Building Carmichael numbers with a large number of prime factors

Ivana Trummová

Spring school of algebra, Rapotín

April 7, 2017

Introduction

Definition (Carmichael number)

A Carmichael number C is a composite integer for which the identity

$$a^{C-1} \equiv 1 \pmod{C}$$

holds for all values of a coprime to C.

Robert Daniel Carmichael

Fermat primality test

Theorem (Fermat's Little Theorem)

Let p be a prime number. Then

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

for all values of $a = 1, 2, \ldots, p-1$.

Fermat primality test

How to do the test?

- Suppose N is the tested number.
- Take a random number a coprime to N
- Check whether $a^{N-1} \equiv 1 \pmod{N}$

Fermat primality test

How to do the test?

- Suppose N is the tested number.
- Take a random number a coprime to N
- Check whether $a^{N-1} \equiv 1 \pmod{N}$
- If not, N is not a prime.

Carmichael numbers

Theorem (Korselt's criterion)

A Carmichael number C is an odd squarefree composite number, $C = p_1 p_2 \cdots p_r$, with $r \geq 3$ such that

$$C - 1 \equiv 0 \pmod{(p_i - 1)} \quad \text{for} \quad 1 \leq i \leq r.$$

Discovery

- $561 = 3 \cdot 11 \cdot 17$ $\qquad (2 \mid 560; \quad 10 \mid 560; \quad 16 \mid 560)$

Discovery

- $561 = 3 \cdot 11 \cdot 17$ $(2 \mid 560;\quad 10 \mid 560;\quad 16 \mid 560)$
- $1105 = 5 \cdot 13 \cdot 17$ $(4 \mid 1104;\quad 12 \mid 1104;\quad 16 \mid 1104)$
- $1729 = 7 \cdot 13 \cdot 19$ $(6 \mid 1728;\quad 12 \mid 1728;\quad 18 \mid 1728)$
- $2465 = 5 \cdot 17 \cdot 29$ $(4 \mid 2464;\quad 16 \mid 2464;\quad 28 \mid 2464)$
- $2821 = 7 \cdot 13 \cdot 31$ $(6 \mid 2820;\quad 12 \mid 2820;\quad 30 \mid 2820)$
- $6601 = 7 \cdot 23 \cdot 41$ $(6 \mid 6600;\quad 22 \mid 6600;\quad 40 \mid 6600)$
- $8911 = 7 \cdot 19 \cdot 67$ $(6 \mid 8910;\quad 18 \mid 8910;\quad 66 \mid 8910)$
- Václav Šimerka (1885), Korselt, Carmichael

Carmichael function

Definition

Carmichael function of a positive integer N, denoted $\lambda(N)$, is defined as the smallest positive integer M such that

$$a^M \equiv 1 \pmod{N}$$

for every integer a that is coprime to N.

Carmichael function

$$\lambda(p) = \varphi(p) = p - 1 \qquad \textit{for primes } p > 2;$$

$$\lambda(N) = \lambda(p_1^{h_1} \cdots p_n^{h_n}) = lcm(\lambda(p_1^{h_1}) \cdots \lambda(p_n^{h_n})).$$

For squarefree numbers we have $\lambda(C) = lcm(p_1 - 1, \ldots, p_r - 1)$.

Carmichael numbers

Alternatively:

$$\lambda(C)|C-1$$

where λ denotes Carmichael function.

$$(\lambda(C) = lcm(p_1 - 1, \ldots, p_r - 1)|C-1$$

since

$$C - 1 \equiv 0 \pmod{(p_i - 1)} \quad for \quad 1 \leq i \leq r.)$$

Carmichael numbers

Another property:

$$p_j \not\equiv 1 \pmod{p_i} \quad \textit{for} \quad 1 \leq i < j \leq r.$$

The Idea

We want to search for Carmichael numbers C with a fixed number of prime factors. The best start is to fix the value of Λ.
Let's have a set of all possible factors of C:

