we know that $P \equiv 1$
(mod 3) implies that \( P \equiv 7 \) (mod 12). So the only possibilities are \( P = 19, 31, 43, 67, 79, \) and 103.

**Case 1: n is odd** (\( P = 31, 103 \))\( n \) is odd (\( P = 31, 103 \)): In the case of 31, 31 = \( 2^5 - 1 \). So \( r < 5 \) by Theorem 2.3.2. But neither \( 2^2 * 31 + 1 = 125 \) nor \( 2^4 * 31 + 1 = 497 = 7 * 71 \) is prime, so \( r \) cannot equal 2 or 4. Thus \( P \neq 31 \).

Similarly, 103 = \( 2^3 * 13 - 1 \). So \( r < 3 \) by Theorem 2.3.2. But \( 2^2 * 103 + 1 = 413 = 7 * 59 \) is not prime, so \( r \neq 2 \). Thus \( P \neq 103 \).

**Case 2:** \( P \equiv 4 \) (mod 5) (\( P = 19, 79 \)) First, we know that for \( r \geq 4 \), we have \( 4 \mid r \), since \( r \) is a power of two. But then \( \forall r \geq 4 \),

\[
2^r * P + 1 \equiv 0 \pmod{5}
\]

(since \( P \equiv 4 \) (mod 5)), which means that \( 5 \mid 2^r * P + 1 \) and contradicts that \( 2^r * P + 1 \) is a prime divisor of \( m \). So if \( P \equiv 4 \) (mod 5) then \( r < 4 \), which means that \( r = 2 \).

Now, in the case of 19, \( 2^2 * 19 + 1 = 77 = 7 * 11 \), which means that \( r = 2 \) is not possible. So \( P \neq 19 \).

In the case of 79, the algorithm tells us that if \( r = 2 \) then \( B = 6 \). But the only combination of at least two Fermat primes less than \( 2^6 \) and greater than \( 2^2 \) which contain 5 is \( 5 * 17 \equiv 6 \) (mod 79).

**Case 3:** \( P \equiv 16 \) (mod 17) (\( P = 67 \)): First, \( \forall r > 8 \), we know that \( 8 \mid r \), since \( r \) is a power of two. So for \( P \equiv 16 \) (mod 17), \( \forall r \geq 8 \),

\[
2^r * P + 1 \equiv 0 \pmod{17},
\]

(since the order of 2 is 8 (mod 17)) which means that \( 17 \mid 2^r * P + 1 \) and thus \( 2^r * P + 1 \) is not prime. So if \( P \equiv 16 \) (mod 17) then \( r < 8 \), which means that \( r = 2 \) or 4. Now, \( 2^4 * 67 + 1 = 1073 = 29 * 37 \) is not prime, which means that \( r \neq 4 \). Further, for \( r = 2 \), the algorithm gives us 9. But the only combinations of at least two Fermat primes
less than $2^0$ and greater than $2^2$ which contain 5 are $5 \times 17$, $5 \times 257$, and $5 \times 17 \times 257$, none of which are $1 \equiv 0 \pmod{67}$.

**Case 4**: $P = 43$: By Theorem 2.3.5, we know that $r \leq n$. Since $n = 2$, $r = 2$. In this case, $B = 5$ (which terminates the algorithm), meaning that the product of the two Fermat primes which divide $m$ is $5 \times 17 \equiv 42 \pmod{43}$. 

8 Carmichael Numbers with Known Fermat Prime Factors

The aim of this section is to prove that the Carmichael numbers found thus far with $L = 2^k \times P$ are the only ones possible where all Type 1 primes are among the known Fermat primes.

**Theorem 2.6.1**: Let $m$ be a Carmichael number with $L = 2^k \times P$ and all Type 1 prime factors are among the five known Fermat primes. Then $m$ is one of the eight Carmichael numbers with $P = 3, 5, 7, \text{ or } 127$.

**Proof**: Recall that Theorem 2.2.5 proved the case where $P \equiv 2 \pmod{3}$ and Theorem 2.4.3 dealt with the case of $P = 3$; thus, we need only consider the cases where $P \equiv 1 \pmod{3}$.

Now, recall from Lemma 2.1.3 and Corollary 2.1.4 that any Carmichael number with $L = 2^k \times P$ must have at least two Fermat prime divisors, and the product of the Fermat primes must be $1 \pmod{P}$. This means that, if $P$ is as required, there must exist a product $R$ of Fermat primes such that $P | R - 1$. Additionally, since $P \equiv 1 \pmod{3}$, the minimal power of two is even, so we can ignore any product which includes 3.

The 11 remaining possible $R$’s are on Table 1. By Theorem 2.5.1, we can ignore any $P \leq 127$. Since $P \equiv 1 \pmod{3}$, this leaves us with only 3 choices for $P$: 151, 331, and
Now, from Table 1, if $P = 151$ or $331$ then $R = 5 \times 17 \times 257 \times 65537$. Thus, the minimal power of two for $m$ must be 2. But $2^2 \times 151 + 1 = 605$ and $32^2 \times 3312 + 1 = 1325$, neither of which is prime. Further, if $P = 241$ then $R = 257 \times 65537$, which means that the minimal power of two in $m$ is 8. But $2^8 \times 241 + 1 = 61697 = 103 \times 599$. Thus, $P \not> 127$. ⊞

The list of Carmichael numbers where $L = 2^k \times P$ and all Type 1 primes are among the known Fermat primes appears in Table 3. From this we find an immediate corollary:

**Corollary 2.6.2** A Carmichael number cannot have the form $2^s \times P + 1$ for an odd prime $P$ and integer $s$ if all Type 1 prime divisors are among the known Fermat primes.

**Proof** Follows from the fact that $L|m - 1$. ⊞

**A Tables**

A.1 Table 1: Prime Divisors for Combinations of Known Fermat Primes

A.2 Table 2: Termination of the Algorithm for $P \equiv 2 \pmod{3}$ and $P \leq 127$

A.3 Table 3: Carmichael Numbers with Known Fermat Primes

**References**

