GENERATING CARMICHAEL NUMBERS

ABRAHAM WANG

1. Introduction

I'm really excited to share with my peers an introduction to Carmichael numbers. We will assume a basic competitive math background, so basic number theory results such as Chinese Remainder Theorem and Fermat's Little Theorem are all that are necessary for this paper. Many results that come from Carmichael numbers require knowledge of pretty complicated abstract algebra, and I will try and provide information that is not derived from those things.

Recall Fermat's little theorem, which states that for a prime p, $a^{p-1} \equiv 1 \mod p$ for all $(a, p) = 1$ (gcd of a and d is 1). Up until the early 20th century, many people believed that the converse was true, although this was never proven. However, in 1885, Václav Šimerka [Ši85] discovered the first seven composite numbers that disproved this converse, although this discovery went unnoticed. It was Alwin Korselt [Kor99] who first "discovered" these numbers in 1899 and later Robert Carmichael in 1910 who studied them in depth, for which these numbers are now named after him.

Definition 1.1. An integer n is Carmichael if n is composite and for all integers a coprime to n: $a^{n-1} \equiv 1 \mod n$. Alternatively, an integer n is Carmichael if n is composite and for all integers $a \in \mathbb{Z}$, $a^n \equiv a \mod n$.

While this is the original definition of a Carmichael number, as you read this paper, you will notice that Korselt's criterion proves as a far more productive definition. For the purposes of this paper, we will mostly be referencing Korselt's criterion, which will be the first thing proved in section 2.

Definition 1.2. Korselt's criterion: $n > 2$ is Carmichael if and only if n is squarefree and $p - 1$ divides $n - 1$ for all primes p dividing n.

We have the condition that $n > 2$ since $n = 2$ satisfies Korselt's criterion, but is a prime number.

Carmichael numbers have many interesting applications in cryptography. Because of their uniqueness, they are indistinguishable from prime numbers when tested with Fermat's little theorem. This makes them useful in public key cryptography, most popularly RSA algorithms. Another usage is in helping develop primality testing algorithms, which make sure a number is prime.

Date: June 2025.

Because of their uniqueness, it was actually very hard to prove that Carmichael numbers were infinitely extended. Up until the late 20th century, many mathematicians believed it was true, but didn't have the techniques to prove it. However, in 1994, Alford, Granville, and Pomerance [AGP94] proved this result, by putting a lower bound on a function $C(x)$, which gives the number of Carmichael numbers up to x. They found that $C(x) > x^{2/7}$. Since as x approaches infinity, so will $C(x)$; thus, there are infinitely many Carmichael numbers.

In this paper, I will dive into some questions and interesting topics of interest about Carmichael numbers. One such question was on the relatedness between the number of unknown primes and number of Carmichael numbers. Are there infinitely many unknown primes that divide a Carmichael number given a fixed number of primes that already do so? If we created an algorithm searching for all Carmichael numbers, how much time would it take? These questions will be answered in this paper. To begin, I will first begin with elementary properties of Carmichael numbers in section 2, such as Korselt's criterion. In section 3, I will then go on to explain properties of Carmichael numbers given fixed primes. These theorems will help us develop section 4 which is about finding and tabulating Carmichael numbers. Finally, section 5 is dedicated to Chernick's construction [Che39], where we can bring up generalizations on how Chernick's construction works and extending its properties to more prime factors (Don't worry we will explain what Chernick's construction in section 2).

There is no one main result of this paper. However, there is a main section, which is on tabulating and algorithmic generation for Carmichael numbers. This is since section 4 builds off of all previous sections and introduces algorithms that search for Carmichael numbers. Section 5 contains many generalizations to Chernick's constructions and those properties, so that is also something you may find interesting.

2. Elementary properties of Carmichael numbers

I will begin this section by proving Korselt's criterion, and then a construction that follows from it. I encourage the reader to work through Corollary 2.2 since it will help you understand how Korselt's criterion is used.

Theorem 2.1. *Korselt's criterion: A composite integer n is Carmichael if and only if n is squarefree and for every prime factor p of n, $p-1$ must also divide $n-1$.*

We first prove that n is squarefree, then prove that for every prime factor p that divides n, $(p-1)|(n-1)$. Finally, we prove that only Carmichael numbers have such a property. If n is squarefree and for every prime factor $p|n \Rightarrow (p-1)|(n-1)$.

Proof. Assume that integer n is Carmichael but not squarefree. Then, $n = p^k * n'$, where $k \geq 2$, and $(p, n') = 1$. By Chinese Remainder Theorem, there exists an $a \equiv 1 \mod p$, but $a \not\equiv 1 \mod p^2$. This is always true, because we can make $a = p + 1$. If we use the definition of a Carmichael number, all we do now is use some modular arithmetic to find the contradiction:

$$a^{n-1} \equiv 1 \mod n$$

$$a^{n-1} = (p+1)^{n-1} = 1^{n-1} + \binom{n-1}{1} 1^{n-2} p + p^2(\cdots) \equiv 1 \mod p^2$$

$$(n-1)p \equiv 0 \mod p^2$$

As you can see, either $n \equiv 1 \mod p$, but since p is a factor of n, $n \equiv 0 \mod p$, which is a contradiction. Therefore, if n is Carmichael, it must be squarefree.

Arbitrarily pick a prime factor p such that Carmichael $n = p^1 * n'$, since we know n is squarefree. Choose a number a such that $a \equiv 1 \mod n'$ and $(a, n) = 1$. By Fermat's little theorem, $a^{p-1} \equiv 1 \mod p$. Since $(a, n) = 1$, $a^{n-1} \equiv 1 \mod n \Rightarrow a^{n-1} \equiv 1 \mod p$. Since order $p - 1$ is the smallest possible number such that $a^{p-1} \equiv 1 \mod p$, this implies that $n - 1$ is divisible by $p - 1$.

