Carmichael Numbers

Dale Liu

July 12, 2024

Introduction

Theorem (Fermat's little theorem)

If p is a prime and a is an integer coprime to p, we must have $a^{p-1} \equiv 1 \pmod{p}$

Naturally, the question arose as to whether p could be a composite integer and still satisfy the equation.

Introduction

Definition

A composite number n is a Carmichael number if for any integer a coprime to n, we have $a^{n-1} \equiv 1 \pmod{n}$.

In 1910, Robert Carmichael began an in-depth study of these numbers. He noted that the first such number was 561. These numbers are useful because they are a class of pseudoprimes that pass Fermat's primality test while being composite.

Korselt's Criterion

Theorem (Korselt's Criterion)

A composite integer $n > 2$ is a Carmichael number if and only if n is squarefree and for all primes p dividing n, $(p-1) \mid (n-1)$.

Alwin Korselt proved this in 1899. We can see $561 = 3 \cdot 11 \cdot 17$ satisfies this because $2 \mid 560$, $10 \mid 560$, and $16 \mid 560$.

Further Properties

Proposition

All Carmichael numbers are odd

Proof.

We will prove this is true by contradiction. Assume $n > 2$ is an even Carmichael number. Now, let $a = n - 1$. Since $(n, n-1) = 1$, by definition,

$$a^{n-1} \equiv 1 \pmod{n} \implies (-1)^{n-1} \equiv 1 \pmod{n}.$$

But since n is even, $1 \equiv (-1)^{n-1} \equiv -1 \pmod{n}$, which gives us a contradiction. □

Further Properties

Proposition

All Carmichael numbers have at least 3 prime factors

Proposition

All prime factors p of a Carmichael number n satisfy $p < \sqrt{n}$

Both proofs follow from Korselt's criterion.

Chernick's construction

In 1939, Jack Chernick found a way to generate Carmichael numbers.

Proposition

Given a positive integer k, if $6k+1, 12k+1$, and $18k+1$ are all prime, then the product $(6k+1)(12k+1)(18k+1)$ is a Carmichael number.

Proof.

By Korselt's, we just need to show $6k, 12k$, and $18k$ all divide $(6k+1)(12k+1)(18k+1)-1$. Expanding the product we get $36k(36k^2+11k+1)$, which is clearly divisible by all 3 numbers. □

The smallest such number is $1729 = 7 \cdot 13 \cdot 19$. Chernick's method provides a simple and easy way of generating very large Carmichael numbers.

There are infinitely many Carmichael numbers

For most of the 20th century, it was believed that the list of Carmichael numbers may be infinitely extended, but no one could come up with a proof.

The breakthrough

Theorem (Alford, Granville, Pomerance)

Let $C(x)$ denote the number of Carmichael numbers less than x. There exists a constant c such that if $x \geq c$, then $C(x) > x^{2/7}$.

In 1994 William Alford, Andrew Granville, and Carl Pomerance published a paper proving this lower bound. As x approaches infinity, $C(x)$ also approaches infinity, thus there are infinitely many Carmichael numbers.

How it was proved

The idea behind the proof involves Number Theory and Group Theory

- Construct a large number L along with a set of k distinct primes such that for each prime p, we have $(p-1) \mid L$.
- Take a subset of the k primes and let its product be P. If $P \equiv 1 \pmod{L}$, then P is a Carmichael number from Korselt's criterion.
- Group Theory is used to find the lower bound on the amount of subsets that satisfy this property.
- There is no limitation on how large L can be, and as L approaches infinity, it can be shown that the lower bound on the number of subsets also approaches infinity.

Further bounds

- In 2005 Glyn Harman proved $C(x) > x^{0.332}$. Then in 2008, he improved his bound to $C(x) > x^{1/3}$
- Many mathematicians including Erdős and Knödel gave upper bounds to $C(x)$. Currently, the best bound is from Richard Pinch, who provided an upper bound of
$$C(x) < x \cdot \exp\left(-\frac{\ln(x)\ln(\ln(\ln(x)))}{\ln(\ln(x))}\right)$$

Bounds compared to C(x)