$$S(\Lambda) = \{p, p \ prime, p \nmid \Lambda, p - 1 | \Lambda\}$$

The Idea

$$S(\Lambda) = \{p, p \text{ prime}, p \nmid \Lambda, p-1|\Lambda\}$$

$\Longrightarrow$ a squarefree product N of elements of $S(\Lambda)$ satisfies

$$\lambda(N)|\Lambda$$

- $N = p_1 \cdots p_n$
- $\lambda(N) = lcm(p_1 - 1, \ldots, p_n - 1)$

The Idea

$$S(\Lambda) = \{p, p \text{ prime}, p \nmid \Lambda, p-1|\Lambda\}$$

$$\implies p_j \not\equiv 1 \pmod{p_i}$$

for $1 \leq i < j \leq r$.
(If $p_j \equiv 1 \pmod{p_i} \implies p_i|(p_j - 1), but\ (p_j - 1)|\Lambda$.)

The Idea

Suppose we want to find Carmichael numbers with r factors built up with the primes of $S := S(\Lambda)$.

The Idea

Suppose we want to find Carmichael numbers with r factors built up with the primes of $S := S(\Lambda)$.

- It is enough to look for r distinct elements $p_1, \ldots, p_r$ such that

$$C = p_1 \cdots p_r \equiv 1 \pmod{\Lambda}$$

The Idea

Suppose we want to find Carmichael numbers with r factors built up with the primes of $S := S(\Lambda)$.

- It is enough to look for r distinct elements $p_1, \ldots, p_r$ such that

$$C = p_1 \cdots p_r \equiv 1 \pmod{\Lambda}$$

- If this is the case, we have $C - 1 \equiv 0 \pmod{\lambda(C)}$ since $\lambda(N) | \Lambda$.

The Idea

Do we really have a Carmichael number?

The Idea

Do we really have a Carmichael number?

- A Carmichael number C is an odd squarefree composite number, $C = p_1 \cdots p_r$, with $r \geq 3$ such that

$$C - 1 \equiv 0 \pmod{(p_i - 1)} \quad \textit{for} \quad 1 \leq i \leq r.$$

The Idea

Do we really have a Carmichael number?

- A Carmichael number C is an odd squarefree composite number, $C = p_1 \cdots p_r$, with $r \geq 3$ such that

$$C - 1 \equiv 0 \pmod{(p_i - 1)} \quad \textit{for} \quad 1 \leq i \leq r.$$

- $\lambda(C) | C - 1$

The Idea

Do we really have a Carmichael number?

- A Carmichael number C is an odd squarefree composite number, $C = p_1 \cdots p_r$, with $r \geq 3$ such that

$$C - 1 \equiv 0 \pmod{(p_i - 1)} \quad \textit{for} \quad 1 \leq i \leq r.$$

- $\lambda(C) | C - 1$
- $p_j \not\equiv 1 \pmod{p_i} \quad \textit{for} \quad 1 \leq i < j \leq r.$

Informal Description

- Let $t = |S|$

Informal Description

- Let $t = |S|$
- and let $P(S) = \prod_{p \in S} p$

Informal Description

- Let $t = |S|$
- and let $P(S) = \prod_{p \in S} p$
- r prime factors, $r < t$ and $u := t - r$ (small)

Informal Description

- Let $t = |S|$
- and let $P(S) = \prod_{p \in S} p$
- r prime factors, $r < t$ and $u := t - r$ (small)
- We look for u primes of S, say $D = \{d_1, \ldots, d_u\}$ such that

$$\Pi(D) = \frac{P(S)}{(d_1 \cdots d_u)} \equiv 1 \pmod{\Lambda}$$

Informal Description

- Let $t = |S|$
- and let $P(S) = \prod_{p \in S} p$
- r prime factors, $r < t$ and $u := t - r$ (small)
- We look for u primes of S, say $D = \{d_1, \ldots, d_u\}$ such that

$$\Pi(D) = \frac{P(S)}{(d_1 \cdots d_u)} \equiv 1 \pmod{\Lambda}$$

- We examine all u-tuples of primes d_i in S in order to find a fitting one.