Let n be a composite integer that is squarefree, and for every prime p that divides n, $(p - 1)|(n - 1)$. By Fermat's little theorem, if we choose a such that $(a, n) = 1$, then a is also coprime to every prime p, meaning this equation holds for all primes p that divide n: $a^{p-1} \equiv 1 \mod p$. Since all $p - 1$ are factors of $n - 1$, $a^{n-1} \equiv 1 \mod p$ for all p. As a result, $a^{n-1} \equiv 1 \mod n$, proving that n must be Carmichael.

■

Corollary 2.2. *(Chernick) If k is a positive integer such that $(6k+1), (12k+1), (18k+1)$ are all prime, then $(6k + 1)(12k + 1)(18k + 1)$ is a Carmichael number.*

Proof. The verification of this construction becomes trivial once we use Korselt's criterion. Let $n = (6k + 1)(12k + 1)(18k + 1)$. By definition, n is squarefree. By the second criteria, $n - 1$ must be divisible by $6k, 12k, 18k$.

$$n - 1 = 1296k^3 + 396k^2 + 36k = 36k(36k^2 + 11k + 1)$$

Since $36k$ is divisible by $6k, 12k, 18k$, and $n - 1$ is divisible by $36k$, then $n - 1$ is divisible by all $p - 1$; by Korselt's criterion, n must be Carmichael. ■

Remark 2.3. The reader may be curious as to how the numbers 6, 12, and 18 come about, as well as if there are other numbers that work. This question also made me curious and is the motivation behind section 5.

Remark 2.4. Chernick's construction makes it very easy to conjecture on the infinitude of Carmichael numbers. However, this cannot be proven right now; as the bridge involved is the First Hardy-Littlewood conjecture. This is still unproven to this day. Of course, this conjecture is also intimately related to the twin primes conjecture. For more information, you can look online at the wiki.

Now we explore some basic properties of Carmichael numbers, for which as you will see, mostly all derive from Korselt's criterion.

Lemma 2.5. *If n is Carmichael, then n is odd.*

Proof. Since $n-1$ and n are coprime:

$$(n-1)^{n-1} \equiv (-1)^{n-1} \equiv 1 \mod n$$

Since $n-1$ must be even, n is odd. ■

Lemma 2.6. *If n is Carmichael, then n has at least three prime factors.*

Proof. Assume that n has two prime factors p and q(it cannot have one because n is composite). By Korselt's criterion, $p \neq q$ and $(p-1)|(n-1)$. Without loss of generality assume $p > q$, for which some algebra will show the rest:

$$\frac{n-1}{p-1} = \frac{pq-1}{p-1} = \frac{(p-1)q + (q-1)}{p-1} = q + \frac{q-1}{p-1}$$

This means $(q-1)|(p-1)$, which is impossible since $q < p$. Thus n has at least three prime factors. ■

Lemma 2.7. *If n is Carmichael, then every prime factor of n is less than $\sqrt{n}$.*

Proof. Let's write $n = \prod_{i=1}^{k} p_i$ and choose and arbitrary p_i. Since $n \equiv 1 \mod p_i - 1$, then $p_1 \dots p_k \equiv 1 \mod p_i - 1$. Since $p_i \equiv 1 \mod p_i - 1$, then the product $p_1 \dots p_{i-1} p_{i+1} \dots p_k \equiv 1 \mod p_i - 1$. ■

Lemma 2.8. *If n is Carmichael, then n and $\varphi(n)$ are coprime, where $\varphi(n)$ denotes the Euler totient function.*

Proof. n is squarefree, so we can write $n = p_1 \cdots p_k$, where $k \geq 2$. $\varphi(n) = (p_1 - 1) \dots (p^k - 1)$. By Korselt's criterion, all $p_i - 1$ divide $n-1$, and since no p divide $n-1$, then $\varphi(n)$ and n must be coprime. ■

Corollary 2.9. *If $n = pqr$ is Carmichael, then $q \not\equiv 1 \mod p$.*

Proof. If $n = pqr$, then pqr and $(p-1)(q-1)(r-1)$ cannot share any prime factors by lemma 2.8. However, $q - 1 \equiv 0 \mod p$, meaning that $(pqr, (p-1)(q-1)(r-1)) \leq p$. ■

Remark 2.10. This last corollary may seem trivial, but it is in fact quite useful in generating Carmichael numbers as you will later see in Section 4.

3. Properties of Carmichael numbers given fixed primes

In section 3, I will begin by stating a few lemmas that involve one unknown primes. The theorems involve two unknown primes. The applications of these can be found in Section 4.

Lemma 3.1. *For a fixed set of primes $\{p_1 \dots p_k\}$ such that $c = p_1 \cdots p_k * q$ is carmichael, then there are only finite primes q that make c carmichael.*

Proof. By Korselt's criterion, $(q-1)|(c-1)$, meaning:

$$c = p_1 \dots p_k q \equiv p_1 \dots p_k \equiv 1 \mod q-1$$

This means that $(q-1)|(p_1 p_2 \cdots p_k - 1)$, giving us the inequality $q - 1 \leq \frac{p_1 \cdots p_k}{2}$. Since $p_1 \dots p_k$ is odd, we can further improve this bound to $q \leq \frac{p_1 \dots p_k - 1}{2} + 1$. Because $\frac{p_1 \cdots p_k - 1}{2} + 1$ is a constant, there can only be a finite number of primes q below this constant. ■

Lemma 3.2. *For a given carmichael $c = p_1 \dots p_k$, the product $p_1 \dots p_k q$ is also a Carmichael number if and only if prime q is of the form $m * \mathrm{lcm}(p_1 - 1, \dots, p_k - 1) + 1$ for some $m \in \mathbb{Z}$ such that $q \leq \frac{c-1}{2} + 1$ (Lemma 3.1).*

Proof. Let $c_2 = p_1 \dots p_k q$ and $c_1 = p_1 \dots p_k$. Choose an arbitrary i in range $1 \leq i \leq k$.

$$c_2 \equiv c_1 \equiv 1 \mod p_i - 1$$

$$q \equiv 1 \mod p_i - 1$$

What we have showed is that $q-1$ must be divisible by all $p_i - 1$, meaning that:

$$q - 1 = m * \mathrm{lcm}(p_1 - 1, \dots, p_k - 1)$$

$$q = m * \mathrm{lcm}(p_1 - 1, \dots, p_k - 1) + 1$$

■

Remark 3.3. Using Lemma 3.2, we can try and find a recursive method for generating Carmichael numbers. This lemma brings about a few interesting questions, such as how often a Carmichael number can be generated from a given Carmichael number, or in what conditions will q be a prime number. The greater the Carmichael number however, the harder it is to find a prime q that will work, and I conjecture the number of q is most likely linear with c.

