Carmichael Numbers

Xinke Guo-Xue

May 2024

Abstract

A Carmichael number is a number n such that for all a relatively prime to n, $a^{n-1} \equiv 1 \pmod{n}$. In this paper, we show several properties of Carmichael numbers. First, we show several basic properties of Carmichael numbers. Second, we prove Korselt's Criterion, which gives a necessary and sufficient condition a number to be a Carmichael number. Third, we present a few corollaries of this condition. Finally, we prove that there are infinitely many Carmichael numbers. Finally, we state a few recent results about Carmichael numbers.

1 Introduction

Fermat's Little Theorem says that for a prime p, $a^{n-1} \equiv 1 \pmod{p}$, for all $\gcd(a, n) \neq 1$. It's natural to then ask the question, is the converse true? That is, if $a^{m-1} \equiv 1 \pmod{m}$ for all a relatively prime to m, then is m prime? It turns out this is false, and the counterexamples to these are called Carmichael numbers.

For example 561 is a counterexample to this, since $561 = 3 \cdot 11 \cdot 17$. For any a relatively prime to 561, $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$, and $a^{16} \equiv 1 \pmod{17}$, so by the Chinese Remainder Theorem, $a^{560} \equiv 1 \pmod{561}$.

2 Basic Properties

In this section we prove several properties of Carmichael numbers.

Theorem 2.1. Every Carmichael number is odd.

Since $n-1$ is relatively prime to n, we have $(n-1)^{n-1} \equiv 1 \mod n$. so $(-1)^{n-1} \equiv 1 \mod n$ and $(-1)^{n-1} = \pm 1$. Since $n > 2$ we have $(-1) \not\equiv 1$, so $(-1)^{n-1} \equiv 1 \pmod{n}$. Thus $n-1$ is even, so n is odd.

Theorem 2.2. Let n be a Carmichael number. Every prime factor of n is less than $\sqrt{p}$.

If p is a prime factor of n, then

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

so $(p-1)|(n/p-1)$. Thus $p \leq n/p$, and the inequality must be strict. Otherwise, $n = p^2$, which is impossible. So $p^2 < n$ and $p < \sqrt{n}$.

This also shows that every Carmichael number must have at least 3 factors as a corollary: if $n = pq$, then $p < \sqrt{n}$ and $q < \sqrt{n}$, so $pq < n$, which is a contradiction.

3 Korselt's Criterion

Theorem 3.1 (Korselt's Criterion, 1899)**.** A number n is a Carmichael number if and only if n is square-free, and for all prime divisors p of n it is true that $p-1|n-1$.

Carmichael found several such Carmichael numbers with 3 distinct prime factors, and one with four distinct prime factors.

For example, the first few Carmichael numbers are $561, 1105, 1729, 2465$, and 2821. We can check that for $561 = 3 \cdot 11 \cdot 17$, $2 \mid 560$, $10 \mid 560$, and $16 \mid 560$, for $1105 = 5 \cdot 13 \cdot 17, 4 \mid 1104, 12 \mid 1104, 16 \mid 1104$, and for $1729 = 7 \cdot 13 \cdot 19$, $6 \mid 1728$, $12 \mid 1728$, and $18 \mid 1728$.

We now prove Theorem 3.1. Assume n is a Carmichael number. First we will show n is square free. If a prime p divides n more than once, write $n = p^k n'$ where $k \geq 1$ and $(p, n') = 1$. We want to show $k = 1$, and will do this by contradiction using the Chinese Remainder Theorem.

Assume $k \geq 2$, so n is divisible by p^2. By the Chinese Remainder theorem there is an $a \in \mathbb{Z}$ such that $a \equiv 1 + p \mod p^k$ and $a \equiv 1 \mod n'$. Then $(a, n) = 1$, so

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

by the definition of Carmichael numbers. Reduce the above congruence modulo p^2, getting $(1+p)^{n-1} \equiv p^2$. By the binomial theorem, $(1+p)^{n-1} \equiv 1 + (n-1)p \mod p^2$. Since N is divisible by p, $1 + (n-1)p \equiv 1 - p \mod p^2$. Thus $1 - p \equiv 1 \mod p^2$. This is a contradiction so $k = 1$.

This gives another proof that all Carmichael numbers are odd.

Suppose n is an even Carmichael number. Then in order for n to be square-free and composite, n must have an odd factor p. Then $p-1|n-1$ by Korselt's Criterion, but an even number cannot divide an odd number. Contradiction.