The Procedure

procedure **FindCarmichael**$(S(\Lambda), r)$
(we want r-factor numbers)

1. Set $t = |S|$; $u := t - r$.
2. Compute $P_\Lambda = P(S) \pmod{\Lambda}$
3. For all u-tuples of distinct primes $d_1, \ldots, d_u$ check whether

$$d_1 \cdots d_u \equiv P(S) \pmod{\Lambda}$$

A Rough Analysis

We build the sets of squarefree products of u elements of S

$$S_u = \{p_1 \cdots p_u \pmod{\Lambda}, p_i \neq p_j, p_i \in S\}$$

A Rough Analysis

We build the sets of squarefree products of u elements of S

$$S_u = \{p_1 \cdots p_u \pmod{\Lambda}, p_i \neq p_j, p_i \in S\}$$

- When does S_u contain the residue P_Λ?

A Rough Analysis

It certainly does if $S_u \supseteq \mathbb{Z}_\Lambda^*$. A necessary condition for that is

$$\binom{t}{u} > |\mathbb{Z}_\Lambda^*| = \varphi(\Lambda).$$

A Rough Analysis

It certainly does if $S_u \supseteq \mathbb{Z}_\Lambda^*$. A necessary condition for that is

$$\binom{t}{u} > |\mathbb{Z}_\Lambda^*| = \varphi(\Lambda).$$

- this condition is sufficient in practice

Choice of Λ

- Let u_0 denote the first u satisfying

$$\binom{t}{u} > |\mathbb{Z}_\Lambda^*| = \varphi(\Lambda).$$

Choice of Λ

- Let u_0 denote the first u satisfying

$$\binom{t}{u} > |\mathbb{Z}_\Lambda^*| = \varphi(\Lambda).$$

- $u \geq u_0 \implies$ Probability that $p_1 \cdots p_u \equiv P(S) \pmod{\Lambda}$ is $\frac{1}{\varphi(\Lambda)}$

Choice of Λ

- Let u_0 denote the first u satisfying

$$\binom{t}{u} > |\mathbb{Z}_\Lambda^*| = \varphi(\Lambda).$$

- $u \geq u_0 \implies$ Probability that $p_1 \cdots p_u \equiv P(S) \pmod{\Lambda}$ is $\frac{1}{\varphi(\Lambda)}$
- We want Λ with a small value of $\varphi(\Lambda)$

How to choose a good Λ?

- Carmichael number with many factors
- We want $S(\Lambda)$ to contain many prime numbers
- Λ must have many divisors

How to choose a good Λ?

- Carmichael number with many factors
- We want $S(\Lambda)$ to contain many prime numbers
- Λ must have many divisors
- $\mathcal{Q} = \{q_1 = 2, 3, \ldots, q_s\}$
- $\mathcal{A} = \{A_1, \ldots, A_s\}$

How to choose a good Λ?

- Carmichael number with many factors
- We want $S(\Lambda)$ to contain many prime numbers
- Λ must have many divisors
- $\mathcal{Q} = \{q_1 = 2, 3, \ldots, q_s\}$
- $\mathcal{A} = \{A_1, \ldots, A_s\}$
- $\Lambda(\mathcal{Q}, \mathcal{A}) = q_1^{A_1} \cdots q_s^{A_s}$.

How to choose a good Λ?

The set S is then

$$S(\mathcal{Q},\mathcal{A}) = \{p \text{ prime}, p \notin \mathcal{Q} \text{ and } p-1 = \prod_{i=1}^{s} q_i^{\alpha_i}, 0 \leq \alpha_i \leq A_i\}$$

Do you remember?

$$S(\Lambda) = \{p \text{ prime}, p \nmid \Lambda, p-1 | \Lambda\}$$

Implementation

Suppose that $(\mathcal{Q}, \mathcal{A})$ is given.

Implementation

Suppose that $(\mathcal{Q}, \mathcal{A})$ is given.

- How to efficiently check whether

$$d_1 \cdots d_u \equiv P(S) \pmod{\Lambda}?$$

Implementation

Suppose that $(\mathcal{Q}, \mathcal{A})$ is given.