Theorem 3.4. *There are finitely many pairs of primes (q, r) such that make $c = p_1 \dots p_k q r$ a Carmichael number.*

Theorem 3.5. *Let $N = \prod_{i=1}^{d} p_i$ be Carmichael with $p_1 < p_2 < \dots < p_d$ and let $P = \prod_{i=1}^{d-2} p_i$. There are integers in range $2 \leq D < P < C$ such that:*

(1)
$$p_{d-1} = \frac{(P-1)(P+D)}{CD - P^2} + 1$$

(2)
$$p_d = \frac{(P-1)(P+C)}{CD - P^2} + 1$$

(3)
$$P^2 < CD < P^2 \left(\frac{p_{d-2} + 3}{p_{d-2} + 1} \right)$$

Proof. To make this proof easier to understand, make $q = p_{d-1}$ and $r = p_d$, so $N = p_1 \dots p_{d-2}qr$. By Korselt's criterion, $q-1|Pr-1$ and $r-1|Pq-1$. Let $D = \frac{Pq-1}{r-1}$, and $C = \frac{Pr-1}{q-1}$. This gives us the inequality:

$$q < r \rightarrow D < P < C$$

$D \neq 1$, so our range becomes the statement's: $2 \leq D < P < C$. Now, we solve for q by eliminating r.

$$D(r-1) = Pq-1 \rightarrow r-1 = \frac{Pq-1}{D} \rightarrow r = \frac{Pq-1+D}{D}$$

$$C(q-1) = Pr-1 \rightarrow Cq-C+1 = Pr \rightarrow r = \frac{Cq-C+1}{P}$$

Equating the two:

$$\frac{Pq-1+D}{D} = \frac{Cq-C+1}{P} \rightarrow P^2q - P + DP = CDq - CD + D$$

$$q(CD-P^2) = CD + DP - D - P \rightarrow q = \frac{CD+DP-D-P}{CD-P^2}$$

$$q = \frac{CD-P^2+P^2+DP-D-P}{CD-P^2} = \frac{(P-1)(P+D)}{CD-P^2} + 1$$

By symmetry, and using the same technique, we can solve for r, giving us:

$$r = \frac{(P-1)(P+C)}{CD-P^2} + 1.$$

Now for the inequalities:

$$CD = \frac{Pq-1}{q-1} * \frac{Pr-1}{r-1}$$

$$\frac{Pr-P}{r-1} < \frac{Pr-1}{r-1} \rightarrow P < \frac{Pr-1}{r-1}$$

Therefore:

$$CD > P^2$$

Since $p_{d-2} + 2 \leq q$, and we have $D < P$, so

$$p_{d-2} + 2 \leq q \rightarrow p_{d-2} + 1 \leq \frac{(P-1)(P+D)}{CD-P^2} < \frac{P(P+P)}{CD-P^2}$$

$$(CD-P^2)(p_{d-2}+1) < 2P^2 \rightarrow CD < P^2\left(1 + \frac{2}{p_{d-2}+1}\right)$$

$$P^2 < CD < P^2\left(\frac{p_{d-2}+3}{p_{d-2}+1}\right)$$

■

The proof of theorem 3.4 easily follows from theorem 3.5. Since $p_1 \dots p_{d-2}$ are fixed, this implies that P is also fixed, which gives us the upper bound on CD. This means that there are only finitely many C and D that satisfy this. Since q and r can be written in terms of P, C, and D, then there must only be finitely many q and r as well.

Definition 3.6. Let carmichael $c = pqr$ for prime p, q, r such that $p < q < r$. Define h_1, h_2, h_3 as:

(1) $h_1 = \frac{qr-1}{p-1}$
(2) $h_2 = \frac{pr-1}{q-1}$
(3) $h_3 = \frac{pq-1}{r-1}$

Since $(p-1)|(qr-1)$ by Korselt's criterion, then all h_i are integers.

Lemma 3.7. *We can restrict h_3 such that $2 \leq h_3 \leq p-1$.*

Proof. By definition, $q < r$, and since q and r are odd, then $q < r-1$, so we can say that

$$qh_3 < (r-1)h_3 = pq - 1 < pq.$$

This shows that $h_3 < p$ or because h_3 and p are integers, we can say that $h_3 \leq p-1$. Now, $h_3 \neq 1$ or else $pq - 1 = r - 1$, implying that r is composite. This contradicts our definition, so $h_3 \neq 1$. This means that $2 \leq h_3 \leq p-1$. ■

Remark 3.8. Using a similar method, we can restrict h_1 and h_2 and derive that $h_1 \geq r+1$ and $p+1 \leq h_2 \leq r-1$.

