On Generalized Carmichael Numbers

Tae Kyu Kim
mentor: Yongyi Chen

Monta Vista High School

Oct 18, 2020
MIT PRIMES Conference
Historical Background

Theorem (Fermat, 1860)

If $p$ is prime, then $p$ divides $a^p - a$ for all integers $a$.

Example

5 is prime, so 5 divides

$0^5 - 0 = 0$, $3^5 - 3 = 240$,

$1^5 - 1 = 0$, $4^5 - 4 = 1020$,

$2^5 - 2 = 30$,

Question: Is the converse true?
Question: Is the converse true?

No! In 1910, Carmichael showed that 561 divides $a^{561} - a$ for all integers $a$. 

Theorem (Korselt's criterion)

A positive integer $n$ divides $a^n - a$ for all integers $a$ if and only if $n$ is squarefree and $p - 1$ divides $n - 1$ for all primes $p$ dividing $n$. 

Example (561 is a counterexample)

Prime factorization of 561: $3 \times 11 \times 17$.

Notice that $3 - 1 = 2$, $11 - 1 = 10$, $17 - 1 = 16$ divide $561 - 1 = 560$. 

Tae Kyu Kim
On Generalized Carmichael Numbers
October 2020
Historical Background

Question: Is the converse true?

No! In 1910, Carmichael showed that 561 divides $a^{561} - a$ for all integers $a$.

**Theorem (Korselt’s criterion)**

A positive integer $n$ divides $a^n - a$ for all integers $a$ if and only if $n$ is squarefree and $p - 1$ divides $n - 1$ for all primes $p$ dividing $n$. 

Example (561 is a counterexample)

Prime factorization of 561: $3 \times 11 \times 17$.

Notice that $3 - 1 = 2$, $11 - 1 = 10$, $17 - 1 = 16$ divide $561 - 1 = 560$. 
Historical Background

Question: Is the converse true?

No! In 1910, Carmichael showed that 561 divides $a^{561} - a$ for all integers $a$.

Theorem (Korselt’s criterion)

A positive integer $n$ divides $a^n - a$ for all integers $a$ if and only if $n$ is squarefree and $p - 1$ divides $n - 1$ for all primes $p$ dividing $n$.

Example (561 is a counterexample)

Prime factorization of 561: $3 \times 11 \times 17$.
Notice that $3 - 1 = 2$, $11 - 1 = 10$, $17 - 1 = 16$ divide $561 - 1 = 560$. 
Historical Background

Definition (Carmichael number)

The composite integers $n$ with the property that $n$ divides $a^n - a$ for all integers $a$ are called the **Carmichael numbers**.

First 8 Carmichael numbers:

\{561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, \ldots\}
### Definition (Carmichael number)

The composite integers $n$ with the property that $n$ divides $a^n - a$ for all integers $a$ are called the **Carmichael numbers**.

First 8 Carmichael numbers:

\[
\{561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, \ldots \}
\]

### Theorem (Alford, Granville, Pomerance)

There are infinitely many Carmichael numbers. The number of Carmichael numbers less than $X$ is at least $X^{\frac{2}{7}}$ for sufficiently large $X$.

### Conjecture (Erdős)

There are $X^{1-o(1)}$ Carmichael numbers less than $X$. 
Question

For what positive integers \( n \) does \( n \) divide \( a^{n-1} - a \) for all integers \( a \)?
Motivation

Question

For what positive integers $n$ does $n$ divide $a^{n-1} - a$ for all integers $a$?

1. For every prime $p$ dividing $n$, $p - 1$ must divide $n$.
2. $n$ is squarefree.

$\Rightarrow \quad n \in \{1, 2, 6, 42, 1806\}$. 
Our Main Problem

Question

Given an integer $k$, for what integers $n > \max(k, 0)$ does $n$ divide $a^{n-k+1} - a$ for all integers $a$?
Our Main Problem

Question

Given an integer \( k \), for what integers \( n > \max(k, 0) \) does \( n \) divide \( a^{n-k+1} - a \) for all integers \( a \)?

Definition

\[
C_k = \{ n > \max(k, 0) : n \text{ divides } a^{n-k+1} - a \text{ for all integers } a \}
\]

\( C_1 = \) all primes and Carmichael numbers

\( C_0 = \{1, 2, 6, 42, 1806\} \)

\( C_{-1} = \) ???
Proposition (Generalized Korselt’s Criterion)

An integer \( n > \max(k, 0) \) is in \( C_k \) if and only if \( n \) is squarefree and \( p - 1 \) divides \( n - k \) for all primes \( p \) dividing \( n \).
First Steps

**Proposition (Generalized Korselt’s Criterion)**

An integer $n > \max(k, 0)$ is in $C_k$ if and only if $n$ is squarefree and $p - 1$ divides $n - k$ for all primes $p$ dividing $n$.

