An Investigation of Erdös' Method: A Scheme for Generating Carmichael Numbers

By: Trevor Brennan

Advisor: John Greene

Contents

Chapter 1: Introduction…………………………………………………….……1

Chapter 2: Number and Group Theory Principles……………………………..…7

Chapter 3: Constructions Related to the set P………………………………….18

Chapter 4: Appendix: Tables, Data and Conclusions…………………………..31

References…………………………………………………………………47

Annotated Code…………………………………………………………..48

Chapter 1

Introduction

Number Theory is a field of mathematics primarily concerned with the study of the positive integers, which are divided into three disjoint sets; the unity 1, the primes 2, 3, 5, 7, 11,… and the composites 4, 6, 8, 9, 10, …. A fundamental problem in Number Theory is to determine whether a large number is prime or composite. Proving primality can be a difficult task, but showing that a number is composite can be less complicated. A compositeness test is a test that will not determine if a number is prime, but can identify most composites. For example, $\frac{2}{3}$ of all composite numbers are divisible by 2 or by 3. So, one compositeness test is to check if n is even or divisible by 3 (for this particular test $n \neq 2, 3$). If either is true then we know n is composite. If not true then we do not know if n is prime. A more sophisticated test is a consequence of the following theorem.

Fermat's Little Theorem

If p is prime and a is any integer, then $a^p - a$ is divisible by p.

To illustrate the theorem, let $a = 2$ and $p = 7$ then $2^7 - 2 = 126 = 18 * 7$ which is divisible by our prime 7. We could also try $a = 3$ and $p = 5$ then $3^5 - 3 = 240 = 2^4 * 3 * 5$ which is divisible by 5. What happens in the case of a composite number n, say $n = 3 * 5 = 15$? With $a = 2$ this gives $2^{15} - 2 = 32{,}766$ which gives a remainder of 6 when divided by 15. We say 15 fails Fermat's primality test, indicating that 15 is composite. To clarify, when n is a composite number we would not expect it to divide $a^n - a$ for most integer$s$ a.

The vast majority of composite numbers will be detected by Fermat's test. However, for certain composite numbers Fermat's test will be satisfied. For example, suppose we have $341 = 11 * 31$ then $2^{341} - 2$ is divisible by 341. Since $2^{341} - 2$ is a 103 digit number, we use a trick to show that it is divisible by 341. We know that $x^k - 1$ has $x - 1$ as a factor. As a consequence, $x^{km} - 1$ is divisible by $x^m - 1$. For our example we have, $2^{341} - 2 = 2(2^{340} - 1)$. It is apparent that with $x = 2$, $2^{10} - 1$ divides $2^{340} - 1$. Since $2^{10} - 1 = 1023 = 3 * 341$ we see that 341 satisfies Fermat's test for $a = 2$.

For a second example, consider the composite number $121 = 11 * 11$. Then $3^{121} - 3$ is divisible by 121. We can use the same method as above: $3^{121} - 3 = 3(3^{120} - 1)$ and $3^5 - 1 = 242 = 2 * 121$ divides $3^{120} - 1$ and thus 121 satisfies Fermat's test. Both numbers $n = 341$ and $n = 121$ pass Fermat's test as if they were primes, at least for $a = 2$ and $a = 3$, respectively. That is, if we were unaware that 341 or 121 were composite we might guess they were prime. Yet, for these examples it would require that we were unwilling to test other integers a.

When the number $a^n - a$ is divisible by n it is highly probable that n is a prime. When numbers that satisfy this condition are unknown to be prime or composite we refer to them as *probable primes*. If we know n is composite but n divides $a^n - a$ for some a, we call n a *pseudoprime* [7, pp.144-146]. So, 341 is a base 2 pseudoprime and 121 is a base 3 pseudoprime. There are only 245 base 2 pseudoprimes $< 10^6$, but there are 78,498 primes $< 10^6$. So, 78,743 numbers pass the Fermat test base-2 and all but 245 of them are prime. Therefore, we label as a probable prime any number which satisfies Fermat's little theorem and is not known to be prime.

Given that 341 is a base 2 pseudoprime, is it also a base 3 pseudoprime? Doing the calculations we see that, $3^{341} - 3$ has a remainder of 165 when divided by 341. Even though 341 is a base 2 psuedoprime it is not a base 3 pseudoprime since, $3^{341} - 3$ is not divisible by 341 and fails Fermat's test. So, with a little more effort we can dismiss 341 as being prime and conclude that it is indeed composite. This raises the question; do pseudoprimes exist that satisfy Fermat's test for any base b? If they do exist, what properties would they satisfy, and how many of them are there?

The numbers in question are called Carmichael numbers. They are addressed in many Number Theory textbooks. Because of this, while studying Number Theory for the first time one often comes into contact with Carmichael numbers. This is especially interesting when you consider they were discovered just over a century ago, even though Number Theory is thousands of years old.

Carmichael numbers are sometimes referred to as absolute pseudoprimes. A Carmichael number is not just a base 2 or base 3 pseudoprime, it will satisfy Fermat's test for any base. Which is to say, a Carmichael number is a pseudoprime to infinitely many bases, or a composite natural number n such that $a^n - a$ is divisible by n for any integer a. Robert Carmichael was the first to discover such numbers and they were named in his honor [2, p.133]. Formally, a Carmichael number is a positive odd composite number that satisfies Fermat's Little Theorem. As an example, $561 = 3 * 11 * 17$ is a Carmichael number. That is, $a^{561} - a$ is divisible by 561 for any integer a. In fact, 561 is the smallest Carmichael number.

In a paper written in 1956 Paul Erdös devised a method for calculating large numbers of Carmichael numbers [3]. His method was originally intended to estimate the number of Carmichael numbers below a certain bound. A modification of the method is as follows:

Erdös' Method

Let m be a highly composite number. That is let m be a number with lots of divisors. For example, we might use $m = lcm(1, 2, \dots, n)$ for some integer n. Let P be the set of primes $P = \{p \mid p\ does\ not\ divide\ m\ but\ p - 1\ does\ divide\ m\}$. Then if S is any subset of P for which $\prod_{p \in S} p$ has remainder 1 when divided by m and $|S| > 2$, then $\prod_{p \in S} p$ is a Carmichael number.

Example 1

Let $m = 2 * 2 * 3 * 3 = 36$. To find the set P we first find all divisors of 36;

$$\{1, 2, 3, 4, 6, 9, 12, 18, 36\},$$

and add 1 to them,

$$\{2, 3, 4, 5, 7, 10, 13, 19, 37\}.$$

This gives us a possible set P, since we are looking for primes such that $p - 1$ divides m. To get our set P we now remove any non-primes and those primes which divide m. We discard 2 and 3 since they are primes that divide 36, also 4 and 10 are composites so we also remove them,

$$\{\cancel{2}, \cancel{3}, \cancel{4}, 5, 7, \cancel{10}, 13, 19, 37\}.$$

This leaves us with our set P,

$$P = \{5, 7, 13, 19, 37\}.$$

To find the Carmichael numbers from this set we find any subset that gives a remainder of 1 when we divide $\prod_{p\in S} p$ by 36. Below we calculate all 32 subset products of P and find their remainders after dividing by 36.

Subset	**Subset Product**	**Remainder**
$\emptyset$	1	1
{5}	5	5
{7}	7	7
{13}	13	13
{19}	19	19
{37}	37	1
{5, 7}	35	35
{5, 13}	65	29
{5, 19}	95	23
{5, 37}	185	5
{7, 13}	91	19
{7, 19}	133	25
{7, 37}	259	7
{13, 19}	247	31
{13, 37}	481	13
{19, 37}	703	19
{5, 7, 13}	455	23
{5, 7, 19}	665	17
{5, 7, 37}	1295	35
{5, 13, 19}	1235	11
{5, 13, 37}	2405	29
{5, 19, 37}	3515	23
{7, 13, 19}	1729	1
{7, 13, 37}	3367	19
{7, 19, 37}	4921	25
{13, 19, 37}	9139	31
{5, 7, 13, 19}	8645	5
{5, 7, 13, 37}	16835	23
{5, 7, 19, 37}	24605	17
{5, 13, 19, 37}	45695	11
{7, 13, 19, 37}	63973	1
{5, 7, 13, 19, 37}	319865	5

Table 1.1

From Table 1.1 the following subsets have products with remainder 1 when divided by 36: $\emptyset, \{37\}, \{7, 13, 19\}, \{7, 13, 19, 37\}$. From these subsets we find the Carmichael numbers. We might expect each subset product to produce a Carmichael number, but this is not the case. We only get Carmichael numbers from the last two subsets once we take their products. That is, $7 * 13 * 19 = 1729$ and $7 * 13 * 19 * 37 = 63{,}973$ are Carmichael numbers, but the empty set and 37 are not. So, $a^{1729} - a$ is divisible by 1729 and $a^{63{,}973} - a$ is divisible by $63{,}973$ for any integer a. For now it is worth noting that Erdös' method produces Carmichael numbers. In the subsequent chapters we will show why this method works and how well it produces large numbers of Carmichael numbers. Also, we will provide some interesting properties and theorems that we have discovered from examining this method.

Erdös' Method is based on the hope that subset products are distributed roughly uniformly among the possible remainders when we divide by m. Not all remainders can occur. For example, when any product of odd numbers is divided by 36, the remainder must be odd. It turns out that for 36, there are only 12 possible remainders: $1, 5, 7, 11,$ $13, 17, 19, 23, 25, 29, 31, 35$. There are $2^5 = 32$ possible subsets of P. Thus, if the remainders were evenly distributed over the 12 possibilities, we would expect to get $\frac{32}{12} \sim 2.67$ occurences of each remainder. Counting how many times each remainder occurs for $m = 36$ we have the following table:

Residue	**Count**
1	4
5	4
7	2
11	2
13	2
17	2
19	4
23	4
25	2
29	2
31	2
35	2

Table 1.2

Under the count column the number 4 occurred 4 times. This means that 4 remainders each occurred 4 times as subset products of P. The remainders that occurred 4 times are $1, 5, 19, 23$ and each occurred 4 times in Table 1.1. If we reference Table 1.1 we can see all the subsets that resulted in each of these remainders, which was how we made Table 1.2. In addition, we can count how many times each remainder occurred 2 times. Under the count column 8 remainders were counted 2 times as subset products of P. These remainders are $7, 11, 13, 17, 25, 29, 31, 35$ and each occurred 2 times in Table 1.1.