Lemma 3.9. *We can rewrite q in terms of p, h_3, and h_2. The reason we do this is so that we can get rid of one unknown, which is r. We can say that*

$$q = \frac{(p-1)(p+h_3)}{h_2h_3 - p^2} + 1.$$

Proof. Using Definition 3.6, we can write $h_2(q-1) = pr - 1$ and $h_3(r-1) = pq - 1$. If we solve for r, then we can equate the two equations.

$$\frac{h_2(q-1)+1}{p} = \frac{pq-1}{h_3} + 1$$
$$h_3h_2(q-1) + h_3 = p^2q - p + ph_3$$
$$h_2h_3(q-1) - p^2q + p^2 = p^2 - p + ph_3 - h_3$$
$$(h_2h_3 - p^2)(q-1) = (p-1)(p+h_3)$$
$$q = \frac{(p-1)(p+h_3)}{h_2h_3 - p^2} + 1$$

■

Lemma 3.10. *The sum $\sum_{i=2}^{n} 1/n$ is always less than $\ln(n)$.*

Proof. It is easy to see that the average value of $[n-1,n]$ of $1/n$ will always be greater than $1/n$. This is since all values $[n-1,n)$ of $1/n$ is greater than $1/n$. Therefore, by the average value formula:

$$\frac{1}{n-(n-1)}\int_{n-1}^{n}\frac{1}{n}dn = \ln(n)-\ln(n-1) > \frac{1}{n}$$

. Using this fact, we can use our summation formula to put an upper bound to $1/n$:

$$\sum_{i=2}^{n}\frac{1}{n} < (\ln(n)-\ln(n-1)) + (\ln(n-1)-\ln(n-2)) + \cdots + (\ln 2 - \ln 1)$$

$$\sum_{i=2}^{n}\frac{1}{n} < \ln(n)-\ln(1) = \ln(n)$$

■

Theorem 3.11. *Define $f_3(p)$ to be the number of Carmichael numbers with three prime factors with smallest prime p. Then, $f_3(p) < (p-2)(\ln(p-1)+2)$.*

Proof. For our proof, we begin by using Definition 3.6 to avoid confusion. Let $d = h_2h_3 - p^2$, and pick an h_3 satisfying $2 \le h_3 \le p-1$ (Lemma 3.7). By Lemma 3.9,

$$d = \frac{(p-1)(p+h_3)}{q-1}.$$

Since d is a positive integer by it's definition and $p-1 < q-1$, then $d < p+h_3$ implies $d \le p+h_3-1$. Since d must be congruent to $-p^2 \mod h_3$, we can set an upper bound on the number of possible d given this construction. Let $d = a + kh_3$, where $a \equiv -p^2 \mod h_3$. If we count the number of k which satisfy the inequalities, it will also equal to the number of d that also satisfy these inequalities. By these inequalities, $1 \le a + kh_3 \le p + h_3 - 1$. Solving for k, it is bounded between the integers:

$$\left\lceil \frac{1-a}{h_3} \right\rceil \le k \le \left\lfloor \frac{p+h_3-1-a}{h_3} \right\rfloor$$

Thus, the number of choices of k are:

$$\left\lfloor \frac{p+h_3-1-a}{h_3} \right\rfloor - \left\lceil \frac{1-a}{h_3} \right\rceil + 1 \le \frac{p+h_3-1-a}{h_3} - \frac{1-a}{h_3} + 1 = \frac{p-2}{h_3} + 2$$

If we iterate through all possible h_3, we can determine the number of choices for k, which is the same as the number of d. Using k to solve d, we can find a solution by solving for h_2, q, and finally r. At most, this gives us one solution. Therefore, we can state the following(in combination with Lemma 3.10) to get:

$$f_3(p) \le \sum_{h_3=2}^{p-1}\left(\frac{p-2}{h_3}+2\right) < (p-2)(\ln(p-1)+2).$$

■

4. Algorithms + Tabulating Carmichael numbers

In this section we will overview some algorithms on generating Carmichael numbers, and be discussing some possible alternatives and current optimal algorithms. The first subsection will be dedicated to tabulating Carmichael numbers and then we will discuss possible algorithms. Our Lemmas/Theorems from section 3 will prove to be quite useful.

Let's begin with a method of quickly calculating all Carmichael numbers below 3000, for which they are all below 3 prime factors. This table will begin by choosing the smallest prime p for which we will choose another prime q. From there, we will search for an r that will make pqr Carmichael using the following steps:

(1) Make sure you find q such that $q \not\equiv 1 \mod p$ by Corollary 2.9. To make this formula more useful, we can use the fact that q is odd to say that $q \not\equiv 1 \mod 2p$.
(2) Assume $p < q < r$
(3) Calculate $pq - 1$ (multiple of $r - 1$) and find even factors (possible $r - 1$)
(4) Test r using the following criteria:
  (a) Find possible $r - 1$ through $pq - 1$
  (b) By lemma 3.1, find possible $q < r \leq \frac{pq-1}{2} + 1$
  (c) Test whether $q - 1 | pr - 1$ and $p - 1 | qr - 1$
  (d) If these conditions are met, then pqr is Carmichael.

p	q	$pq - 1$	$\frac{pq-1}{2} + 1$	r	pqr
3	5	$14 = 2 * 7$	8	None	None
3	11	$32 = 2^6$	17	17	$3 * 11 * 17 = 561$
3	17	$50 = 2 * 5^2$	26	None	None
3	23	68	35	None	None
5	7	34	18	None	None
5	13	64	33	17	$5 * 13 * 17 = 1105$
5	17	84	43	29	$5 * 17 * 29 = 2465$
5	19	94	48	None	None
7	11	76	39	None	None
7	13	90	46	19 and 31	$7 * 13 * 19 = 1729$ and $7 * 13 * 31 = 2821$
7	17	118	60	None	None
11	13	142	72	None	None

Table 1. Iterating using q.

Pretty evidently, this method is pretty inefficient, since we must do a lot of work for little results. Additionally, as we go onto larger and larger Carmichael numbers, they become much harder to find; as a result, this method will not suffice.

For a similar method but more efficient, we can iterate through a different variable. To do this, we use Definition 3.6 to help with our tabulation and Lemma 3.9. Define $d = h_2h_3 - p^2$. If we assign a value for a prime p and iterate through h_3, we can find d using a few properties that will be proven here.

Lemma 4.1. *Let $d = h_2h_3 - p^2$, where h_2 and h_3 are defined using Definition 3.6. Then:*

(1) $d \leq p + h_3 - 1$
(2) $d \equiv -p^2 \mod h_3$
(3) $d | (p-1)(p+h_3)$

Proof. (1) By Lemma 3.9, we can rewrite d as

$$d = \frac{(p-1)(p+h_3)}{(q-1)}$$

Since we know that $p < q$, then $d < p + h_3$. Since both these values are integers, we can say that $d \leq p + h_3 - 1$.