**Definition**

The *Carmichael function* $\lambda(n)$ is defined as the smallest positive integer such that $a^{\lambda(n)} \equiv a \pmod{n}$ for all integers $a$.

For squarefree $n$,

$$\lambda(n) = \lcm_{p \mid n} \{p - 1\}.$$

**Proposition (Alternate Korselt’s Criterion)**

An integer $n > \max(k, 0)$ is in $C_k$ if and only if $n$ is squarefree and $\lambda(n)$ divides $n - k$. 
Approach for $k > 0$

<table>
<thead>
<tr>
<th>$k$</th>
<th>$C_k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>${2, 3, 5, 7, 11, 13, 17, \ldots}$</td>
</tr>
<tr>
<td>2</td>
<td>${6, 10, 14, 22, 26, 30, 34, \ldots}$</td>
</tr>
<tr>
<td>3</td>
<td>${15, 21, 33, 39, 51, 57, 69, \ldots}$</td>
</tr>
<tr>
<td>5</td>
<td>${65, 85, 145, 165, 185, 205, \ldots}$</td>
</tr>
</tbody>
</table>

Table: $C_k$ for $k = 1, 2, 3, 5$
Approach for $k > 0$

<table>
<thead>
<tr>
<th>$k$</th>
<th>$C_k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>${2, 3, 5, 7, 11, 13, 17, \ldots}$</td>
</tr>
<tr>
<td>2</td>
<td>${6, 10, 14, 22, 26, 30, 34, \ldots}$</td>
</tr>
<tr>
<td>3</td>
<td>${15, 21, 33, 39, 51, 57, 69, \ldots}$</td>
</tr>
<tr>
<td>5</td>
<td>${65, 85, 145, 165, 185, 205, \ldots}$</td>
</tr>
</tbody>
</table>

Table: $C_k$ for $k = 1, 2, 3, 5$

For squarefree $k$, set $n = km$ where $m$ is a squarefree integer coprime to $k$. 
### Approach for $k > 0$

<table>
<thead>
<tr>
<th>$k$</th>
<th>$C_k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>{2, 3, 5, 7, 11, 13, 17, \ldots}</td>
</tr>
<tr>
<td>2</td>
<td>{6, 10, 14, 22, 26, 30, 34, \ldots}</td>
</tr>
<tr>
<td>3</td>
<td>{15, 21, 33, 39, 51, 57, 69, \ldots}</td>
</tr>
<tr>
<td>5</td>
<td>{65, 85, 145, 165, 185, 205, \ldots}</td>
</tr>
</tbody>
</table>

**Table:** $C_k$ for $k = 1, 2, 3, 5$

For squarefree $k$, set $n = km$ where $m$ is a squarefree integer coprime to $k$.

\[\lambda(n) | n - k \iff \lambda(km) | k(m - 1)\]

\[\iff \begin{cases} 
\lambda(k) | k(m - 1) \\
\lambda(m) | k(m - 1)
\end{cases}\]
Approach for $k > 0$

With $n = km$:

1. $\lambda(k) \mid k(m - 1)$ leads to the congruence condition $m \equiv 1 \pmod{\frac{\lambda(k)}{\gcd(\lambda(k), k)}}$.

2. $\lambda(m) \mid k(m - 1)$ is a looser variant of $\lambda(m) \mid m - 1$. In particular, all primes satisfy this condition.
Approach for \( k > 0 \)

With \( n = km \):

1. \( \lambda(k) \mid k(m - 1) \) leads to the congruence condition \( m \equiv 1 \mod \left( \frac{\lambda(k)}{\gcd(\lambda(k), k)} \right) \).

2. \( \lambda(m) \mid k(m - 1) \) is a looser variant of \( \lambda(m) \mid m - 1 \). In particular, all primes satisfy this condition.

**Theorem (Dirichlet)**

Let \( a, m \) be coprime integers. The number of primes \( \equiv a \pmod{m} \) less than \( X \) is approximately \( \frac{1}{\phi(m)} \cdot \frac{X}{\log(X)} \), where \( \phi \) is Euler’s Totient function. In particular, there are infinitely many primes \( \equiv a \pmod{m} \).