We expected to find each remainder 2.67 times and we were not far off with remainders occurring either 4 times or 2 times. While $m = 36$ is a small example we are still following near a uniform distribution. We also might have expected to find more than two Carmichael numbers but not many more. This particular example was especially small, it is the smallest number m where we get Carmichael numbers by Erdös' method. This raises the question, what happens with larger m?

In this project we investigate the question of how the subset products are distributed among the possible remainders when dividing by m. In particular, how many times does each remainder occur? Are there any underlying behaviors or properties we can establish? Ascertaining how many times each remainder occurs will give a lower bound for how many Carmichael numbers we can expect for m above a certain bound.

In the subsequent chapters many more theorems and definitions will be introduced. We will describe in greater detail how each contributes to this project and how they all tie together to create some very interesting mathematics.

Chapter 2

Number and Group Theory Principles

As this is a Number Theory project it will require the use of several properties and theorems that are fundamental to this branch. Some of these have already been used and if problematic before will hopefully be apparent after the following chapter. Many of these definitions and theorems will provide motivation for further definitions and theorems. We will begin with a basic idea, the greatest common divisor of two integers.

The Greatest Common Divisor (GCD)

The greatest common divisor of two integers m and n is the largest integer d with the property that both m and n are divisible by d. This is written as $gcd(m,n)$ or often just (m,n) [7, p.118].

For example, suppose we have the integers 36 and 20 then the divisors of 36 are {1, 2, 3, 4, 6, 9, 12, 18, 36} and the divisors of 20 are {1, 2, 4, 5, 10, 20}. The largest common element being 4, therefore $(36, 20) = 4$. This says 4 is the largest integer that divides both 36 and 20.

If we have two integers a and b such that $(a, b) = 1$ we say these two integers are *relatively prime* [6, p.32]. For example, $(14, 9) = 1$ since 14 and 9 have no common divisors except 1.

Reduced Residue

A reduced residue is a positive integer less than n but relatively prime to n [6, p.53].

We will be using reduced residues repeatedly throughout this paper and it is important to be familiar with this definition. Also, it will be crucial to know the number of reduced residues of a particular number m. Fortunately, we have a function to designate the number of reduced residues.

Euler's Totient Function

$\varphi(n)$ is the number of positive integers less than n which are relatively prime to n [6, p.53]. For $n = 1$ we define $\varphi(1) = 1$.

For example, if we let $n = 14$ then the reduced residues are $\{1, 3, 5, 9, 11, 13\}$. There are 6 of these, so $\varphi(14) = 6$. It is not very easy to calculate all the reduced residues for any particular n, let alone count them. Fortunately we have a formula for $\varphi(n)$.

Formula for $\boldsymbol{\varphi(n)}$

If $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, then $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$ [6, p.54].

For example, the primes dividing 180 are $2, 3, 5$ so,

$$\varphi(180) = 180\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 48.$$

The idea of congruence (denoted ≡) is essential for our discussion of reduced residues. This symbol should not be confused with equality.

Definition of Congruence

We say $a \equiv b(mod\ m)$ (read "a is congruent to b modulo m") if $a - b$ is divisible by m [7, p.121].

We have $2^5 \equiv 2(mod\ 5)$ because $2^5 - 2 = 32 - 2 = 30$, which is divisible by 5. Along with this definition we provide the different properties of operations we will be using with modular arithmetic.

Properties of Modular Arithmetic

Let $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$ [6, p.p.48-50]. Then,

1.) $a + c \equiv b + d(mod\ m)$

2.) $ac \equiv bd(mod\ m)$

3.) For any $n > 0$, $a^n \equiv b^n(mod\ m)$.

4.) If $(m, n) = 1$ and $xn \equiv yn(mod\ m)$, then $x \equiv y(mod\ m)$.

Suppose we were to find the product of two reduced residues of a number m. Once reducing modulo m, will we produce a new reduced residue? In fact, we will always return to a reduced residue while performing such operations. To see this, let $a, b, m \in Z$ where $(a, m) = (b, m) = 1$, and $ab \equiv r(mod\ m)$ where $0 \leq r < m$, if r is not relatively prime to m then for some prime p, $p|r$ and $p|m$. Now $ab = r + km$ for some integer k, so $p|ab$. This implies either $p|a$ or $p|b$ but then $(a, m) \neq 1$ or $(b, m) \neq 1$. Therefore, if $(a, m) = (b, m) = 1$ then $(ab, m) = 1$. In other words, once ab is reduced modulo m it is a reduced residue.

How many times can we multiply a reduced residue by itself, while reducing modulo m before we return to the same reduced residue? This property of reduced residues is essential to the ensuing material and it is the subject of the next definition.

Definition of Order Modulo m

The order modulo m of the reduced residue r is the smallest positive integer n where $r^n \equiv 1 \ (mod\ m)$ [6, p.55]. This is often denoted as $|r| = n$.

For example, let $m = 10$ then the residue classes of $x(mod\ m)$ are $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and the reduced residues are $\{1, 3, 7, 9\}$. To find the orders we begin multiplying the reduced residues by themselves. Since, $1 \equiv 1 \ (mod\ 10)$ it has order 1. Trying a more interesting reduced residue, $3^2 \equiv 9(mod\ 10)$, $3^3 \equiv 7(mod\ 10)$ and $3^4 \equiv 1(mod\ 10)$. Thus, 3 has order 4 modulo 10. In entirety the orders of $\{1, 3, 7, 9\}$ are respectively $\{1, 4, 4, 2\}$.

With the definition of congruence and order understood we now can begin to introduce some group theory. A *group* [4, p.p. 42-46] is a nonempty set with an associative operation such that; an identity exists, each element has an inverse and the set is closed under the group operation.

Multiplicative Group of Integers Modulo n

For $n > 1$, the multiplicative group of integers modulo n is as follows, $U(n) = \{k \mid 1 \leq k < n \ with\ gcd(k, n) = 1\}$.

A *cyclic group* [4, p.p.73-77] is a group G with element a such that $G = \{a^n \mid n \in \mathrm{Z}\}$. Here a is called a *generator* of G, that is each element in G is a multiple of a. For certain n, $U(n)$ will always produce a cyclic group.

$U(n)$ is Cyclic for particular n

For $n = 2, 4, p^k, 2p^k$ where p is an odd prime and k is an integer, we have that $U(n)$ is a cyclic group and has a generator [6, p.82].

For example, suppose $n = 7$ then $U(7) = \{1, 2, 3, 4, 5, 6\}$. Since n is prime this is a cyclic group with generator 3. We can see that it is the generator of the group since, $3^1 \equiv 3(mod\ 7)$, $3^2 \equiv 2(mod\ 7)$, $3^3 \equiv 6(mod\ 7)$, $3^4 \equiv 4(mod\ 7)$, $3^5 \equiv 5(mod\ 7)$ and $3^6 \equiv 1(mod\ 7)$.

In any cyclic group if we continually multiply by the generator we will eventually cycle through all group elements and return to where we began. The following property describes an instance of this particular situation and will be necessary for the proof of further statements.

$a^k \equiv 1$ implies that $|a|$ divides k

Let G be a group and let a be an element of order n in G. If $a^k \equiv 1$, then n divides k [4, p.p.74-75].

We now rephrase the definition of Fermat's Little Theorem in terms of congruence.

Congruence Form of Fermat's Little Theorem

If p is prime and a is any integer, then $a^p \equiv a\ (mod\ p)$. If $p \nmid a$ then $a^{p-1} \equiv 1\ (mod\ p)$ [6, p.55] (the symbol $\nmid$ means does not divide).

We have used the preceding theorem throughout the paper and it is worth remembering both versions as we carry on the discussion of Erdös' method. The following theorem is a generalization of Fermat's little theorem.

Euler's Theorem

If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1(mod\ n)$. Where $\varphi(n)$ is Euler's Totient Function [6, p.55].

From Euler's Theorem we are guaranteed that reduced residues will have an order modulo n.

With the set P of Erdös' method we want to find all subset products and then reduce modulo m. For the number of times we will be doing this operation it is important that we have a function to denote it.

Function f

This function gives the products of any set of numbers. If A is any set of numbers, then

$$f(A) = \prod_{x \in A} x$$

Function F

Using $f(A)$ from above let $F(A)$ be the least residue of $f(A)$ modulo m. That is, $F(A) \equiv f(A)(mod\ m)$ and $0 \leq F(A) < m$.

Using these functions we will be performing various operations. One that will often be used in our theorems is that of the symmetric difference.

Symmetric Difference

For sets A and B the symmetric difference is the set containing those elements in either A or B, but not both A and B. We will denote this by $A \oplus B$ (the symmetric difference of A and B), so $A \oplus B = A \cup B - A \cap B$.

Suppose we have two sets $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 6\}$ then $A \oplus B = \{1, 2, 5, 6\}$. We exclude the 3 and 4 since they are in both sets. The symmetric difference will for our purposes primarily be used with our newly defined functions.

From the definition of the symmetric difference we can derive a useful formula for f. Using the sets from above consider $f(A \oplus B) = 1 * 2 * 5 * 6 = 60$. The following lemma provides a formula for this operation.

Lemma 2.1

If A and B are disjoint, $f(A \oplus B) = f(A)f(B)$.

This is obvious. For the function F we get a similar definition with a slight difference. We will interpret F as acting on $U(m)$, so we will say $F(A \oplus B) = F(A)F(B)$, but recognize that its product is in $U(m)$. That is, $0 \leq F(A)F(B) < m$.

Lemma 2.2

$f(A \oplus B) = f(A)f(B)f(A \cap B)^{-2}$

Proof

If we denote the *complement* of a set A as $\bar{A}$ then for any sets A and B we have $A \oplus B = (A \cap \bar{B}) \cup (\bar{A} \cap B)$, which is a union of disjoint sets. So $f(A \oplus B) = f(A \cap \bar{B}) * f(\bar{A} \cap B)$. Finally, $A = (A \cap \bar{B}) \cup (A \cap B)$, again the union of disjoint sets. So $f(A) = f(A \cap \bar{B}) * f(A \cap B)$ which implies $f(A \cap \bar{B}) = f(A)f(A \cap B)^{-1}$. Thus, we combine these to get $f(A \oplus B) = f(A \cap \bar{B}) * f(\bar{A} \cap B) = f(A)f(B)f(A \cap B)^{-2}$.■

This formula gives the product of all the elements in A and B excluding anything that occurs in both. Doing the calculations for the sets A and B from our examples above we have,

$$\begin{aligned} f(A)f(B)f(A \cap B)^{-2} &= (1 * 2 * 3 * 4)(3 * 4 * 5 * 6)(3 * 4)^{-2} \\ &= \frac{1*2*3*4}{3*4} * \frac{3*4*5*6}{3*4} \\ &= 1 * 2 * 5 * 6 \\ &= f(A \oplus B) \end{aligned}$$

With an understanding of the symmetric difference we will now introduce some group properties associated with this new operation, but first we introduce a new set.