A number is said to be cyclic if $\phi(n)$ and n are relatively prime. It follows from Korselt's Criterion that n and $\phi(n)$ are relatively prime, as by Korselt's Criterion, it is true that for any Carmichael number n,

$$\phi(n) = \prod_{p|n} (p-1)$$

But if $p-1|n-1$ for all $p \mid n$, then n and $p-1$, and hence $\phi(n)$, are relatively prime.

Corollary 1. A Carmichael number cannot have exactly two prime divisors

Proof: Suppose n is a product of two primes, so $n = pq$, where p and q are prime. Then by Korselt's criterion, $p - 1 \mid pq - 1$. By clearly $p - 1 \mid (p-1)q = pq - q$, so $p-1|q-1$ by the Euclidean Algorithm. But we can argue similarly that $q-1|p-1$. Contradiction.

4 Chernick's Theorem

Jack Chernick proved a theorem which can be used to construct a subset of the Carmichael numbers.

Theorem 4.1 (Chernick, 1939)**.** The number $(6k+1)(12k+1)(18k+1)$ is a Carmichael number if all its three factors are prime.

Erdős argued heuristically that there should be infinitely many Carmichael numbers.

5 A Lower Bound on Carmichael Numbers

Theorem 5.1 (Alford, Granville, Pomerance)**.** For sufficiently large n there are at least $n^{2/7}$ Carmichael numbers between 1 and n.

For brevity's sake, we will not include every proof in the paper by Alford, Granville and Pomerance on the infinitude of Carmichael Numbers.

The proof of Theorem 5.1 relies on 5 main theorems, namely, Theorems 5.2 to 5.6.

Let $\pi(x)$ denote the number of primes $p \leq x$, and let $\pi(x, y)$ be the number of these for which $p-1$ is free of prime factors exceeding y. Let $\mathcal{E}$ denote the set of numbers E in the range $0 < E < 1$ for which there exist numbers $x_1(E)$, $\gamma_1(E) > 0$ such that

$$\pi(x, x^{1-E}) \geq \gamma_1(E)\pi(x)$$

for all $x \geq x_1(E)$.

Erdős proved that there is a small positive number in $\mathcal{E}$. The best known result is that any positive number less than $1 - (2\sqrt{e})^{-1}$ is in $\mathcal{E}$. One can show using the Brun-Titmarsh theorem that if $E \in \mathcal{E}$, then $E' \in \mathcal{E}$ for some $E' > E$. That is $\mathcal{E}$ is an open interval.

Theorem 2 (Brun-Titmarsh theorem)**.** Let $\pi(x; q, a)$ count the number of primes p congruent to a modulo q with $p \leq x$. Then

$$\pi(x; q, a) \leq \frac{2x}{\phi(q)\log(x/q)} \tag{1}$$

for all $q \leq x$.

Let $\pi(x; d, a)$ be the number of primes up to x that are $a \mod d$. The prime number theorem for arithmetic progressions states that $\pi(x; d, a) \sim \pi(x)/\varphi(x)$ as $x \to \infty$, where φ is the Euler's function.

It is conjectured that equation (1) above holds for $1 \leq d \leq x^{1/2} - \epsilon$ assuming the Riemann Hypothesis.

If one is willing to relax the asymptotic relation in (1), one can take $1 \leq d \leq x^B$ for some small $B > 0$.

Let $\mathcal{B}$ denote the set of numbers in the range $(0 < B < 1)$ for which there is a number $X_2(B)$ and a positive integer D_B, such that for each $x \geq x_2(B)$, there is a set $\mathcal{D}_B(x)$ of at most D_B integers, each exceeding $\log x$, with

$$\pi(y; d, a) \geq \frac{\pi(y)}{2\varphi(d)}$$

whenever $(a, d) = 1$, $1 \leq d \leq \min\{x^B, y/x^{1-B}\}$ and d not divisible by any member of $\mathcal{D}_B(x)$.

It can be shown that the interval $(0, 5/12) \subset \mathcal{B}$.

Theorem 5.2. For each $E \in \mathbb{E}$ and $B \in \mathbb{B}$ there is a number $x_0 = x_0(E, B)$ such that $C(x) \geq x^{EB}$ for all $x \geq x_0$.

Since $(0, 1 - (2\sqrt{\epsilon})^{-1}) \subset \mathcal{E}$ and $(0, 5/12) \subset \mathcal{B}$, we conclude that $C(x) \geq x^{\beta-\epsilon}$ for any $\epsilon > 0$ and all large x depending on the choice of ϵ, where

$$\beta = (1 - 2(\sqrt{\epsilon}^{-1})\frac{5}{12} = .290306\ldots.$$

This implies Theorem 5.1.