**Theorem (Makowski, 1962)**

For any squarefree \( k > 0 \), there are infinitely many elements in \( C_k \).
Conjectures for $k < 0$

For $k > 0$: $C_k = \text{noise} + k \cdot \left\{ \text{primes } \equiv 1 \pmod{\frac{\lambda(k)}{\gcd(\lambda(k),k)}} \right\}$.

For $k < 0$: $C_k = \text{noise}.$

(noise = generalized Carmichael numbers)
Conjectures for $k < 0$

For $k > 0$: $C_k = \text{noise} + k \cdot \left\{ \text{primes} \equiv 1 \mod \left( \frac{\lambda(k)}{\gcd(\lambda(k), k)} \right) \right\}$.

For $k < 0$: $C_k = \text{noise}$.

(noise = generalized Carmichael numbers)

Conjecture (Chen, Kim)

Let $k > 0$. Then

$$\lim_{X \to \infty} \frac{|C_{-k} \cap (0, X]|}{|C_k \cap (0, X]| - \frac{\gcd(\lambda(k), k)}{\lambda(k)} \pi \left( \frac{X}{k} \right)} = 1$$

where $\pi(X)$ denotes the number of primes $\leq X$. 
General patterns

1. $n$ is usually a multiple of $k$
2. $n$ and $k$ usually share factors
General patterns

1. $n$ is usually a multiple of $k$
2. $n$ and $k$ usually share factors

Example

For $k = -11$ and large $n$:
$C_{-11} = \{\ldots, 283309, 306229, 319189, 337249, 352429, 382789, \ldots\}$
General patterns

1. $n$ is usually a multiple of $k$
2. $n$ and $k$ usually share factors

Example

For $k = -11$ and large $n$:
$C_{-11} = \{ \ldots, 283309, 306229, 319189, 337249, 352429, 382789, \ldots \}$

Heuristic (Chen, Kim)

For large $n \in C_k$ and small integers $m$, $n - k$ will often be divisible by $m$. The proportion of $n$ with such property increases with the value of $n$ and decreases with the value of $m$.

Idea: for large $n$, $m$ often divides $\lambda(n)$. 
Simple cases (Short products)

Proposition (Halbeisen, Hungerbühler)

If $k \neq 1$, then $C_k$ contains finitely many primes.

Proposition (Halbeisen, Hungerbühler)

Unless $k > 0$ and $k$ is prime, there are finitely many pairs of primes $p, q$ such that $pq \in C_k$.

Proposition (Chen, Kim)

For any integers $k$ and $l > k$, there are finitely many pairs of primes $p, q$ such that $lpq \in C_k$.

Corollary (Chen, Kim)

For any $k < 0$, there are finitely many triples of primes $p, q, r$ such that $pqr \in C_k$ and $p - 1$ divides $q - 1$ and $r - 1$. 
Alternate Problems

1. Given integers $a, k$, for what integers $n > \max(k, 0)$ does $n$ divide $a^{n-k+1} - a$? When does $a^{n-k} - 1$?

We extend the work of Kiss and Phong [KP87] on $k > 0$ to all integers $k$:

Theorem (Chen, Kim)

*If $a \geq 2$ and $k$ are integers with $(k, a) \neq (0, 2)$, there are infinitely many positive integers $n$ such that $a^{n-k} \equiv 1 \pmod{n}$. If $(k, a) = (0, 2)$, then there are no integers $n > 1$ such that $a^{n-k} \equiv 1 \pmod{n}$.***
Alternate Problems

2. Given an integer \( k \), for what \( n \) does \( \lambda(n) \) divide \( n - k \)?

The exponents in the prime factorization of \( n \) are bounded by \( k \):

**Proposition (Chen, Kim)**

If \( \lambda(n) \) divides \( n - k \) and \( n = \prod_{i=1}^{r} p_i^{e_i} \), then \( \prod_{i=1}^{r} p_i^{e_i-1} \) divides \( k \).
Summary

1 Historical background
   • Fermat’s little theorem, Carmichael numbers
   • Korselt’s criterion

2 Our research
   • Generalization of Korselt’s criterion
   • Patterns in data → theorems, conjectures, heuristics
   • Simpler cases with 2, 3 prime factors
   • Alternative problems
Special thanks to Stefan Wehmeier for suggesting the project and providing advice on the best direction for research. I would also like to thank Yongyi Chen for his immense support in mentoring this project. Finally, I would like to thank the MIT PRIMES program for the research opportunity.
References