Power Set of a Set

The set of all subsets of a set is the power set.

Given a set X, let G be the power set of X. Then G is a group with respect to the symmetric difference operator. For $A, B \in G$ we have closure, $A \oplus B = (A \cap \bar{B}) \cup (\bar{A} \cap B) \subseteq A \cup B \subseteq G$. The identity is $e = \emptyset$ since $A \oplus e = A \oplus \emptyset = A$. Inverses exist since for each element in G we have $A \oplus A = \emptyset = e$, i.e. each element is its own inverse. Finally, the symmetric difference is associative: $A \oplus (B \oplus C) = (A \oplus B) \oplus C$, we omit a proof but see [5, p.34-35]. Therefore, G is a group under the symmetric difference.

Lemma 2.3

Let $Q = \{p \in P \mid p^2 \equiv 1 (mod\ m)\}$ and let H be the power set of Q. Let G be as above then H is a subgroup of G.

Proof

If $B_1, B_2 \in H, B_1 \oplus B_2 = (B_1 \cap \overline{B_2}) \cup (\overline{B_1} \cap B_2) \subseteq B_1 \cup B_2 \subseteq H$ so, $B_1 \oplus B_2 \in H$. Therefore, H is a subgroup of the group G by the finite subgroup test.■

Lemma 2.4

For any $A \in H, f(A)^2 \equiv 1(mod\ m)$, or equivalently, $F(A)^2 = 1$.

Proof

If $\{p_1, p_2, \dots, p_n\} = A$ where $|p_i| \leq 2$ for $i = 1, 2, \dots, n$ then $f(A)^2 = (p_1 * p_2 * \dots * p_n)^2 = {p_1}^2 * {p_2}^2 * \dots * {p_n}^2 \equiv 1(mod\ m)$.■

The following corollary is the formula of f simplified for F on H.

Corollary

If A and B are in H, then $F(A \oplus B) = F(A)F(B)$. Moreover, if A is in H and B is in G, it still follows that $F(A \oplus B) = F(A)F(B)$.

The formula for the case where A and B are both in H implies that F is a group homomorphism from H to the set of reduced residues. Also, if $r \in F(H)$ then $r^2 \equiv 1(mod\ m)$. This is because there must be some $B \in H$ with $F(B) = r$, so $r^2 = F(B)F(B) = F(B \oplus B) = F(\emptyset) = 1$. One final group which we will make use of is $H' = \{A \in H \mid F(A) = 1\}$. Then we have that $H' = \ker(F)$.

The next theorem is considered one of the most important results in finite group theory and we will soon see that it is essential to the proceeding material.

Lagrange's Theorem

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$ [4, p.140].

This project originated in looking at Erdös' Method for calculating Carmichael numbers. Before explaining this method and what constitutes a Carmichael number we will need to discuss two more concepts.

Square-free Numbers

A number is called square-free if for any prime p which divides a number n, p^2 is not a factor of n [6, p.23].

The number 15 is square-free since the squares of its prime divisors {3, 5} do not divide 15. On the other hand, 24 is not square-free since $2^2 = 4$ divides 24.

The next theorem we give is of great significance. Carmichael numbers must satisfy this criterion and so it provides us with a new way to define Carmichael numbers.

Korselt's Criterion

An integer n divides $a^n - a$ for all integers a if and only if n is square-free and $(p-1)|(n-1)$ for all prime divisors p of n [2, p.p.133-134].

Proof

Suppose we have a number n such that $n|a^n - a$ for all integers a. Since, $n|a^n - a$ then $p|a^n - a$ for all $p|n$. Suppose n is not square-free. Then we can find some factor of n of the form b^2. This implies that $b^2|n$ and $n|b^n - b$ thus $b^2|b^n - b$. This implies that $b^2|b$ which is impossible. Thus, n must be square-free.

Next, let $p|n$ and suppose we have a generator a of the finite group $U(p)$with order $p-1$. If $n|a^n - a$ then $p|a^n - a$. This implies, $a^n \equiv a(mod\ p)$. Now, p does not divide a so $p|a^{n-1} - 1$ and hence $a^{n-1} \equiv 1(mod\ p)$. If $a^k \equiv 1(mod\ p)$ then $ord(a)|k$ and we have that $n-1$ is divisible by the order of a. That is, $(p-1)|(n-1)$.

Conversely, suppose that n is a composite square-free integer and $(p-1)|(n-1)$ for all $p|n$. If $p \nmid a$ then $a^{p-1} \equiv 1(mod\ p)$ and since $(p-1)|(n-1)$ we have, $a^{n-1} \equiv 1(mod\ p)$. Multiplying by a we have $a^n \equiv a(mod\ p)$. Suppose $p|a$ then $a^n \equiv a(mod\ p)$. In both cases $a^n \equiv a(mod\ p)$ for each prime divisor p of n. Since n is square-free, $a^n \equiv a(mod\ n)$. ■

With an understanding of Korselt's Criterion we examine Erdös' Method a little more and explain why we get Carmichael numbers. Below we restate Erdös' method with proof of its Carmichael generating capability.

Erdös' Method

Let m be a highly composite number. Let P be the set of primes $P = \{p \mid p\ does\ not\ divide\ m\ but\ p - 1\ does\ divide\ m\}$. Then if S is any subset of P with $|S| > 2$ for which $f(S) \equiv 1(mod\ m)$, then $f(S)$ is a Carmichael number.

Proof

Let P be the set of primes $P = \{p \mid p\ does\ not\ divide\ m\ but\ p - 1\ does\ divide\ m\}$. Suppose we have some subset S of P with $|S| > 2$ such that $f(S) = C$ and $C \equiv 1(mod\ m)$.Then C is square-free (it is the product of the primes in S) and since each $p - 1$ divides m and m divides $C - 1$ we can apply Korselt's Criterion. That is, $p - 1|C - 1$ so, C must be a Carmichael number. ■

For a given m, the subset products of the set P will not necessarily give the full set of reduced residues modulo m. The next definition describes whether or not a particular reduced residue occurred from a subset product of P.

Cover

We say the set A covers a reduced residue r if $f(A) \equiv r(mod\ m)$ (or $F(A) = r$). We also say that r is covered by A.

Full Cover

We have a *full cover* for m if every reduced residue of m is covered by some subset of P.

Knowing that a reduced residue is covered or that we have a full covering is not all the information we will need. We also want to know how many times each reduced residue was covered as a subset product of the set P and how many reduced residues were covered the same number of times as the other reduced residues. We will be referencing these so often that we have devised two more functions.

$\boldsymbol{cov(r)}$

We define $cov(r)$ to be the number of subsets covering the reduced residue r. That is, $cov(r) = |\{A \subseteq P \mid F(A) = r\}|$. In particular, the number of Carmichael numbers produced by Erdös' method is, Number of Carmichael numbers = $\begin{cases} cov(1)-2, & if\ m+1\ is\ prime \\ cov(1)-1, & otherwise. \end{cases}$

For example, from Table 1.1 the reduced residue 5 occurred 4 times as a remainder of a subset product of P so, $cov(5)=4$. To determine how many Carmichael numbers we calculated we counted how many times a 1 occurred discarding the empty set and $m+1$. For the above definition this gives $cov(1)-2=4-2=2$. In Table 1.2 the count column can now be replaced by $cov(r)$.

Residue	$\boldsymbol{cov(r)}$
1	4
5	4
7	2
11	2
13	2
17	2
19	4
23	4
25	2
29	2
31	2
35	2

Table 2.1

Note from this table that the $cov(r)'s$ are repeated several times. It will be important to know how many times the $cov(r)'s$ occur and for this we have the next function.

$\boldsymbol{COV(k)}$

We define $COV(k)$ to be the number of residues covered k times. That is, $COV(k)$ is the number of r with $cov(r)=k$.

For example, from the above table, which is a variation of Table 1.2, we can count how many times a 2 occurred. This gives, $COV(2)=8$. Also, $COV(4)=4$ since, there are four r's with $cov(r)=4$. We can represent this as a table,

$\boldsymbol{cov(r)=k}$	$\boldsymbol{COV(k)}$
2	8
4	4

Table 2.2

From now on we will be presenting a great deal of information using tables in the form of Table 2.1 and Table 2.2.

With the previous well understood, we will inspect Erdös' method more closely. For instance, is there any underlying structure to Erdös' method? How well does Erdös' method generate Carmichael numbers? We will soon see that the method works very well and it has lead to many interesting results. The remaining pages will hopefully shed more light on this topic.

Chapter 3
Constructions Related to the Power Set Group of *P*

Erdös' method was intended to generate large numbers of Carmichael numbers. We will address how well his method works in this respect, but we first will describe the symmetries and other properties that have emerged throughout our investigation.

Before we discuss the various properties we must provide some details about the different sets and operations we will be using. We will make extensive use of the following terms and sets from the previous chapter:

$\boldsymbol{m}\ is\ some\ fixed\ highly\ composite\ number.$
$\boldsymbol{P} = \{p \mid p\ does\ not\ divide\ m\ but\ p-1\ does\ divide\ m\}$, p is a prime number.
$\boldsymbol{G}\ is\ the\ power\ set\ of\ P.$
$\boldsymbol{Q} = \{p \in P \mid p^2 \equiv 1(mod\ m)\}$.
$\boldsymbol{H}\ is\ the\ power\ set\ of\ Q.$
$\boldsymbol{H'} = \{A \in H \mid F(A) = 1\}$, A is a set of primes from P.

Lemma 3.1.1

$|F(H)| = |H|/|H^{'}|$

Proof

From the first Isomorphism Theorem [4, p.206] if $\varphi : A_1 \rightarrow A_2$ is a group homomorphism, then $A_1/\ker(\varphi) \cong \varphi(A_1)$. In our case, letting A_1 be H and using F for φ, we have $H/H' \cong F(H)$. Taking the order of each side we have, $|H|/|H^{'}| = |F(H)|$. ■

Lemma 3.1.2

If A is in G(as opposed to in H), then $|F(AH)| = |F(H)|$.

