Carmichael numbers

Pablo Cageao & Sergio Hernando

January 2025

Objective & index

Definition

Definition

An integer $n > 1$ is called a *Carmichael number* if n is composite and $(a, n) = 1 \rightarrow a^{n-1} \equiv 1 \mod n$ for all $a \in \mathbb{Z}$.

Korselt's theorem

Theorem (Korselt's Criterion)

A composite integer $n > 1$ is a Carmichael number if and only if

1. *n is squarefree.*
2. *for every prime p dividing n, $(p - 1)|(n - 1)$.*

Carmichael are squarefree

Carmichael is Squarefree.

Proceed by contradiction

1. $\exists p,\ p^2 | n$

Carmichael are squarefree

Carmichael is Squarefree.

Proceed by contradiction

1. $\exists p,\ p^2 | n$
2. $\exists a :\ a \equiv 1 + p \pmod{p^k}$ and $a \equiv 1 \pmod{n'}$.

Carmichael are squarefree

Carmichael is Squarefree.

Proceed by contradiction

1. $\exists p,\ p^2 | n$
2. $\exists a :\ a \equiv 1 + p \pmod{p^k}$ and $a \equiv 1 \pmod{n'}$.
3. $(a, n) = 1$, and $a^{n-1} \equiv 1 \pmod{n}$.

Carmichael are squarefree

Carmichael is Squarefree.

Proceed by contradiction

1. $\exists p,\ p^2 | n$
2. $\exists a : \ a \equiv 1 + p \pmod{p^k}$ and $a \equiv 1 \pmod{n'}$.
3. $(a, n) = 1$, and $a^{n-1} \equiv 1 \pmod{n}$.
4. $(1 + p)^{n-1} \equiv 1 \pmod{p^2}$.

Carmichael are squarefree

Carmichael is Squarefree.

Proceed by contradiction

1. $\exists p,\ p^2|n$
2. $\exists a:\ a \equiv 1+p \pmod{p^k}$ and $a \equiv 1 \pmod{n'}$.
3. $(a,n)=1$, and $a^{n-1} \equiv 1 \pmod{n}$.
4. $(1+p)^{n-1} \equiv 1 \pmod{p^2}$.
5. $1+(n-1)p \equiv 1 \pmod{p^2}$.

Carmichael are squarefree

Carmichael is Squarefree.

Proceed by contradiction

1. $\exists p,\ p^2 | n$
2. $\exists a :\ a \equiv 1 + p \pmod{p^k}$ and $a \equiv 1 \pmod{n'}$.
3. $(a, n) = 1$, and $a^{n-1} \equiv 1 \pmod{n}$.
4. $(1 + p)^{n-1} \equiv 1 \pmod{p^2}$.
5. $1 + (n - 1)p \equiv 1 \pmod{p^2}$.
6. $p \equiv 0 \pmod{p^2}$.

$\square$

Divisibility rule

Divisibility rule.

1. $\exists b$: $b \bmod p$ has order $p-1$.

Divisibility rule

Divisibility rule.

1. $\exists b$: $b \bmod p$ has order $p-1$.
2. $\exists a$: $a \equiv b \pmod{p}$ and $a \equiv 1 \pmod{n/p}$.

Divisibility rule

Divisibility rule.

1. $\exists b$: $b \bmod p$ has order $p-1$.
2. $\exists a$: $a \equiv b \pmod{p}$ and $a \equiv 1 \pmod{n/p}$.
3. $a^{n-1} \equiv b^{n-1} \equiv 1 \pmod{p}$.

$\square$

Sufficient conditions

Sufficient conditions.

For each prime p, for which $p|n$, if $a \in \mathbb{Z}$ satisfies $gcd(a,n) = 1$

1. $a^{p-1} \equiv 1 \pmod{p}$.

Sufficient conditions

Sufficient conditions.

For each prime p, for which $p|n$, if $a \in \mathbb{Z}$ satisfies $gcd(a,n) = 1$

1. $a^{p-1} \equiv 1 \pmod{p}$.
2. $a^{n-1} \equiv 1 \pmod{p}$.

Sufficient conditions

Sufficient conditions.

For each prime p, for which $p|n$, if $a \in \mathbb{Z}$ satisfies $gcd(a, n) = 1$

1. $a^{p-1} \equiv 1 \pmod{p}$.
2. $a^{n-1} \equiv 1 \pmod{p}$.

Then if n is squarefree, $a^{n-1} \equiv 1 \pmod{n}$. $\square$

Theorem statement

Theorem

A composite integer n is a Carmichael number if and only if $a^n \equiv a \mod n$ for all $a \in \mathbb{Z}$.

Sufficient

Lemma

for all $a \in Z$, $a^n \equiv a \mod n \Rightarrow (a, n) = 1 \rightarrow a^{n-1} \equiv 1 \mod n$

Proof.