- How to efficiently check whether

$$d_1 \cdots d_u \equiv P(S) \pmod{\Lambda}?$$

- CRT!

Implementation

- $\Lambda = m_1 \cdots m_k$ (integers $m_i < 2^{16}$, $m_1 > \cdots > m_k$)
- $$\Pi(D) = \frac{P(S)}{(d_1 \cdots d_u)} \equiv 1 \pmod{m_j}$$
- $(d_1 \cdots d_u) \equiv P(S) \pmod{m_j}$

Implementation

What's the cost?
The algorithm C_0 needs to examine all u-tuples of primes in S.

$$O(\binom{t}{u}(uM))$$

where $M =$ multiplication modulo a 16-bit number.
Asymptotically $C_0(t) = O(t^u)$.

First improvement

We examine all $(u-1)$-tuples and find d_u such that

$$d_u \equiv \frac{P(S)}{d_1 \cdots d_{u-1}} \pmod{\Lambda}.$$

First improvement

We examine all $(u-1)$-tuples and find d_u such that

$$d_u \equiv \frac{P(S)}{d_1 \cdots d_{u-1}} \pmod{\Lambda}.$$

- if d_u is in S and different from the previous d_i's, we have found a Carmichael number.

First improvement

We examine all $(u-1)$-tuples and find d_u such that

$$d_u \equiv \frac{P(S)}{d_1 \cdots d_{u-1}} \pmod{\Lambda}.$$

- if d_u is in S and different from the previous d_i's, we have found a Carmichael number.
- S has to be sorted.

First improvement

Final cost:

$$O(\binom{t}{u-1}((u-1)M + c_1 logt))$$

Asymptotically: $C_1(t) = O(t^{u-1} logt)$ (bigger space is needed)

Second improvement

- $S_u = \{p_1 \cdots p_u \pmod{\Lambda}, p_i \neq p_j, p_i \in S\}$

Second improvement

- $S_u = \{p_1 \cdots p_u \pmod{\Lambda}, p_i \neq p_j, p_i \in S\}$
- $S_2 = \{pq \pmod{\Lambda}, p \neq q, p, q \in S\}$ ($+$ sorting: $O(t^2 log t)$ operations)

Second improvement

- $S_u = \{p_1 \cdots p_u \pmod{\Lambda}, p_i \neq p_j, p_i \in S\}$
- $S_2 = \{pq \pmod{\Lambda}, p \neq q, p, q \in S\}$ ($+$ sorting: $O(t^2 log t)$ operations)
- then we look for $(u-2)$-tuples of elements in S such that

$$\frac{P(S)}{d_1 \cdots d_{u-2}} \pmod{\Lambda}$$

is in S_2.

Second improvement

- When this is so, there exists p and q in S such that

$$\frac{P(S)}{d_1 \cdots d_{u-2}} \equiv pq \pmod{\Lambda}$$

- and we have Carmichael number.
- cost: $C_2(t) = O(t^{u-2} log t)$

Zhang's method

- highly composite values of Λ
- $S(\Lambda) = \Sigma_1 \cup \Sigma_2$, Σ_2 contains $t - n$ primes
- for a subset T of Σ_2 with $t - n - h$ elements he computes

$$f = \prod_{p \in T} p$$

and

$$g \equiv 1/f \pmod{\Lambda}.$$

Zhang's method

If g is squarefree and has all prime factors in Σ_1, then fg is a Carmichael number.

Lehmer's problem

Does there exist composite integers N for which

$$\varphi(N)|N-1$$

(where φ denotes the Euler's function)?

- No such numbers are known.
- N would need to be a Carmichael number, since for every element b in the integers $\pmod N$: $ord(b)|\varphi(n)|(n-1)$
- $b^{n-1} \equiv 1 \pmod N$

Lehmer's problem

- In 1980 Cohen and Hagis proved that, for any solution N to the problem, $N > 10^{20}$ and number of prime factors has to be ≥ 14.
- In 1988 Hagis showed that if 3 divides any solution N then $N > 10^{1937042}$ and number of prime factors has to be ≥ 298848.

Questions?