Proof

Let B be an element of H. We have $F(A \oplus B) = F(A)F(B)$. If B_1 and B_2 are two elements of H and $F(A \oplus B_1) = F(A \oplus B_2)$, then $F(A)F(B_1) = F(A)F(B_2)$. By cancellation, $F(B_1) = F(B_2)$. That is duplication in AH matches duplication in $H.$ ■

Lemma 3.1.3

Either $F(AH) = F(BH)$ or $F(AH)$ and $F(BH)$ are disjoint. In particular, the sets $F(AH)$ form a partition of $U(m)$.

Proof

Let $r \in F(AH) \cap F(BH)$. This means that for some C_1, C_2 in H, $r = F(A \oplus C_1)$ and $r = F(B \oplus C_2)$. In particular, $F(A)F(C_1) = F(B)F(C_2)$. Since $F(C_2)^2 = 1$, we have $F(A)F(C_1\ )F(C_2) = F(B)$ or $F\big(A \oplus (C_1 \oplus C_2)\big) = F(B)$. Since, $C_1 \oplus C_2 \in H$, it follows that $F(B)$ is in $F(AH)$. For any C_3 in H, $F(B \oplus C_3) = F(B)F(C_3) = \ F\big(A \oplus (C_1 \oplus C_2)\big)F(C_3) = \ F\big(A \oplus (C_1 \oplus C_2 \oplus C_3)\big)$. This implies that $F(B \oplus C_3)$ is in $F(AH)$, and C_3 was arbitrary so, $F(BH) \subseteq F(AH)$. By symmetry, $F(AH) \subseteq F(BH)$. Therefore if $F(AH)$ and $F(BH)$ intersect then they must be equal.■

It may be best to see these three lemmas worked out in an example. Let $m = 72$, we then construct from Erdös' method the set $P = \{5, 7, 13, 19, 37, 73\}$ with respective orders $\{6, 6, 6, 2, 2, 1\}$. Now that we have the orders we can define $Q = \{19, 37, 73\}$. From Q we form $H = \{\emptyset, \{19\}, \{37\}, \{73\}, \{19, 37\}, \{19, 73\}, \{37, 73\}, \{19, 37, 73\}\}$ and we have the following table.

$\boldsymbol{H}$	$\boldsymbol{f}(\boldsymbol{H})$	$\boldsymbol{F}(\boldsymbol{H})$
$\emptyset$	1	1
$\{19\}$	19	19
$\{37\}$	37	37
$\{73\}$	73	1
$\{19, 37\}$	703	55
$\{19, 73\}$	1387	19
$\{37, 73\}$	2701	37
$\{19, 37, 73\}$	51319	55

Table 3.1

There are two subset products of H congruent to 1 modulo 72, which gives $H' = \{\emptyset, \{73\}\}$. Then we have $|H| = 8$, $\left|H'\right| = 2$ and $|F(H)| = \frac{|H|}{|H'|} = \frac{8}{2} = 4$. From the Table

3.1 we have $F(H) = \{1, 19, 37, 55\}$ verifying that $|F(H)| = 4$, which is what we expected from Lemma 3.1.1.

For Lemma 3.1.2 (See the Appendix Table 4.1 for the values $A \in G$ and $F(A)$) we need $A \in G$ but $A \notin H$ so we let $A = \{5, 7, 13\}$, then $AH = \{\{5, 7, 13\}, \{5, 7, 13, 19\}, \{5, 7, 13, 37\}, \{5, 7, 13, 73\}, \{5, 7, 13, 19, 37\}, \{5, 7, 13, 19, 73\}, \{5, 7, 13, 37, 73\}, \{5, 7, 13, 19, 37, 73\}\}$ and $F(AH) = \{23, 5, 59, 23, 41, 5, 59, 41\} = \{5, 23, 41, 59\}$. It is clear that $|F(H)| = |F(AH)| = 4$.

Now to address Lemma 3.1.3 we will keep $A = \{5, 7, 13\}$ and let $B = \{5\}$. Then $BH = \big\{\{5\}, \{5, 19\}, \{5, 37\}, \{5, 73\}, \{5, 19, 37\}, \{5, 19, 73\}, \{5, 37, 73\}, \{5, 19, 37, 73\}\big\}$ and we have $F(BH) = \{5, 23, 41, 5, 59, 23, 41, 59\} = \{5, 23, 41, 59\}$. In this case, $F(AH) = F(BH)$, which shows that AH and BH can be different sets but still have $F(AH) = F(BH)$. On the other hand, if we choose $B^{'} = \{5, 13\}$ we have $B^{'}H = \{\{5, 13\}, \{5, 13, 19\}, \{5, 13, 37\}, \{5, 13, 73\}, \{5, 13, 19, 37\}, \{5, 13, 19, 73\}, \{5, 13, 37, 73\}, \{5, 13, 19, 37, 73\}\}$. Then $F(B^{'}H) = \{65, 11, 29, 65, 47, 11, 29, 47\} = \{11, 29, 47, 65\}$, which shows that $F(AH)$ is disjoint from $F(B'H)$.

Much of the previous discussion was a direct result of group theory. We will now discuss some of the theorems which have arose from the analysis of Erdös' method.

Theorem 1

If $\left|H^{'}\right| = k$, then k divides $cov(r)$ for all reduced residues r.

Proof

If $C \in H'$, then $F(C) = 1$, so for any A in G, $F(A \oplus C) = F(A)$. Accordingly, everything in CH' has the same F-value. This implies that $\{A \in G \mid F(A) = r\}$ is the union of cosets of H', so $|\{A \in G \mid F(A) = r\}| = cov(r)$ is divisible by $|H^{'}|$.■

One important aspect of this theorem is that since H' is a subgroup of G, $\left|H^{'}\right| = k$ must be a power of 2. We know this because of Lagrange's theorem and $|G| = 2^{|P|}$. To better recognize what is happening let's do an example.

<u>Example 3.1</u>

Let $m = 120$. Then we have $P = \{7, 11, 13, 31, 41, 61\}$. These elements have respective orders $\{4, 2, 4, 2, 2, 2\}$. So we have $Q = \{11, 31, 41, 61\}$ and this gives,
$H = \{\emptyset, \{11\}, \{31\}, \{41\}, \{61\}, \{11, 31\}, \{11, 41\}, \{11, 61\}, \{31, 41\}, \{31, 61\}, \{41, 61\},$
$\{11, 31, 41\}, \{11, 31, 61\}, \{11, 41, 61\}, \{31, 41, 61\}, \{11, 31, 41, 61\}\}$. Now calculating $F(H)$ we have two subset products congruent to 1 modulo 120. This gives $H^{'} =$
$\{\emptyset, \{11, 31, 41, 61\}\}$. We should find that $cov(r)$ is divisible by $|H^{'}| = 2$ for any given reduced residue r of 120. For all $A \in G$ we analyze $F(A)$ to create the following table of reduced residues and $cov(r)$. See Appendix Table 4.2 for the values of $A \in G$ and $F(G)$.

$\boldsymbol{r}$	$\boldsymbol{cov(r)}$
1	4
7	2
11	4
13	2
17	2
23	2
31	4
37	2
41	4
43	2
47	2
53	2
61	4
67	2
71	4
73	2
77	2
83	2
91	4
97	2
101	4
103	2
107	2
113	2

Table 3.2

It is easy to see that each $cov(r)$ is divisible by 2 since each is either itself 2 or 4.

Before we commence with the next theorem we require the following lemma to simplify the proof. Recall that $COV(k)$ is the number of residues covered k times. That is, $COV(k) = |cov^{-1}(k)|$, the size of the inverse image of k with the cov function.

Lemma 3.2

If $r \in cov^{-1}(k)$, and $s \in F(H)$, then $rs \in cov^{-1}(k)$.

Proof

Let $A_1, A_2, \dots, A_k$ be a complete list of sets in G with $F(A_i) = r$. Since $s \in F(H)$ there exists a B in H with $s = F(B)$. Now $F(A_i \oplus B) = F(A_i)F(B) = rs$, so each $A_i \oplus B$ covers rs. Suppose that $F(C) = rs$. Then $F(C \oplus B) = F(C)F(B) \equiv rs^2 \equiv r$, since $s^2 \equiv 1$. This means that $C \oplus B$ is one of the A_i's, say $C \oplus B = A_j$. Thus, $C = A_j \oplus B$, so only the sets of the form $A_i \oplus B$ cover rs, meaning that there are exactly k of them.■

Theorem 2

If $j = |H|/|H^{'}|$, then j divides $COV(k)$ for every k.

Proof

From the lemma it follows that every r in $F(AH)$ has the same number of covers. Thus, if $cov(r) = k$, and $r = F(A)$, then $F(AH) \subset \{r \mid cov(r) = k\}$. Then it must be that the set $\{r \mid cov(r) = k\}$ consists of the form $F(BH)$ for various B's. That is, there will be a set of B's that partition $\{r \mid cov(r) = k\}$. But all $F(BH)$ have the same size, j, so $COV(k)$ must be divisible by j.■

Example 3.2

We will once again let $m = 120$. We already have found H and H', so we have $j = \frac{|H|}{|H'|} = \frac{16}{2} = 8$. From Theorem 2, we must have $8|COV(k)$ for each reduced residue of 120. Since we already have a table of reduced residues r and $cov(r)$ we need only find $COV(k)$. That is, we must count how many times each reduced residue was covered the same number of times as other reduced residues. This gives the following table.

$\boldsymbol{cov(r) = k}$	$\boldsymbol{COV(k)}$
2	16
4	8

Table 3.3

In Table 3.3 we find 16 residues were covered 2 times and 8 were covered 4 times. We can see that 8 divides both 16 and 8, thus our theorem holds true for the example $m = 120$.

In our exploration of Erdös' method we noticed that $cov(r)$ was often an even number which we can attribute to the above theorems, but we also observed that $COV(k)$ was almost exclusively even. We found only a few instances where $COV(k)$ gave odds. This can be attributed to Theorem 3 below. First, we provide a lemma,

Lemma 3.3

If $A \subseteq P$ then $F(A) = F(\bar{A})$ if and only if $F(P) = F(A)^2$. Where $\bar{A}$ denotes the *complement* of A in P.