Sufficient

Lemma

for all $a \in Z$, $a^n \equiv a \mod n \Rightarrow (a, n) = 1 \rightarrow a^{n-1} \equiv 1 \mod n$

Proof.

1. Let $a \in \mathbb{Z}$ s.t. $(a, n) = 1$.

Sufficient

Lemma

for all $a \in Z$, $a^n \equiv a \mod n \Rightarrow (a, n) = 1 \rightarrow a^{n-1} \equiv 1 \mod n$

Proof.

1. Let $a \in \mathbb{Z}$ s.t. $(a, n) = 1$.
2. $a^{-1}a^n \equiv a^{-1}a \mod n$.

Sufficient

Lemma

for all $a \in Z$, $a^n \equiv a \mod n \Rightarrow (a, n) = 1 \rightarrow a^{n-1} \equiv 1 \mod n$

Proof.

1. Let $a \in \mathbb{Z}$ s.t. $(a, n) = 1$.
2. $a^{-1}a^n \equiv a^{-1}a \mod n$.
3. $a^{n-1} \equiv 1 \mod n$.

$\square$

Necessary

Lemma

n is a Carmichael number $\Rightarrow a^n \equiv a \mod n$ *for all* $a \in Z$

Proof.

Necessary

Lemma

n is a Carmichael number $\Rightarrow a^n \equiv a \mod n$ for all $a \in Z$

Proof.

1. Is enough to show $a^n \equiv a \mod p$ for all p prime factor of n.

Necessary

Lemma

n is a Carmichael number $\Rightarrow a^n \equiv a \mod n$ *for all* $a \in Z$

Proof.

1. Is enough to show $a^n \equiv a \mod p$ for all p prime factor of n.
2. $a \equiv 0 \mod p$.

Necessary

Lemma

n is a Carmichael number $\Rightarrow a^n \equiv a \mod n$ *for all* $a \in Z$

Proof.

1. Is enough to show $a^n \equiv a \mod p$ for all p prime factor of n.
2. $a \equiv 0 \mod p$.
3. $a \not\equiv 0 \mod p$.

Necessary

Lemma

n is a Carmichael number $\Rightarrow a^n \equiv a \mod n$ for all $a \in Z$

Proof.

1. Is enough to show $a^n \equiv a \mod p$ for all p prime factor of n.
2. $a \equiv 0 \mod p$.
3. $a \not\equiv 0 \mod p$.
4. $a^{p-1} \equiv 1 \mod p$.

Necessary

Lemma

n is a Carmichael number $\Rightarrow a^n \equiv a \mod n$ for all $a \in Z$

Proof.

1. Is enough to show $a^n \equiv a \mod p$ for all p prime factor of n.
2. $a \equiv 0 \mod p$.
3. $a \not\equiv 0 \mod p$.
4. $a^{p-1} \equiv 1 \mod p$.
5. $(p-1)|(n-1) \Rightarrow a^{n-1} \equiv 1 \mod p$.

Necessary

Lemma

n is a Carmichael number $\Rightarrow a^n \equiv a \mod n$ for all $a \in Z$

Proof.

1. Is enough to show $a^n \equiv a \mod p$ for all p prime factor of n.
2. $a \equiv 0 \mod p$.
3. $a \not\equiv 0 \mod p$.
4. $a^{p-1} \equiv 1 \mod p$.
5. $(p-1)|(n-1) \Rightarrow a^{n-1} \equiv 1 \mod p$.
6. $a^n \equiv a \mod p$.

□

561 is a Carmichael number

$$561 = 3 * 11 * 17$$

$$2|560$$

$$10|560$$

$$16|560$$

561 is the lowest Carmichael number

Lemma (Decision criteria)

For every number n, so that $n < 561$, try:

1. *If $p|n$ then $p-1|n-1$*
2. *n is squarefree*

Statements

Corollary (Jack Chernick, 1939)

If k is a positive integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime, then the product $n=(6k+1)(12k+1)(18k+1)$ is a Carmichael number.

Statements

Corollary (Jack Chernick, 1939)

If k is a positive integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime, then the product $n = (6k+1)(12k+1)(18k+1)$ is a Carmichael number.

Lemma

Every Carmichael number

Statements

Corollary (Jack Chernick, 1939)

If k is a positive integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime, then the product $n = (6k+1)(12k+1)(18k+1)$ is a Carmichael number.

Lemma

Every Carmichael number

- *Is odd.*

Statements

Corollary (Jack Chernick, 1939)

If k is a positive integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime, then the product $n = (6k+1)(12k+1)(18k+1)$ is a Carmichael number.

Lemma

Every Carmichael number

- *Is odd.*
- *Has at least three different prime factors.*

Statements

Corollary (Jack Chernick, 1939)

If k is a positive integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime, then the product $n=(6k+1)(12k+1)(18k+1)$ is a Carmichael number.