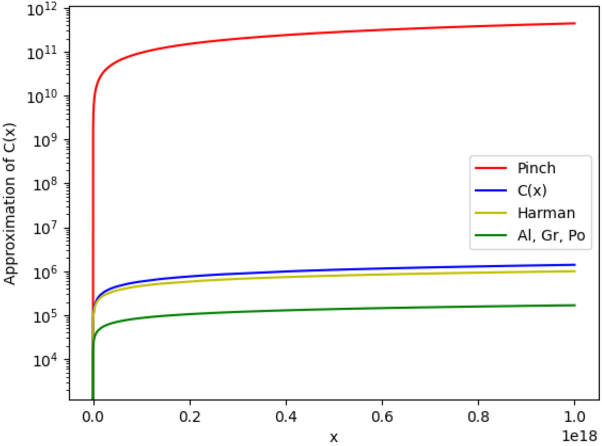


Figure: Upper and lower bounds compared to C(x) for $x \leq 10^{18}$

Finding larger Carmichael numbers

How do we check if a number n is a Carmichael number?

1. Check if all integers a satisfy $a^{n-1} \equiv 1 \pmod{n}$

Finding larger Carmichael numbers

How do we check if a number n is a Carmichael number?

1. Check if all integers a satisfy $a^{n-1} \equiv 1 \pmod{n}$
2. Prime factorize n and check if Korselt's criterion holds.

Finding larger Carmichael numbers

The prime factorization process is the most time consuming part. Checking Korselt's criterion will only take as many iterations as $\omega(n)$, which is the number of distinct prime factors of n.

Theorem (Hardy-Ramanujan)

For most integers n, $\omega(n) \sim \ln(\ln(n))$

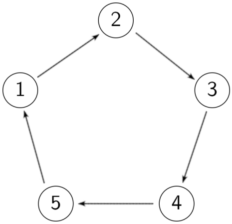
For example, if we take the 100th Carmichael number $9439201 = 61 \cdot 271 \cdot 571$, the Hardy-Ramanujan theorem states that $\omega(9439201) \sim 2.776$ which is pretty accurate.

Prime factorization algorithms

What is an efficient way of finding the prime factors of n? A simple method is to check all numbers from 2 to $\sqrt{n}$ and see if they divide n. This algorithm runs in $O(\sqrt{n})$.

Pollard's rho algorithm

This technique cleverly uses Floyd's cycle-detection algorithm to find prime factors. Let $g(x)$ return the child node of node x.



Definition

Define the sequence a as $a_0 = 1$, and $a_{i+1} = g(a_i)$.
Similarly, define the sequence b as $b_0 = a_0$, and $b_{i+1} = g(g(b_i))$.

Floyd's algorithm states that if there is an index $j > 0$ such that $a_j = b_j$, then the graph has a cycle.

Pollard's rho

The idea was to use a polynomial $f(x)$ to generate pseudorandom numbers, and detect cycles of $f(x) \pmod{p}$ for the prime divisors p of n.

Definition

Define the sequence x as $x_0 = f(0)$, and $x_{i+1} = f(x_i)$.
Similarly, define the sequence y as $y_0 = x_0$, and $y_{i+1} = f(f(y_i))$.

The sequence $f(x)$ taken modulo p must cycle, so there is an index j such that $x_j \equiv y_j \pmod{p}$. On each step $i > 0$, we check if $\gcd(|x_i - y_i|, n) > 1$. If it is, then it is very likely that it's a prime factor. If not, change $f(x)$ slightly and try again.

Pollard's rho

This algorithm runs in $O(n^{1/4})$ on average because the expected value of the smallest index j such that $x_j \equiv y_j \pmod{p}$ is $\sqrt{p}$. This method is a good way of checking large values of n.

Definition

A squarefree composite integer n is a Quasi-Carmichael number if every prime p that divides n satisfies $p + b \mid n + b$, with b being any nonzero integer.

This is a generalization of the Carmichael numbers. The smallest Quasi-Carmichael number is 35 with $b = -3$.

Further research

There are still many unsolved questions relating to Carmichael numbers. A few main ones are

- Understanding how Carmichael numbers are distributed (spacing and gaps)
- Finding the smallest Carmichael number with k prime factors
- Developing more efficient algorithms to identify Carmichael numbers

Solving these problems may also give us more insight on the properties of prime numbers.

Thank you

Thank you for listening!