Proof

Suppose $F(A) = F(\bar{A})$ then,

$$\begin{aligned} F(A) &= F(\bar{A}) \\ F(A) * F(A) &= F(A) * F(\bar{A}) \\ F(A)^2 &= F(A \oplus \bar{A}) \\ &= F(P) \end{aligned}$$

Conversely, if $F(A)^2 = F(P)$, then since $P = A \oplus \bar{A}$, $F(A)^2 = F(A \oplus \bar{A}) = F(A)F(\bar{A})$, so $F(A) = F(\bar{A})$. ■

Theorem 3

Suppose $COV(k) = j$. Then there are exactly j residue classes, $r_1, r_2, \dots, r_j$ which are covered k times. If ${r_i}^2 \neq F(P)$ for $1 \leq i \leq j$, then $2|COV(k)$.

Proof

Suppose for the j residue classes, $r_1, r_2, \dots, r_j$ we have ${r_i}^2 \neq F(P)$ for $1 \leq i \leq j$ then from the previous lemma we know $F(A) \neq F(\bar{A})$, for any A with $F(A) = r_i$. Let $F(A) = r$ and $F(\bar{A}) = s$. If $F(B) = r$ then we have,

$$\begin{aligned} F(P) &= F(A)F(\bar{A}) \\ &= r * s \\ &= F(B) * s \end{aligned}$$

Since, $F(P) = F(B)F(\bar{B})$ this implies $F(B)F(\bar{B}) = F(B) * s$ and $F(\bar{B}) = s$. If we let $t = F(P)$, then we have shown that $cov(r) = k$ if and only if $cov(tr^{-1}) = k$, thus the r's pair up. Therefore, $2|COV(k)$. ■

Corollary

If $F(P)$ is not a square modulo m, then $2|COV(k)$ for all k.

Now that we have discussed each theorem and many of their properties we will provide two more examples. In the first example we will have $F(P) = r^2$ for particular reduced residues r and in the second we will have $F(P) \neq r^2$ for all reduced residues.

Example 3.3

Let $m = 576$, then we have $P = \{5, 7, 13, 17, 19, 37, 73, 97, 193, 577\}$ and these elements have respective orders of $\{48, 24, 48, 4, 16, 16, 8, 6, 3, 1\}$. Notice that we have no elements of order 2 but one element of order 1. This guarantees that $H = H' = \{\emptyset, \{577\}\}$. This implies from Theorem 1 that $cov(r)$ will be divisible by 2 and from Theorem 2 that $COV(k)$ will be divisible by 1. Also, note that $F(P) = 49 = 7^2$ ($F(P)$ actually has 8 roots modulo 576 which are 7, 25, 263, 281, 295, 313, 551 and 569) and from Theorem 3 we have the possibility that $2 \nmid COV(k)$. That is 576 gives even $cov(r)$ and has the potential for odd $COV(k)$. We can see from Table 4.3 in the Appendix that indeed $cov(r)$ is divisible by 2.

One thing worth noting about Table 4.3 is that we do not have a full cover of the reduced residues. We only cover 185 of the 192 reduced residues. Although, this does not violate our divisibility by 2 since 0 is divisible by 2. In the following table we produce $COV(k)$ for each of the $cov(r)$'s.

$\boldsymbol{cov(r) = k}$	$\boldsymbol{COV(k)}$
0	7
2	26
4	53
6	60
8	33
10	10
12	3

Table 3.4

Something important to notice is that for the first time we have odd numbers for $COV(k)$. That is, $COV(0) = 7$, $COV(4) = 53$, $COV(8) = 33$ and $COV(12) = 3$. We can attribute this to our sets H and $H^{'}$ being equal and $F(P)$ being a square. Also, if we were to examine each subset product of P we would find that $F(A) \neq F(\bar{A})$ for $F(A)^2 \neq F(P)$. For instance, let $A = \{5, 7, 13, 17\}$ then $\bar{A} = \{19, 37, 73, 97, 193, 577\}$. We then have $F(A) = 247$ and $F(\bar{A}) = 343$, neither is a root of $F(P)$. If we select a set A such that $F(A)^2 = F(P)$ then $F(A) = F(\bar{A})$. For example, let $A = \{5, 13, 17, 73\}$ then $\bar{A} = \{7, 19, 37, 97, 193, 577\}$. We then have $F(A) = 25$ and $F(\bar{A}) = 25$ since 25 is a root of $F(P)$ we found $F(A) = F(\bar{A})$. This was of course expected.

Taking a closer, look let's examine $cov(r) = 12$ which gives $COV(k) = 3$. This says that there are 3 reduced residues covered 12 times by subset products of P. If we create a table of these 36 sets and their resulting reduced residues we have,

$\boldsymbol{r}$	$\boldsymbol{A \in G}$	$\boldsymbol{r}$	$\boldsymbol{A \in G}$	$\boldsymbol{r}$	$\boldsymbol{A \in G}$
89	{17,73}	473	{5,7,13,19,37,97,193,577}	569	{5,37,193}
89	{5,7,19}	473	{13,17,37,73,97,193,577}	569	{17,73,97}
89	{5,37,97}	473	{7,13,17,19,73,193,577}	569	{5,7,19,97}
89	{17,73,577}	473	{5,7,13,19,37,97,193}	569	{5,37,193,577}
89	{5,7,19,577}	473	{13,17,37,73,97,193}	569	{17,73,97,577}
89	{5,37,97,577}	473	{7,13,17,19,73,193}	569	{5,7,19,97,577}
89	{7,13,17,19,73}	473	{5,37,97,193,577}	569	{13,17,37,73,193}
89	{13,17,37,73,97}	473	{5,7,19,193,577}	569	{5,7,13,19,37,193}
89	{5,7,13,19,37,97}	473	{17,73,193,577}	569	{7,13,17,19,73,97}
89	{7,13,17,19,73,577}	473	{5,37,97,193}	569	{13,17,37,73,193,577}
89	{13,17,37,73,97,577}	473	{5,7,19,193}	569	{5,7,13,19,37,193,577}
89	{5,7,13,19,37,97,577}	473	{17,73,193}	569	{7,13,17,19,73,97,577}

Table 3.5

In Table 3.5 the reduced residues $r = 89$ and $r = 473$ have the property that if $F(A) = 89$ then $F(\bar{A}) = 473$. So, the sets that give 89 are complements of those that give 473. Also, for $r = 569$ we have that $F(A) = F(\bar{A})$. Remember that $m = 576$ has 8 square roots and that 569 was one of them. From Theorem 3 if $F(P) = r^2$ we do not necessarily get odds for $COV(k)$ but we get the possibility of odds occurring. When $F(A) = F(\bar{A})$, one of the reduced residues is covered by some sets and their complements k times. In this case it is 569 covered 12 times. So, instead of A and $\bar{A}$ covering two reduced residues we get one reduced residue. This allowed odd $COV(k)$ to occur, which is exactly what happened in example 3.3. Although, if another square root overlaps and is also covered k times then we don't get odd $COV(k)$.

Example 3.4

Let $m = 720$ then we have $P = \{7, 11, 13, 17, 19, 31, 37, 41, 61, 73, 181, 241\}$ and these elements have respective orders of $\{12, 12, 12, 4, 4, 6, 4, 6, 12, 4, 4, 3\}$. Note that we have no elements of order 2 which guarantees that, $H = H' = \{\emptyset\}$ and $cov(r)$ can be odd. From table 4.4 in the Appendix of the values r and $cov(r)$ it is apparent $cov(r)$ is not always divisible by 2. In fact, the very first reduced residue $r = 1$ occurs 27 times. Also, note that $F(P) = 713$ which is not a square modulo 720 thus $2|COV(k)$. Using Table 4.4 in the Appendix we create a new table,

$\boldsymbol{cov(r) = k}$	$\boldsymbol{COV(k)}$
11	4
12	4
13	6
14	2
15	8
16	8
17	14
18	8
19	18
20	14
21	10
22	16
23	10
24	18
25	12
26	14
27	4
28	6
29	6
30	4

31	4
32	2

Table 3.6

Looking at the $COV(k)$ columns we can see that each is divisible by 2 which can be attributed to $F(P)$ not being a square.

We began the chapter with why Erdös devised his method. We will now show how well Erdös' method calculates large numbers of Carmichael numbers. We want a highly composite m so, let $m = LCM(1, 2, 3, \ldots, 17) = 12{,}252{,}240$. The set P for this particular m is given in the Appendix with $|P| = 141$, which is a very large set when compared with the previous examples we have had. To find G we would need to calculate 2^{141} subsets which is overwhelming for our computing power but we used a special procedure, which will be described shortly, to achieve the needed results. From this m we found Erdös' method would produce $1{,}260{,}305{,}062{,}670{,}142{,}107{,}465{,}085{,}647{,}449{,}504{,}076$ Carmichael numbers. In general, this number is expected to be approximately $\frac{2^{|P|}}{\varphi(m)}$. In this case,

$$\frac{2^{141}}{\varphi(12{,}252{,}240)} = \frac{2{,}787{,}593{,}149{,}816{,}327{,}892{,}691{,}964{,}784{,}081{,}045{,}188247{,}552}{2{,}211{,}840}$$

$$\cong 1.2603050626701425 * 10^{36}.$$

To manage these calculations it was necessary to concoct a few algorithms which allowed us to keep track of $cov(r)$ for each reduced residue without holding each subset product in memory. We achieved this by creating "bins" in which each bin corresponded to a reduced residue and the bin stored $cov(r)$ as we proceeded to do multiplications.

Algorithm

First, we find our set P and all reduced residues of our number m. Let $|P| = k$, and $\varphi(m) = n$. Form an array of size n, one entry for each reduced residue. Initialize the array by setting the first entry to 1 and the rest of the entries equal to 0. Let A_0 be the empty set. For each prime p_i in P we let $A_i = A_{i-1} \cup \{p_i\}$. For $1 \leq i \leq k$ we do the following, A_0 gives the initial count with a 1 in the empty sets position. We then multiply each reduced residue by the next element in P and reduce modulo m. This uses the elements from A_1 and permutes the set of reduced residues. These permuted numbers correspond to the non-permuted numbers in the array we constructed. We sort by the permuted reduced residues and sort the corresponding numbers from the array as we sort. Then add the corresponding newly arranged numbers to the previous array, that is the array from A_0. We would then multiply each reduced residue by the next number in P which will handle A_2. We sort and add this sorted array to the previous array we got from adding the arrays of A_0 and A_1. We continue doing this for each i until all the $i's$ have been exhausted.