(2) If we take the definition of d modulo h_3, we get:

$$h_2h_3 - p^2 \equiv -p^2 \mod h_3.$$

(3) We can rewrite $q-1$ as:

$$q - 1 = \frac{(p-1)(p+h_3)}{d}.$$

Since $q-1$ is an integer, then d must divide $(p-1)(p+h_3)$.

■

Using the properties discussed in Lemma 4.1, we can find d quickly. Afterwards, we can then solve for q and r, respectively.

Let's first given an example to show how the process works.

Example. Lets start with $p = 3$. By Lemma 3.7, h_3 is bounded by $2 \leq h_3 \leq 2$, which means that $h_3 = 2$. From here, we can find that $d \leq 4$, $d|10$, and $d \equiv 1 \mod h_3$. This makes $d = 1$. By Lemma 3.9, we can solve for $q = 11$. Finally, using Definition 3.6 of $h_3 = \frac{pq-1}{r-1}$, we can solve r to get $r = 17$.

Remark 4.2. As you may have noticed, there can be multiple solutions to d for a certain h_3. The upper bound for this is defined as $\frac{p-2}{h_3} + 2$, for which this is proved in Theorem 3.11.

p	h_3	$-p^2 \mod h_3$	$(p-1)(p+h_3)$	$p+h_3-1$	d	q	r
3	2	$1 \mod 2$	$2*5=10$	4	1	11	17
5	2	$1 \mod 2$	$4*7=28$	6	1	29	73
5	3	$2 \mod 3$	$4*8=32$	7	2	17	29
5	4	$3 \mod 4$	$4*9=36$	8	3	13	17
7	2	$1 \mod 2$	$6*9=54$	8	1	55	
7	2	$1 \mod 2$	$6*9=54$	8	3	19	67
7	3	$2 \mod 3$	$6*10=60$	9	2	31	73
7	3	$2 \mod 3$	$6*10=60$	9	5	13	31
7	4	$3 \mod 4$	$6*11=66$	10	3	23	41
7	5	$1 \mod 5$	$6*12=72$	11	1	73	103
7	5	$1 \mod 5$	$6*12=72$	11	6	13	19
7	6	$5 \mod 6$	$6*13=78$	12			

Table 2. Iterating using h_3.

As you may have noticed, this method has a success rate that is much higher than of our previous method. Not only does it produce more Carmichael numbers, it is able to produce all Carmichael numbers with three prime factors for a certain prime p. This is great for Carmichael numbers with three prime factors, but what happens when we reach Carmichael numbers with four, five, or more prime factors? This segues nicely into how algorithms search for Carmichael numbers. In particular, we describe the algorithm Pinch [Pin93] uses to find all Carmichael numbers up to 10^{15}.

Before we discuss Pinch's algorithm, we must start by defining some terms and prove a few lemmas, as they will be quite important to understanding the process by which we will find Carmichael numbers.

Lemma 4.3. *Let $N = \prod_{i=1}^{d} p_i$ be a Carmichael number less than some number X.*

1. *Let $r < d$ and $P = \prod_{i=1}^{r} p_i$. Then, $p_{r+1} < (\frac{X}{P})^{1/d-r}$*
2. *Put $P = \prod_{i=1}^{d-1} p_i$ and $L = \operatorname{lcm}\{p_1 - 1, \dots, p_{d-1} - 1\}$. Then, $Pp_d \equiv 1 \mod L$ and $p_d - 1 | P - 1$.*
3. *Each p_i satisfies $p_i < \sqrt{N} < \sqrt{X}$.*

Proof.

1. Because $p_{r+1} < p_{r+2} < \dots < p_d$, then $(p_{r+1})^{d-(r+1)+1} < p_{r+1} \cdots p_d = N/P$. Since $N/P < X/P$, we can say that $(p_{r+1})^{d-r} < X/P$. Thus, $p_{r+1} < (\frac{X}{P})^{1/d-r}$.
2. $Pp_d = N$, and so since $N \equiv 1 \mod p_i - 1$ for all $1 \leq i \leq d$, then $N \equiv 1 \mod L$.
3. This is simply satisfied by Lemma 2.7.

■

Lemma 4.4. *Let $P = \prod_{i=1}^{d-2} p_i$. Then*

(1) $p_{d-1} < 2P^2$
(2) $p_d < P^3$

Proof. This proof relies on all the facts from Lemma 3.4, for which they are stated below:

(1)

$$p_{d-1} = \frac{(P-1)(P+D)}{CD-P^2} + 1$$

Since by definition $D < P$ and $CD - P^2 \geq 1$, we can say:

$$p_{d-1} = \frac{(P-1)(P+D)}{CD-P^2} + 1 < \frac{(P-1)(P+P)}{1} + 1 = 2P^2 - 2P + 1 < 2P^2$$

$$p_{d-1} < 2P^2$$

(2)

$$p_d = \frac{(P-1)(P+C)}{CD-P^2} + 1$$

(3)

$$CD < P^2 \left(\frac{p_{d-2}+3}{p_{d-2}+1} \right)$$

We use the fact that $D \geq 2$ by definition and $p_{d-2} \geq 3$ since 3 is the least prime number.

$$C * 2 < C * D < P^2 \frac{3+3}{3+1} = \frac{3P^2}{2}$$

$$C < \frac{3P^2}{4}$$

This inequality will help us use our second fact from Lemma 3.4, since we can substitute it in.

$$p_d = \frac{(P-1)(P+C)}{CD-P^2} + 1 < \frac{(P-1)(P+3P^2/4)}{1} + 1$$

$$3P^3/4 + P^2 - 3P^2/4 - P + 1 = 3P^3/4 + P^2/4 - P + 1 < 3P^3/4 + P^2/4$$

$$p_d < 3P^3/4 + P^2/4 < P^3$$

■

Remark 4.5. Pinch's algorithm was used to compute all 105,212 Carmichael numbers below 10^{15}.