Lemma

Every Carmichael number

- *Is odd.*
- *Has at least three different prime factors.*
- *Satisfies that every prime factor of n is less than $\sqrt{n}$.*

Chernick's construction

Corollary (Jack Chernick, 1939)

If k is a positive integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime, then the product $n = (6k+1)(12k+1)(18k+1)$ is a Carmichael number.

Chernick's construction

Corollary (Jack Chernick, 1939)

If k is a positive integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime, then the product $n=(6k+1)(12k+1)(18k+1)$ is a Carmichael number.

Proof.

Korselt

Chernick's construction

Corollary (Jack Chernick, 1939)

If k is a positive integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime, then the product $n=(6k+1)(12k+1)(18k+1)$ is a Carmichael number.

Proof.

Korselt

- n composite greater than 1

Chernick's construction

Corollary (Jack Chernick, 1939)

If k is a positive integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime, then the product $n = (6k+1)(12k+1)(18k+1)$ is a Carmichael number.

Proof.

Korselt

- n composite greater than 1
- n is squarefree

Chernick's construction

Corollary (Jack Chernick, 1939)

If k is a positive integer such that $6k+1$, $12k+1$, *and* $18k+1$ *are all prime, then the product* $n = (6k+1)(12k+1)(18k+1)$ *is a Carmichael number.*

Proof.

Korselt

- n composite greater than 1
- n is squarefree
- for every prime p dividing n, also $(p-1)|(n-1)$.

Chernick's construction

Corollary (Jack Chernick, 1939)

If k is a positive integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime, then the product $n = (6k+1)(12k+1)(18k+1)$ is a Carmichael number.

Proof.

Korselt

- n composite greater than 1
- n is squarefree
- for every prime p dividing n, also $(p-1)|(n-1)$.
  - $n \equiv (0+1)(0+1)(0+1) \equiv 1 \mod 6k$.
  - $n \equiv (6k+1)(0+1)(6k+1) \equiv 1 \mod 12k$.
  - $n \equiv (6k+1)(12k+1)(0+1) \equiv 1 \mod 18k$.

Lemma

Every Carmichael number is odd.

Proof.

Let n be a Carmichael number

Lemma

Every Carmichael number is odd.

Proof.

Let n be a Carmichael number

1. $n - 1$ relatively prime with n.

Lemma

Every Carmichael number is odd.

Proof.

Let n be a Carmichael number

1. $n - 1$ relatively prime with n.
2. $(n-1)^{(n-1)} \equiv (-1)^{(n-1)} \equiv 1 \mod n$.

Lemma

Every Carmichael number is odd.

Proof.

Let n be a Carmichael number

1. $n-1$ relatively prime with n.
2. $(n-1)^{(n-1)} \equiv (-1)^{(n-1)} \equiv 1 \mod n$.
3. $n > 2 \Rightarrow -1 \not\equiv 1 \mod n$.

Lemma

Every Carmichael number is odd.

Proof.

Let n be a Carmichael number

1. $n-1$ relatively prime with n.
2. $(n-1)^{(n-1)} \equiv (-1)^{(n-1)} \equiv 1 \mod n$.
3. $n > 2 \Rightarrow -1 \not\equiv 1 \mod n$.
4. $n-1$ even.

□

Lemma

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

Proof.

Let n be a Carmichael number and p one of it's prime factors.

Lemma

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

Proof.

Let n be a Carmichael number and p one of it's prime factors.

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

Lemma

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

Proof.

Let n be a Carmichael number and p one of it's prime factors.

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

Lemma

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

Proof.

Let n be a Carmichael number and p one of it's prime factors.

1. $\frac{n-1}{p-1} = \frac{p(n/p)-1}{p-1} = \frac{(p-1)(n/p)+n/p-1}{p-1} = \frac{n}{p} + \frac{n/p-1}{p-1}$.
2. $p - 1 | n/p - 1$.
3. $p \leq n/p \Rightarrow p^2 \leq n$.

Lemma

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

Proof.

Let n be a Carmichael number and p one of it's prime factors.

1. $\frac{n-1}{p-1} = \frac{p(n/p)-1}{p-1} = \frac{(p-1)(n/p)+n/p-1}{p-1} = \frac{n}{p} + \frac{n/p-1}{p-1}$.
2. $p-1|n/p-1$.
3. $p \leq n/p \Rightarrow p^2 \leq n$.
4. $n \neq p^2$ (squarefree).

$\square$

Lemma

Every Carmichael number has at least three different prime factors.

Proof.

Contradiction

$$n = pq \Rightarrow p > \sqrt{n} \text{ or } q > \sqrt{n}$$

$\square$

Future work

Conjecture (Dickson's conjecture)

There are infinitely many numbers generated by Chernick's construction.

Theorem (W. R. Alford, A. Granville, C. Pomerance, 1994)

There are infinitely many Carmichael numbers.