For example, if we have found $cov(r)$ for A_{10} we then multiply each reduced residue by the 11^{th} number from our set P. Then the $cov(r)$'s from the array of A_{10} correspond to the permuted reduced residues. Sorting the permuted reduced residues and their corresponding $cov(r)'s$ we add them to the previous $cov(r)$'s from A_{10}. We continue to multiply each reduced residue by the next element in P and add the previous $cov(r)$'s to the newly shuffled $cov(r)$'s until we have exhausted each number from P. We will be left with $cov(r)$ for our entire set P. Let's do a small example using this algorithm to better see how it works.

Example 3.5

We will return to the first example from the introduction and let $m = 2 * 2 * 2 * 3 * 3 = 36$. We know $P = \{5, 7, 13, 19, 37\}$ and so $A_0 = \emptyset$, $A_1 = \{5\}$, $A_2 = \{5, 7\}$, $A_3 = \{5, 7, 13\}$, $A_4 = \{5, 7, 13, 19\}$ and $A_5 = \{5, 7, 13, 19, 37\}$. The set of reduced residues of 36 is $\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$. Let's set up an array to keep track of the $cov(r)$'s. We begin with the empty set. Since the empty product is 1 by definition we put 1 in the 1's bin. The other reduced residues give 0 and do not occur. We then have the table for A_0.

Red. Res.	1	5	7	11	13	17	19	23	25	29	31	35
$\boldsymbol{cov(r)}$	1	0	0	0	0	0	0	0	0	0	0	0

Multiplying each reduced residue by the next element in our set P and reducing modulo m we get the permuted set of reduced residues $\{5, 25, 35, 19, 29, 13, 23, 7, 17, 1, 11, 31\}$.

This gives the table of permuted reduced residues with the corresponding $cov(r)$'s from the table for A_0,

Red. Res.	5	25	35	19	29	13	23	7	17	1	11	31
$\boldsymbol{cov(r)}$	1	0	0	0	0	0	0	0	0	0	0	0

The important feature is that the 5 is in the 1's position from the previous array of reduced residues. What our algorithm does is move the $cov(r)$associated with the previous reduced residue to the position that the new reduced residue came from. So we sort the previous permuted table by the column header (the reduced residues) and have,

Red. Res.	1	5	7	11	13	17	19	23	25	29	31	35
$\boldsymbol{cov(r)}$	0	1	0	0	0	0	0	0	0	0	0	0

Thus the $cov(r)$ from the 1 is moved to the bin below 5 and we can add the two arrays to get the following table for A_1,

Red. Res.	1	5	7	11	13	17	19	23	25	29	31	35
$\boldsymbol{cov(r)}$	1	1	0	0	0	0	0	0	0	0	0	0

We repeat the previous steps and we multiply each reduced residue by the next element in P, which is 7. This gives, $\{7, 35, 13, 5, 19, 11, 25, 17, 31, 23, 1, 29\}$. We now have a new array where the 7 is in the 1's position and 35 is in the 5's position. So 7 and 35 receive the $cov(r)$'s from the 1 and 5 bins respectively and the sorted table is,

Red. Res.	1	5	7	11	13	17	19	23	25	29	31	35
$\boldsymbol{cov(r)}$	0	0	1	0	0	0	0	0	0	0	0	1

We can add this to the previous array from A_1 and we have the table for A_2,

Red. Res.	1	5	7	11	13	17	19	23	25	29	31	35
$\boldsymbol{cov(r)}$	1	1	1	0	0	0	0	0	0	0	0	1

Multiplying by the next number, which is 13, we get $\{13, 29, 19, 35, 25, 5, 31, 11, 1, 17, 7, 23\}$. Thus we have that the 13, 29, 19 and 23 receive the counts from the previous table for A_2 and we add the sorted array to the array from A_2 to get the table for A_3,

Red. Res.	1	5	7	11	13	17	19	23	25	29	31	35
$\boldsymbol{cov(r)}$	1	1	1	0	1	0	1	1	0	1	0	1

Now multiplying by 19 we have, $\{19, 23, 25, 29, 31, 35, 1, 5, 7, 11, 13, 17\}$. We again add the two arrays and get the new table for A_4,

Red. Res.	1	5	7	11	13	17	19	23	25	29	31	35
$\boldsymbol{cov(r)}$	2	2	1	1	1	1	2	2	1	1	1	1

Finally, we multiply by the last number in P which is 37 and we get, $\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$. The final table for A_5 is then,

Red. Res.	1	5	7	11	13	17	19	23	25	29	31	35
$\boldsymbol{cov(r)}$	4	4	2	2	2	2	4	4	2	2	2	2

If we compare this to the very first example we see that this is exactly the same result. We have saved a great deal of time in not having to multiply each subset product and saved memory by not storing each product. This has allowed us to calculate $cov(r)$ for larger sets P, as well as, increase our number m.

We can see from the example of $m = 12{,}252{,}240$ that Erdös' method is very powerful in its intended purpose. It is also full of many interesting mathematical structures and intriguing theorems. In the following chapter we will discuss some of the extreme examples and perhaps why Erdös' method produced such examples.

Chapter 4

Appendix: Tables, Data and Conclusions

In the study of Erdös' method we have attempted many different calculations and generated an immense amount of data. In the following we have compiled this data into an organized format for further analysis and reference.

The following table is a reference for the examples of Lemmas 3.1.2 and 3.1.3. It consists of the entire set of elements $A \in G$ and the associated values $F(A)$ using $m = 72$.

$\boldsymbol{A \in G}$	$\boldsymbol{F(A)}$
$\emptyset$	1
{5}	5
{7}	7
{13}	13
{19}	19
{37}	37
{73}	1
{5,7}	35
{5,13}	65
{5,19}	23
{5,37}	41
{5,73}	5
{7,13}	19
{7,19}	61
{7,37}	43
{7,73}	7
{13,19}	31
{13,37}	49
{13,73}	13
{19,37}	55
{19,73}	19
{37,73}	37
{5,7,13}	23
{5,7,19}	17
{5,7,37}	71
{5,7,73}	35
{5,13,19}	11
{5,13,37}	29
{5,13,73}	65
{5,19,37}	59

$\{5,19,73\}$	23
$\{5,37,73\}$	41
$\{7,13,19\}$	1
$\{7,13,37\}$	55
$\{7,13,73\}$	19
$\{7,19,37\}$	25
$\{7,19,73\}$	61
$\{7,37,73\}$	43
$\{13,19,37\}$	67
$\{13,19,73\}$	31
$\{13,37,73\}$	49
$\{19,37,73\}$	55
$\{5,7,13,19\}$	5
$\{5,7,13,37\}$	59
$\{5,7,13,73\}$	23
$\{5,7,19,37\}$	53
$\{5,7,19,73\}$	17
$\{5,7,37,73\}$	71
$\{5,13,19,37\}$	47
$\{5,13,19,73\}$	11
$\{5,13,37,73\}$	29
$\{5,19,37,73\}$	59
$\{7,13,19,37\}$	37
$\{7,13,19,73\}$	1
$\{7,13,37,73\}$	55
$\{7,19,37,73\}$	25
$\{13,19,37,73\}$	67
$\{5,7,13,19,37\}$	41
$\{5,7,13,19,73\}$	5
$\{5,7,13,37,73\}$	59
$\{5,7,19,37,73\}$	53
$\{5,13,19,37,73\}$	47
$\{7,13,19,37,73\}$	37
$\{5,7,13,19,37,73\}$	41

Table 4.2

The following is a reference for examples 3.1 and 3.2, where $m = 120$.

$\boldsymbol{A} \in \boldsymbol{G}$	$\boldsymbol{F}(\boldsymbol{G})$
$\emptyset$	1
$\{5\}$	5
$\{7\}$	7
$\{13\}$	13
$\{19\}$	19
$\{37\}$	37

{73}	1
{5,7}	35
{5,13}	65
{5,19}	23
{5,37}	41
{5,73}	5
{7,13}	19
{7,19}	61
{7,37}	43
{7,73}	7
{13,19}	31
{13,37}	49
{13,73}	13
{19,37}	55
{19,73}	19
{37,73}	37
{5,7,13}	23
{5,7,19}	17
{5,7,37}	71
{5,7,73}	35
{5,13,19}	11
{5,13,37}	29
{5,13,73}	65
{5,19,37}	59
{5,19,73}	23
{5,37,73}	41
{7,13,19}	1
{7,13,37}	55
{7,13,73}	19
{7,19,37}	25
{7,19,73}	61
{7,37,73}	43
{13,19,37}	67
{13,19,73}	31
{13,37,73}	49
{19,37,73}	55
{5,7,13,19}	5
{5,7,13,37}	59
{5,7,13,73}	23
{5,7,19,37}	53
{5,7,19,73}	17
{5,7,37,73}	71
{5,13,19,37}	47
{5,13,19,73}	11

{5,13,37,73}	29
{5,19,37,73}	59
{7,13,19,37}	37
{7,13,19,73}	1
{7,13,37,73}	55
{7,19,37,73}	25
{13,19,37,73}	67
{5,7,13,19,37}	41
{5,7,13,19,73}	5
{5,7,13,37,73}	59
{5,7,19,37,73}	53
{5,13,19,37,73}	47
{7,13,19,37,73}	37
{5,7,13,19,37,73}	41

Table 4.2

The following table is a reference for example 3.3, where $m = 576$.

$\boldsymbol{r}$	$\boldsymbol{cov(r)}$	$\boldsymbol{r}$	$\boldsymbol{cov(r)}$	$\boldsymbol{r}$	$\boldsymbol{cov(r)}$
1	8	193	6	385	2
5	10	197	2	389	8
7	8	199	4	391	4
11	4	203	4	395	4
13	8	205	6	397	6
17	8	209	2	401	6
19	10	211	8	403	2
23	8	215	2	407	6
25	4	217	2	409	2
29	4	221	10	413	6
31	4	223	6	415	6
35	8	227	4	419	8
37	4	229	6	421	2
41	4	233	0	425	4
43	2	235	8	427	10
47	6	239	2	431	8
49	8	241	2	433	6
53	4	245	2	437	6
55	4	247	8	439	4
59	8	251	6	443	6
61	6	253	0	445	6
65	8	257	4	449	4
67	2	259	6	451	4
71	6	263	4	455	6
73	8	265	10	457	6
77	4	269	6	461	2

79	4	271	4	463	8
83	6	275	4	467	2
85	10	277	6	469	4
89	12	281	0	473	12
91	6	283	2	475	4
95	8	287	2	479	6
97	8	289	4	481	4
101	4	293	6	485	10
103	6	295	4	487	6
107	4	299	6	491	2
109	10	301	4	493	6
113	4	305	4	497	8
115	8	307	6	499	6
119	6	311	2	503	8
121	2	313	4	505	2
125	10	317	8	509	2
127	8	319	4	511	4
131	6	323	8	515	6
133	6	325	6	517	0
137	4	329	0	521	4
139	6	331	8	523	6
143	6	335	4	527	6
145	4	337	4	529	8
149	0	341	6	533	6
151	4	343	8	535	4
155	4	347	8	539	8
157	4	349	2	541	6
161	6	353	2	545	8
163	2	355	6	547	4
167	6	359	6	551	4
169	6	361	10	553	8
173	6	365	6	557	0
175	6	367	6	559	4
179	4	371	4	563	4
181	8	373	6	565	6
185	6	377	6	569	12
187	6	379	2	571	4
191	4	383	6	575	6

Table 4.3

The following table is a reference to example 3.4 of Theorem 3, where $m = 720$.