Now, we will explain the methodology of Pinch's algorithm. Pinch first produced lists of primes up to $p_1, \dots, p_{d-2}$ up to a certain number X, using the first statement in Lemma 4.3. Once here, Pinch described two different ways of finding the last two primes.

Let $P = \prod_{i=1}^{d-2}$. If P is small enough, then we can use Lemma 3.4, looping through all D and C such that CD are within the third statement of Lemma 3.4. For each pair (C, D), they test whether p_{d-1} and p_d are prime by the first two statements of Lemma 3.4. Finally, test whether $\prod_{i=1}^{d} p_i$ is Carmichael using Korselt's Criterion.

Let's say that P is large, and then we loop over all values p_{d-1} using the statements from Lemmas 3.4 and 4.4. Once we find p_{d-1}, we can use the second statement from Lemma 4.3 to find p_d that satisfy $Pp_d \equiv 1 \mod L$ and use bounds from Lemmas 4.3 and 4.4.

To verify that this process actually works, Pinch used a sieving method to verify that the list of Carmichael numbers. First, he would precompute the list of prime p up to a certain number $\sqrt{X}$. Because by Lemma 2.7, a prime will be less than the square root of a Carmichael number, which means that we are finding Carmichael numbers up to a number X.

This sieving method involves forming a table of entries for the integers up to X; for each p in the list of primes, and finding possible values of N by making $N \equiv 0$ mod p and $N \equiv 1 \mod p-1$, or in other words, $N \equiv p \mod p(p-1)$. Additionally, the use of the fact that $N \geq p^2$ and the square-freeness of N is also applied. This helps eliminate many candidates and N is Carmichael if all prime factors of N can be found within the precomputed list of primes. This helps us generate an inequality on the boundedness of this sieving technique.

$$X + \sum_{p \leq Y} \left\lfloor \frac{X}{p(p-1)} \right\rfloor \leq X + \sum_{p \leq Y} \frac{X}{p(p-1)} = O(X)$$

Theorem 4.6. *Testing the condition $2^{N-1} \equiv 1 \mod N$ for all N up to X would take time $O(X(\log X)^3)$.*

Proof. To begin, we first would like to determine the time at which $2^{N-1} \equiv 1 \mod N$ is computed for a single number N.

To compute 2^{N-1}, we use the square and multiply algorithm, which is efficient for very large exponents. Therefore, this is performed at a rate of $\log_2(N-1) \approx O(\log N)$. Since each N has $\log_2 N$ bits, multiplication/squaring is performed at a rate of $O((\log N)^2)$. As a result, the total time to compute for a single number N would be $O((\log N)^3)$.

Now, the total time is simply the sum of the time for each test. In other words,

$$T(X) = \sum_{N=2}^{X} O((\log N)^3)$$

Now, we can approximate this sum using an integral.

$$T(x) \approx \int_2^X (\log t)^3 dt$$

This integral can be solved using integration by parts, for which we will can then evaulate.

$$\int_2^X (\log t)^3 dt = X((\log X)^3 - 3(\log X)^2 + 6(\log X) - 6) + 2((\log 2)^3 - 3(\log 2)^2 + 6(\log 2) - 6)$$

$$\approx X(\log X)^3$$

This gives us time $O(X(\log X)^3)$. ■

Remark 4.7. The reason for the proof of theorem 4.6 is to show the inefficiency of bashing the numbers out and how we can improve the search of finding Carmichael numbers through different techniques.

5. On the matter of Chernick's construction

5.1. **Three prime factors.** First, we will review Chernick's construction(Corollary 2.2, which states that for all integers k such that $6k+1, 12k+1, 18k+1$ are prime, then the product $(6k+1)(12k+1)(18k+1)$ is Carmichael. Now consider the numbers, $6, 12, 18$. How do they come about? If we reduce these ratios, you will notice that we get original ratios of $(1:2:3)$. Indeed, you may also notice that $(6, 12, 18) = \text{lcm}(1, 2, 3) * (1, 2, 3)$. From now on, we will treat a construction by it's original ratios. This will help us further develop a method for solving such constructions.

Example. The construction for a triple like $(1, 3, 5)$ is $(15k+13)(45k+37)(75k+61)$. This can be proved using Korselt's Criterion. You may notice that we can also rewrite this similar to Chernick's construction by rewriting the expression into $((15k+12)+1)(3(15k+12)+1)(5(15k+12)+1)$. Rewriting in this form also makes validating using Korselt's Criterion much easier. This is the motivation for a definition.

Definition 5.1. Call the set $\mathcal{A} = \{a_1, a_2, a_3\}$ a Chernick triple if the product $\prod_{i=1}^3 a_i(Lk+r)+1$ produces a Carmichael number for all prime $(a_i(Lk+r)+1)$, where $L = \gcd(a_1L, a_2L, a_3L)$ and r is some number that creates a construction.

Remark 5.2. The reason for this strange arrangement is so that a_1, a_2, a_3 together are coprime.

Lemma 5.3. *Given Definition 5.1,* $\text{lcm}(a_1, a_2, a_3) | L$.