Alford et al.'s arugment is based on Erdős's heuristic that there are infinitely many Carmichael numbers.

The idea is to construct an integer L for which there are a very large number of prime p such that $p-1$ divides L. Suppose that the product of some of these primes, say $C = p_1 \dots p_k$ is congruent to 1 mod L. If C is a Carmichael number, since each $p_j - 1$ divides L which divides $C-1$, we may apply Korselt's criterion. The more such products we can find, the more Carmichael numbers we will have constructed.

Theorem 5.3. If G is a finite abelian group in which the maximal order of an element is m, then in any sequence of at least $m(1+\log(|G|/m))$ (not necessarily distinct) elements of g, there is a non-empty subsequence whose product is the identity.

In order to apply Theorem 1.2 to finding Carmichael numbers, we will need to find an integer L with at least

$$\lambda(L)\left(1+\log\frac{\varphi(L)}{\lambda(L)}\right) \geq \lambda(L)$$

primes p for which $p-1$ divides L. Here, Carmichael's lambda function λ_L is the largest order of an element in $(Z/LZ)*$. However, the number of such primes p cannot exceed $d(L)$, the number of divisors of L, since each p is a 1 plus a divisor of l, and usually $\lambda(L)$ is much larger than $d(L)$. To avoid this problem, we pick our L so that $\lambda(L)$ is surprisingly small, while, at the same time, there are many primes p for which $p-1$ divides L. To do this, we select L to be the product of certain primes q for which the prime factors of $q-1$ are all at most y. This is how $E \in \mathcal{E}$ enters into the proof.

Theorem 5.4. For each $B \in \mathcal{B}$, $(0, B) \subset \mathcal{E}$.

Theorem 5.5. Let $\epsilon > 0$. Suppose there is a number x_ϵ such that

$$\pi(x; d, 1) \geq \frac{\pi(x)}{2\varphi(d)}$$

for all positive integers $d \leq x^{1-\epsilon}$, once $x \geq x_\epsilon$. Then there is a number x'_ϵ such that $C(x) \geq x^{1-2\epsilon}$ for all $x \geq x'_\epsilon$.

Since every positive number $B < 5/12$ is in $\mathcal{B}$, and by theorem 5.4, we have that values for $\gamma_1(E)$ and $x_1(E)$ are effectively computable for every positive number $E < 5/12$. We thus have

Theorem 5.6. For each number α in the range $0 < \alpha < 25/144$, there is an effectively computable number $x(\alpha)$ such that $C(x) \geq x^\alpha$ for all $x \geq x(\alpha)$.

6 Bounds on Carmichael Numbers

Let $C(x)$ denote the number of Carmichael numbers less than or equal to X.

Knodel proved that

$$C(X) < X\exp(-k_1(\log X \log\log X)^{1/2})$$

for some constant k_1.

Erdős improved the bound to

$$C(X) < X\exp\left(\frac{-k_2 \log X \log\log\log X}{\log\log X}\right)$$

Alford, Granville, and Pomerance proved in 1994 that for sufficiently large X,

$$C(X) > X^{2/7}.$$

In 2005, this bound was improved by Harman to

$$C(X) > X^{0.332.}$$

and this was later improved by the same to $0.7039 \cdot 0.4736 = 0.33336704 > 1/3$.

Using techniques developed by Yitang Zhang and James Maynard to establish results about small gaps between primes, Daniel Larsen proved an analogue of Bertrand's Postulate for Carmichael numbers. He showed that

Theorem 6.1 (Larsen)**.** For $\delta > 0$ and sufficiently large x in terms of δ, there will always be at least

$$\exp\left(\frac{\log x}{(\log\log x)^{2+\delta}}\right)$$

Carmichael numbers between x and

$$x + \frac{x}{(\log x)^{\frac{1}{2+\delta}}}.$$

7 References

Alford, Pomerance, Granville: There are infinitely many Carmichael Numbers. https://math.dartmouth.edu/~carlp/PDF/paper95.pdf

Erdos, Paul. On pseudoprimes and Erdos numbers. https://www.renyi.hu/~p_erdos/1956-10.pdf

Jack Chernick:

https://www.ams.org/journals/bull/1939-45-04/S0002-9904-1939-06953-X/S0002-9904-1939-06953-X.pdf

Larsen, Daniel. There are infinitely many Carmichael numbers. https://arxiv.org/pdf/2111.06963

Korselt's Criterion: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/carmichaelkorselt.pdf