$\boldsymbol{r}$	$\boldsymbol{cov(r)}$	$\boldsymbol{r}$	$\boldsymbol{cov(r)}$	$\boldsymbol{r}$	$\boldsymbol{cov(r)}$
1	27	241	21	481	24
7	26	247	22	487	24

11	26	251	24	491	22
13	19	253	20	493	17
17	25	257	22	497	25
19	29	259	31	499	28
23	24	263	23	503	25
29	11	269	14	509	15
31	24	271	23	511	25
37	32	277	29	517	27
41	25	281	23	521	24
43	24	283	22	523	26
47	22	287	24	527	26
49	18	289	19	529	19
53	16	293	22	533	18
59	30	299	28	539	30
61	26	301	22	541	24
67	12	307	15	547	13
71	26	311	22	551	24
73	20	313	19	553	17
77	28	317	31	557	29
79	18	319	18	559	20
83	25	323	23	563	24
89	22	329	17	569	17
91	19	331	21	571	16
97	22	337	17	577	17
101	23	341	26	581	23
103	20	343	19	583	17
107	11	347	16	587	13
109	31	349	29	589	28
113	20	353	15	593	21
119	19	359	17	599	20
121	20	361	15	601	21
127	19	367	17	607	20
131	20	371	17	611	19
133	26	373	23	613	23
137	19	377	19	617	18
139	16	379	13	619	11
143	19	383	16	623	21
149	27	389	32	629	29
151	19	391	16	631	21
157	15	397	11	637	14
161	19	401	17	641	20
163	17	403	19	643	20
167	18	407	20	647	18
169	25	409	22	649	25
173	24	413	26	653	22

179	13	419	12	659	15
181	18	421	16	661	22
187	30	427	30	667	28
191	19	431	17	671	20
193	25	433	23	673	24
197	15	437	12	677	13
199	22	439	24	679	26
203	16	443	19	683	21
209	26	449	21	689	25
211	24	451	25	691	23
217	26	457	21	697	25
221	19	461	20	701	17
223	26	463	22	703	24
227	29	467	31	707	28
229	12	469	13	709	15
233	21	473	24	713	27
239	22	479	24	719	26

Table 4.4

The set P for $m = LCM(1, 2, 3, \ldots, 17) = 12{,}252{,}240$.

$P = \{19, 23, 29, 31, 37, 41, 43, 53, 61, 67, 71, 73, 79, 89, 103, 113, 127, 131, 137, 157,$
$181, 199, 211, 239, 241, 281, 307, 313, 331, 337, 397, 409, 421, 443, 463, 521, 547,$
$613, 617, 631, 661, 859, 881, 911, 937, 953, 991, 1009, 1021, 1093, 1123, 1171, 1321,$
$1327, 1361, 1429, 1531, 1871, 1873, 2003, 2143, 2311, 2341, 2381, 2521, 2731,$
$2857, 2861, 3061, 3121, 3433, 3571, 3697, 4421, 4621, 5237, 6007, 6121, 6553,$
$6733, 7481, 8009, 8191, 8581, 9241, 9283, 9521, 10711, 12241, 12377, 14281,$
$15913, 16381, 16831, 17137, 17681, 18481, 19891, 20021, 20593, 21841, 22441,$
$23563, 25741, 27847, 29173, 30941, 36037, 42841, 43759, 46411, 48049, 51481,$
$52361, 55441, 65521, 72073, 72931, 74257, 78541, 79561, 87517{,}92821, 97241,$
$102103, 116689, 117811, 120121, 145861, 157081, 180181, 185641, 235621,$
$291721, 314161, 371281, 471241, 612613, 680681, 816817, 4084081\}.$

In the following table we present data from the least common multiple of integers 1 through some number n. We did this to produce a variety of prime factors in our composite number m with the hope of creating a sufficient set P to produce a large number of Carmichael numbers.

$\underline{\boldsymbol{LCM(1,\ldots,n)}}$

$\boldsymbol{n}$	$\boldsymbol{\lvert P\rvert}$	$\boldsymbol{Number\ of}$ $\boldsymbol{Carmichael\ Numbers}$	$\boldsymbol{\frac{2^{\lvert P\rvert}}{\varphi(m)}}$
5	5	2	2
7	9	4	$5.3\bar{3}$
8	11	12	$10.6\bar{6}$
9	18	468	$455.1\bar{1}$
11	31	373,004	$372{,}827.0\bar{1}$
13	60	16,679,993,081,129	16,679,998,619,890.726
16	75	273,285,099,875,777,838	273,285,097,388,289,653.57
17	141	1,260,305,062,670,142,107,465,085,647,449,504,075	1,260,305,062,670,142,457,271,757,805,302,845,227

Table 4.5

Note in Table 4.5 how the number of Carmichael numbers produced is almost identical to the estimate $\frac{2^{|P|}}{\varphi(m)}$, especially for $n = \{11, 13, 16, 17\}$. With this data we can see that the expected value of $cov(r)$ trends towards the actual calculated value. It is also important to notice that as we increase the size of m we see the estimate becomes a better approximation.

From Table 4.5 it can be seen that Erdös' method does what it was intended to do. That is, it produces a very large number of Carmichael numbers and it does so very quickly. After increasing $m = LCM(1, 2, 3, \ldots, 16)$ to $m = LCM(1, 2, 3, \ldots, 17)$ we have $4.61169 * 10^{18}$ times as many Carmichael numbers.

When we have a full cover of the reduced residues for a particular m we know that we have $cov(1) > 0$. This allows us to begin calculating the expected number of Carmichael numbers we can produce. For $m < 20{,}000$ we have 154 numbers that result in a full cover. The following table lists these numbers along with information related to some sets from chapter 3. Also, the numbers {11016, 11592, 15552} appear in bold because they produce odd $COV(k)$.

Full Cover for $m < 20,0000$

m	$\|P\|$	$\|H\|$	$\|H'\|$	$cov(1)$	$F(P) = r^2$
2	1	2	2	2	Yes
4	2	4	2	2	No
8	2	4	1	1	No
12	3	8	2	2	No
24	3	8	1	1	No
36	5	4	2	4	No
72	6	8	2	4	No
144	7	4	1	3	Yes
180	8	4	2	6	No
216	7	2	1	4	No
360	10	4	1	12	Yes
420	9	16	2	6	No
480	9	4	1	5	No
540	11	8	2	18	No
720	12	1	1	27	No
756	10	4	2	10	No
792	11	8	1	10	No
840	11	64	2	12	No
900	10	1	1	5	No
960	10	2	1	7	No
1008	12	4	2	16	No
1080	13	8	1	31	No
1200	13	16	2	38	No
1224	11	4	1	6	Yes
1260	14	8	1	58	No
1320	11	16	2	12	No
1344	11	8	1	10	No
1440	13	1	1	27	No
1512	11	4	1	9	No
1560	11	8	1	8	No
1584	12	4	1	7	No
1620	14	4	2	48	No
1680	15	8	1	80	No
1728	12	1	1	8	No
1800	14	2	2	36	No
1872	12	4	2	8	No
1920	11	2	1	7	No
1980	14	4	1	37	No

2016	15	8	2	62	No
2100	13	4	1	16	No
2160	17	4	2	206	No
2280	12	32	2	10	No
2304	13	2	1	11	No
2340	13	8	2	12	No
2376	13	4	2	10	No
2400	14	4	1	27	No
2520	18	16	2	468	No
2640	14	16	1	28	No
2700	13	1	1	16	No
2760	12	16	1	4	No
2772	12	1	1	7	No
2880	15	1	1	48	No
2940	12	4	1	7	No
3024	16	2	1	80	No
3060	14	4	2	16	No
3120	14	8	2	20	No
3168	15	2	2	34	No
3240	16	4	1	85	No
3360	18	2	2	332	No
3456	14	2	2	16	No
3600	18	2	1	284	No
3672	14	4	2	20	No
3696	13	8	2	14	No
3744	14	2	1	13	No
3780	19	2	1	611	No
3840	13	4	1	11	No
3960	18	8	1	289	No
4032	18	8	1	224	No
4140	15	2	1	31	No
4176	13	8	2	2	No
4200	17	16	2	128	No
4284	13	4	1	9	No
4320	18	4	1	218	No
4500	13	4	1	8	No
4536	13	2	1	14	No
4560	15	16	2	28	No
4608	13	1	1	5	No
4620	15	4	2	32	No
4680	18	16	1	245	No

4752	15	2	1	23	No
4800	17	4	2	130	No
4860	16	2	2	72	No
5040	23	16	1	7254	No
5184	15	2	1	14	No
5280	17	8	2	106	No
5376	14	4	1	22	No
5400	17	1	1	99	No
5460	16	4	1	57	No
5520	15	2	2	22	No
5544	15	1	1	25	No
5616	14	1	1	9	No
5760	17	1	1	89	No
5796	13	1	1	4	No
5880	15	8	2	40	No
5940	18	4	1	185	No
6000	16	4	1	58	No
6048	19	2	1	301	No
6120	19	8	2	338	No
6240	17	16	1	84	No
6300	19	4	2	342	No
6336	19	4	2	280	No
6480	22	2	2	2348	No
6552	15	4	2	24	No
6600	15	2	1	29	No
6624	14	2	1	7	No
6720	20	4	1	672	No
6840	16	2	2	38	No
6912	16	2	1	25	No
6930	14	1	1	12	No
7020	17	2	1	77	No
7056	16	4	2	32	No
7128	16	4	2	38	No
7140	15	32	2	20	No
7200	19	1	1	283	No
7344	15	4	1	14	No
7380	13	4	1	2	No
7392	17	8	2	72	No
7488	17	2	2	48	No
7560	24	4	2	9780	No
7776	15	2	1	17	Yes