Proof. Begin by using Korselt's criterion for a certain prime $(a_i(Lk+r)+1)$. Without loss of generality, let $a_i = a_1$. In other words, I can write:

$$(a_1(Lk+r)+1)(a_2(Lk+r)+1)(a_3(Lk+r)+1) - 1 \equiv 0 \mod a_1(Lk+r)$$

Expanding this form, I get:

$$(Lk+r)^3(a_1a_2a_3)+(Lk+r)^2(a_1a_2+a_1a_3+a_2a_3)+(Lk+r)(a_1+a_2+a_3) \equiv 0 \mod a_1(Lk+r)$$

Now, I can divide out by $Lk + r$.

$$(Lk + r)^2(a_1a_2a_3) + (Lk + r)(a_1a_2 + a_1a_3 + a_2a_3) + a_1 + a_2 + a_3 \equiv 0 \mod a_1$$

Now reduce modulo a_1.

$$(Lk + r)a_2a_3 + a_2 + a_3 \equiv 0 \mod a_1$$

Since k is the only variable and the rest are constants, then $(Lk + r)a_2a_3 + a_2 + a_3 \mod a_1$ depends on k. Since k can take on different values modulo $\mod a_1$. As a result, to make this expression not depend on k, $L \equiv 0 \mod a_1$. Since we did not assume anything about a_1, we can say that $L \equiv 0 \mod a_i$, when we iterate i between 1 and 3. As a result, the smallest number that can be created will be $\operatorname{lcm}(a_1, a_2, a_3)$, which means that $\operatorname{lcm}(a_1, a_2, a_3)|L$. ■

Lemma 5.4. *Given Definition 5.1, a_1, a_2, a_3 are relatively prime in pairs.*

Proof. We will prove this statement by contradiction. Assume that $a_2 \equiv 0 \mod a_1$ and $a_3 \neq 0 \mod a_1$ without loss of generality. If we expand the construction form and consider Korselt's Criterion modulo a_1:

$$(a_1(Lk + r) + 1)(a_2(Lk + r) + 1)(a_3(Lk + r) + 1) - 1 \equiv 0 \mod a_1(Lk + r)$$

$$(Lk + r)^2(a_1a_2a_3) + (Lk + r)(a_1a_2 + a_1a_3 + a_2a_3) + a_1 + a_2 + a_3 \equiv 0 \mod a_1$$

$$(Lk + r)a_2a_3 + a_2 + a_3 \equiv 0 \mod a_1$$

Since $a_1|L$ or in other words, $L \equiv 0 \mod a_1$:

$$ra_2a_3 + a_2 + a_3 \equiv 0 \mod a_1$$

As you can see, if a_2 and a_1 share a factor, then so must a_3, because if a number has a certain prime factor, adding a number with that factor to a number that doesn't have that factor will result in a number that doesn't have that prime factor, in which this contradicts our assumption. Since a_2, a_3 cannot both share prime factors with a_1 or else it will contradict Definition 5.1, a_1, a_2, a_3 must be relatively prime in pairs. ■

Remark 5.5. You may notice that by Lemma 5.4, $a_1a_2a_3 = \operatorname{lcm}(a_1, a_2, a_3)$. We can assume for the purposes of this paper $L = \operatorname{lcm}(a_1, a_2, a_3) = a_1a_2a_3$, and this will consider cases where $L \neq a_1a_2a_3$. The reason this is useful is because the smaller L, the more solutions to a construction there is. To prove that L doesn't matter, first let $L = c * M$, where $M = a_1a_2a_3$. Consider Korselt's criterion for a_i. You will notice that c is canceled out and is trivial since $M \equiv 0 \mod a_i$.

Lemma 5.6. $r(a_1a_2 + a_2a_3 + a_3a_1) \equiv -(a_1 + a_2 + a_3) \mod a_1a_2a_3$.

Proof. If we use Korselt's criterion on a_i without loss of generality, then we can say that:

$$(a_1(Lk+r)+1)(a_2(Lk+r)+1)(a_3(Lk+r)+1)-1 \equiv 0 \mod a_1(Lk+r).$$

$$a_1a_2a_3(Lk+r)^2+(a_1a_2+a_2a_3+a_3a_1)(Lk+r)+a_1+a_2+a_3 \equiv 0 \mod a_1$$

By Lemma 5.3:

$$r(a_1a_2+a_2a_3+a_3a_1)+a_1+a_2+a_3 \equiv 0 \mod a_i.$$

By Chinese Remainder Theorem, there is a unique solution $r \mod a_1a_2a_3$ such that:

$$r(a_1a_2+a_2a_3+a_3a_1)+a_1+a_2+a_3 \equiv 0 \mod a_1a_2a_3.$$

■

Corollary 5.7. *There are infinitely many different Chernick triples for constructions for three prime factors taken modulo $a_1a_2a_3$.*

Since there are infinitely many primes, then there are infinitely many triples of prime numbers, for which there is always a unique solution. Now, we will give an example solve for a random construction.

Example. Consider the triple $(1,3,5)$. We first let $L = 1*3*5$ and now use the fact that $r(3+5+15) \equiv -1-3-5 \mod 15$ to solve for r. In other words, $8r \equiv -9 \mod 15$. The multiplicative inverse of 8 modulo 15 is 2, so by multiplying by 2, we get that $r \equiv -18 \equiv 12 \mod 15$. As a result, our construction is $(15k+13)(45k+37)(75k+61)$.

A table of constructions for $(1,2,x)$, where x can be any odd number by Lemma 5.4.

$(1,2,x)$	Modular equation for r	$r \mod a_1a_2a_3$	Construction
$(1,2,3)$	$5r \equiv -6 \mod 6$	$r \equiv 0 \mod 6$	$(6k+1)(12k+1)(18k+1)$
$(1,2,5)$	$7r \equiv -8 \mod 10$	$r \equiv 6 \mod 10$	$(10k+7)(20k+13)(50k+31)$
$(1,2,7)$	$9r \equiv -10 \mod 14$	$r \equiv 12 \mod 14$	$(14k+13)(28k+25)(98k+85)$
$(1,2,9)$	$11r \equiv -12 \mod 18$	$r \equiv 12 \mod 18$	$(18k+13)(36k+25)(162+109)$
$(1,2,11)$	$13r \equiv -14 \mod 22$	$r \equiv 4 \mod 22$	$(22k+5)(44k+9)(242k+45)$
$(1,2,13)$	$15r \equiv -16 \mod 26$	$r \equiv 18 \mod 26$	$(26k+19)(52k+37)(338k+235)$
$(1,2,15)$	$17r \equiv -18 \mod 30$	$r \equiv 6 \mod 30$	$(30k+7)(60k+13)(450k+91)$

5.2. **Generalization to more prime factors.** This section will carry on the same techniques but generalizing towards more prime factors.