7800	16	4	1	32	No
7920	21	16	2	1092	No
8064	20	4	1	448	No
8100	18	4	2	134	No
8190	15	2	2	20	No
8280	18	2	1	113	No
8316	17	4	2	56	No
8352	16	4	2	24	No
8400	24	8	1	8754	No
8448	14	4	1	7	No
8568	18	8	1	117	No
8580	14	16	2	12	No
8640	21	2	2	936	No
8712	16	8	2	34	No
8736	16	4	2	26	No
8820	19	2	2	280	No
8880	15	4	1	20	No
9000	19	8	2	198	No
9072	19	1	1	217	No
9108	15	2	2	8	No
9120	17	8	1	64	No
9180	20	16	2	442	No
9240	21	8	2	1062	No
9360	22	2	1	1827	No
9504	18	1	1	95	No
9600	19	8	2	254	No
9660	20	32	2	532	No
9720	19	4	2	248	Yes
9828	15	2	2	16	No
9900	19	8	2	238	Yes
9936	16	2	1	29	No
9984	14	4	1	7	No
10080	27	2	1	58059	No
10200	15	8	1	12	Yes
10260	14	1	1	11	No
10296	17	1	1	47	No
10368	18	2	2	70	No
10440	16	2	1	22	No
10500	16	4	2	28	No
10560	19	2	1	217	No
10584	15	2	1	19	No

10710	15	2	2	16	No
10800	23	1	1	2943	No
10920	20	4	1	453	No
11016	**15**	**1**	**1**	**11**	**Yes**
11040	16	2	1	22	No
11088	20	1	1	360	No
11160	16	8	2	24	No
11232	16	1	1	13	No
11340	23	4	1	3234	No
11400	18	16	1	84	No
11424	15	2	1	17	No
11484	14	4	1	8	No
11520	19	1	1	183	No
11592	**17**	**2**	**2**	**42**	**Yes**
11664	15	1	1	11	No
11700	19	4	2	174	No
11760	19	4	1	180	No
11880	23	4	1	2794	No
12000	18	4	1	91	No
12096	23	2	2	2380	No
12240	22	4	2	1344	No
12420	20	4	2	334	No
12480	18	4	1	91	No
12528	16	2	1	18	No
12600	27	8	2	46640	No
12672	21	2	1	548	No
12852	19	4	2	170	No
12960	24	2	1	4773	No
13104	20	4	1	297	No
13200	20	1	1	329	No
13248	17	2	2	24	No
13320	16	4	1	21	No
13440	24	16	2	5504	No
13464	18	4	1	66	No
13500	16	1	1	21	No
13680	20	4	2	298	No
13728	16	2	2	18	No
13800	16	2	1	18	No
13824	16	1	1	12	No
13860	23	1	1	2952	No
13920	16	8	2	22	No

14040	22	2	1	1219	No
14112	19	2	1	137	No
14256	19	8	1	134	No
14280	22	64	2	1344	No
14400	24	4	2	4342	No
14580	18	2	1	94	No
14688	16	1	1	17	No
14700	17	2	1	41	No
14760	15	4	1	10	No
14784	20	4	1	276	No
14976	19	2	1	109	No
15120	32	4	2	1244092	No
15180	17	8	1	40	No
15300	18	1	1	58	No
15456	16	2	1	26	No
15480	17	8	1	34	No
15540	15	8	2	10	No
15552	**17**	**1**	**1**	**22**	**Yes**
15600	22	4	2	1070	No
15660	17	2	2	34	No
15840	25	8	1	8747	No
15912	18	2	2	42	No
15960	18	2	1	74	No
16128	22	2	1	921	No
16200	22	4	1	967	No
16320	16	4	1	16	No
16380	25	8	2	9726	No
16560	23	2	2	2030	No
16632	22	8	2	944	No
16704	19	2	1	96	No
16740	17	2	2	26	No
16800	27	2	1	34985	No
16848	16	1	1	14	No
16920	18	8	2	76	No
17100	15	1	1	7	No
17136	22	8	2	916	No
17160	20	16	1	266	No
17280	24	2	1	3635	No
17388	17	2	2	36	No
17400	16	16	2	10	No
17424	17	2	1	30	No

17472	18	2	1	56	No
17640	25	4	1	8596	No
17760	17	2	2	30	No
17820	22	1	1	990	No
17940	17	8	1	26	No
18000	23	2	1	1667	No
18144	23	1	1	1616	No
18216	20	4	2	176	No
18240	19	4	1	118	No
18360	26	16	1	14388	No
18480	28	16	2	69986	No
18720	25	1	1	7291	No
18900	24	2	1	3857	No
19008	23	2	2	1444	No
19152	16	1	1	15	No
19200	21	2	1	402	Yes
19320	23	64	2	2008	No
19440	27	8	2	25726	No
19584	16	2	1	13	No
19656	19	2	1	91	No
19800	26	16	2	14612	No
19872	17	1	1	28	No
19980	16	2	1	16	No

Table 4.6

There may be several observable patterns in the previous table. One in particular is that the larger our set P the greater $cov(1)$ will be. The two largest sets of P have orders 28 and 32 both produce the largest numbers for $cov(1)$. So it seems that the greater the variety in the set P the greater the Carmichael number generating capability of Erdös' method.

Throughout our discussion of Erdös'method we have used the idea of adding 1 to the primes which divide our number m. Suppose we modify his method and instead of adding 1 we subtract 1. We could then find $P = \{p \mid p\ does\ not\ divide\ M\ but\ p + 1\ does\ divide\ M\}$. This would not create Carmichael numbers but with other conditions it would produce Fibonacci pseudoprimes. Although, would similar constructions occur in our set P? Might there be other properties present which were either absent or overlooked when adding 1? What differences in the two procedures exist?

In conclusion, the previous data may contain numerous unnoticed trends. In addition, with more time and further examination might these constructions and additional analysis provide better bounds for Carmichael numbers than those which have already been discovered? We have found many new facts and answered a few questions. This has created the opportunity to find yet unknown facts and answer new questions, which will hopefully lead to a better understanding of Carmichael numbers.

References

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

[2] R. Crandall and C. Pomerance. *Prime numbers: a computational perspective*. Springer (2005): 133-135.

[3] P. Erdös. *On pseudoprimes and Carmichael numbers*. Publicationes Mathematicae, Debrecenv 4 (1956): 201-206.

[4] J. Gallian. *Contemporary Abstract Algebra*. Brooks/Cole, Cengage Learning (2009).

[5] C. Kuratowksi. *Introduction to set theory and topology*. Pergamon (1961).

[6] W. LeVeque. *Fundamentals of Number Theory*. Dover Publications (1996).

[7] K. Rosen. *Discrete Mathematics and Its Applications*. WCB McGraw-Hill (1999).

[8] Wolfram Research, Inc., Mathematica, Version 7.0, Champaign, IL (2008).

Annotated Code

We have written many different versions of code to implement Erdös' method. The following code is the final version which was implemented with mathematica version 7 using our algorithm from chapter 2. We included the output for $m = 36$ in the hopes of assisting in understanding how the code operates.

Since this is annotated code the comments appear within *(**)*. For example, *(*This code is annotated and comments look like this.*).* Also, the actual code is bold face and all output generated from the code is separated by a single space from input.

```
m=36;
RES={};
i=1;
While[i≤m,If[CoprimeQ[i,m],AppendTo[RES,i]];i+=2]
(*finds set of reduced residues of m by comparing odd integers less than m for relatively
primeness and if true puts in RES,*)
RES;
(*RES is the set of all reduced residues of m*)
DIV=Divisors[m];
(*finds all divisors of m*)
R=PrimeQ[DIV+1];
(*determines if DIV+1 is prime*)
P={};
(*this will become the set P from erdoes' method*)
For[i=1,i≤Length[DIV],i++,If[R[[i]],AppendTo[P,DIV[[i]]+1],Null]]
(*finds all prime numbers contained in R and places them in P*)
INT=Intersection[P,DIV];
For[i=1,i≤Length[INT],i++,P=DeleteCases[P,INT[[i]]]]
(*deletes all divisors of m from P*)
p=Length[P];
ORDP={};
(*set of orders of elements of P*)
For[i=1,i≤p,i++,AppendTo[ORDP,MultiplicativeOrder[P[[i]],m]]]
(*Loop calculates order of elements in set P*)
phi=EulerPhi[m];
(*Euler's phi function calculates ϕ (m)*)
phi⩵Length[RES]
(*compares phi to what we found in the loop above to determine if all reduced residues
were found*)
PrimeQ[m+1]
(*determines if m+1 is prime*)
Roots[x^2⩵Fold[Times,1,P],x,Modulus→m]
(*if F (P) is a square modulo m  prints all square roots*)
```

```
True
```

```
True
x==0||x==6||x==12||x==18||x==24||x==30
```

```
binTotal=BinCounts[{1},{Union[RES,{m}]}];
(*puts first count of empty product into binTotal. binTotal will become cov (r) for each
reduced residue r*)
h[x_]:=Mod[RES*P[[x]],m]
(*function to find product of elements from RES (reduced residues of m) and elements in
P*)
resMod=RES;(*copy RES into resMod*)
j=1;
While[j≤p,resMod=h[j];sres=Drop[Flatten[Sort[Partition[Riffle[resMod,binTotal],2
]]],{1,-1,2}];binTotal+=sres;++j]
(*this loop calculates the product of each element of P and reduced residues of m and
uses counts of resMod to insert counts into binTotal*)
cov=Partition[Riffle[RES,binTotal],2];
(*creates list of {r, cov (r)}*)
COV=Tally[Sort[binTotal]];
(*creates list of {k, COV (k)}*)
```

```
No Output
```

```
Print[m];
Print[FactorInteger[m]];
Print[P];
Print[ORDP];
Print[p];
Print[COV];
Print[cov];
```

```
36
{{2,2},{3,2}}
{5,7,13,19,37}
{6,6,3,2,1}
5
{{2,8},{4,4}}
{{1,4},{5,4},{7,2},{11,2},{13,2},{17,2},{19,4},{23,4},{25,2},{29,2},{31,2},{35,2}}
```