Definition 5.8. (Generalization of Definition 5.1)Call a set $\mathcal{B} = \{a_1, \ldots, a_n\}$ a Chernick tuple if $\prod_{i=1}^{n} a_i(Lk+r)+1$ always produces a Carmichael number for prime $a_i(Lk+r)+1$, where $L = \gcd(a_1L, \ldots, a_nL)$.

Lemma 5.9. *(Generalization of Lemma 5.3) Given Definition 5.8,* $\operatorname{lcm}(a_1, \ldots, a_n)|L$.

Proof. Look at Korselt's criterion for a_i. Since k can take on different values modulo a_i, L must equal $0 \mod a_i$ or else the product $\prod_{i=1}^{n} a_i(Lk + r) + 1$ will take on different values modulo a_i. This, of course, cannot happen since it must be $1 \mod a_i$ by Korselt's criterion. ■

Lemma 5.10. *(Generalization of Lemma 5.4) By Definition 5.8, set $\mathcal{B} = \{a_1, \ldots, a_n\}$ are relatively prime in all subsets of length $n - 1$.*

Proof. We will assume that without loss of generality that only the set $\{a_1, \ldots, a_{n-1}\}$ shares a certain prime factor and apply Korselt's criterion for a_1, for which the expression will look something like this:

$$(Lk+r)^{n-1}(a_1 \cdots a_{n-1}+\cdots+a_2 \cdots a_n)+\cdots+(Lk+r)(a_1+\cdots+a_n) \equiv 0 \mod a_1(Lk+r)$$
$$(Lk + r)^{n-2}(a_1 \cdots a_{n-1} + \cdots + a_2 \cdots a_n) + \cdots + (a_1 + \cdots + a_n) \equiv 0 \mod a_1$$

Since $a_1 + \cdots + a_n$ is relatively prime to a_1, and all other products share this prime factor(since a_n is always multiplied with a number with this prime factor), then the sum will always produce a relatively prime number. This is the inherit contradiction, and since we assumed nothing about the set $\{a_1, \ldots, a_{n-1}\}$, then all subsets of length $n - 1$ are relatively prime. ■

Lemma 5.11. *(Generalization of Lemma 5.6) Let S_k be the kth elementary symmetric sum for the set $\{a_1 \ldots a_n\}$. Then the following congruence can be made:*

$$\sum_{i=1}^{n-1} r^{i-1} * S_i \equiv 0 \mod a_1 \cdots a_n$$

Proof. By Korselt's Criterion, we can rewrite our product using S_k. Choose a_1 without loss of Generality.

$$\sum_{i=1}^{n} (Lk + r)^i * S_i \equiv 0 \mod a_1(Lk + r)$$

Divide out $Lk + r$ and use the fact that $L \equiv 0 \mod a_1$

$$\sum_{i=1}^{n} r^{i-1} S_i \equiv 0 \mod a_1$$

Since $S_n \equiv 0 \mod a_1$:

$$\sum_{i=1}^{n-1} r^{i-1} S_i \equiv \quad \mod a_1$$

Since this is true for all a_i, then we can say that

$$\sum_{i=1}^{n-1} r^{i-1} * S_i \equiv 0 \mod a_1 \cdots a_n.$$

■

Remark 5.12. Using this generalized formula found in Lemma 5.11 makes the solve pretty tedious. Looking at $n = 4$, we already have the following ridiculously long equation:

$$r^2(a_1a_2a_3 + a_1a_2a_4 + a_1a_3a_4 + a_2a_3a_4) + r(a_1a_2 + a_1a_3 + a_1a_4 + a_2a_3 + a_2a_4 + a_3a_4) \\ \equiv -(a_1 + a_2 + a_3 + a_4) \mod a_1a_2a_3a_4$$

As of my knowledge, the best method for generally solving these equations is to simply brute force them by trying all the possibilities.

6. Further Questions

(1) **Further bounds on unknown primes:** You have seen in section 3 has bounds for the number of unknown primes and the largest possible value. However, many of these bounds can be further restricted since proving only finitely many unknowns gives lots of leeway for proofs that are very simple and simply inefficient. Hopefully, there will be more research done into this and you will be able to find better and more advanced ways to restrict these unknowns.

(2) **Properties for more unknown primes:** We've already proven that there are finitely many Carmichael numbers given one and two unknown primes; however, it's possible that once there are three unknown primes, there are infinitely many, even given a fixed number of primes. There are infinitely Carmichael numbers with three prime factors, which has been proved by Thomas Wright [Wri24]; therefore, if there are no fixed primes, then there are infinitely many Carmichael numbers. I conjecture that with three unknown prime factors there are infinite many Carmichael numbers. We used quite elementary algebra for our cases for one and two unknown primes and I predict that if we are to make any progress for three and more unknown primes, different tools will be necessary.

(3) **Generalized Constructions** There are still many questions we can make about constructions with more than 3 prime factors. Is there always a solution to a construction given $a_1 \ldots a_n$ that satisfy Lemma 5.10? Are there more than one? Are there still infinitely many constructions? Or finitely many?

References

[AGP94] W. R. Alford, Andrew Granville, and Carl Pomerance. There are infinitely many Carmichael numbers. *Ann. Math. (2)*, 139(3):703–722, 1994.

[Che39] Jack Chernick. On Fermat's simple theorem. *Bull. Am. Math. Soc.*, 45:269–274, 1939.

[Con] Keith Conrad. Carmichael numbers and korselt's criterion.

[Kor99] Alwin Korselt. Probleme chinois. *L'intermédiaire des mathématiciens*, 6:142–143, 1899.

[Pin93] R. G. E. Pinch. The Carmichael numbers up to 10^{15}. *Math. Comput.*, 61(203):381–391, 1993.

[Wri24] Thomas Wright. Carmichael numbers with prime numbers of prime factors, 2024.

[Ši85] Václav Šimerka. On reminders from arithmetical sequence. *Časopis pro pěstování mathematiky a fysiky*, 14:221–225, 1885.