Algorithms for Carmichael numbers

Andrew Shallue and Jonathan Webster

Illinois Wesleyan University and Butler University, USA
ashallue@iwu.edu, jewebste@butler.edu

ANTS 2026
Groningen, Netherlands

One-page summary

- Complexity class of "is n a Carmichael number?"
  - CARMICHAELS is in $\mathbf{P}$[1].
  - CARMICHAELS is in **ZPP**.
- Optimal algorithm for tabulating Carmichael numbers[2]
- New world record: table of Carmichael numbers up to 10^{24}
- To a first approximation, tabulating Carmichaels is solved

[1] Run-time uses ERH but the correctness is unconditional.

[2] conditional, heuristic

Outline

Table of Contents

Fermat's Little Theorem

Theorem (Fermat)

If p is prime, then $b^p \equiv b \pmod{p}$ for all $b \in \mathbb{Z}$.

Theorem (Contrapositive of FLT)

If there exists $b \in \mathbb{Z}$ with $b^n \not\equiv b \pmod{n}$, then n is composite.

Fermat's Little Theorem

Theorem (Fermat)

If p is prime, then $b^p \equiv b \pmod{p}$ for all $b \in \mathbb{Z}$.

Theorem (Contrapositive of FLT)

If there exists $b \in \mathbb{Z}$ with $b^n \not\equiv b \pmod{n}$, then n is composite.

Definition (Carmichael number)

A Carmichael number is a composite integer n satisfying $b^n \equiv b \pmod{n}$ for all $b \in \mathbb{Z}$.

[AGP] There are infinitely many.

Korselt's Criterion

Theorem (Korselt's Criterion)

A composite number n is a Carmichael number if and only if n is squarefree and $(p-1) \mid (n-1)$ for all prime divisors p of n.

Korselt's Criterion

Theorem (Korselt's Criterion)

A composite number n is a Carmichael number if and only if n is squarefree and $(p-1) \mid (n-1)$ for all prime divisors p of n.

Example

The number $3 \cdot 11 \cdot 17 = 561$ is a Carmichael number.

- $2|560$
- $10|560$
- $16|560$

561 is the smallest Carmichael number.

Table of Contents

Problem

Given bound B, tabulate all Carmichael numbers up to B.

Strategy (Classical)

Given an integer P and a bound B, determine the finite list of primes r such that $n = Pr < B$ is Carmichael.

Strategy (New)

Given an integer P and a bound B, determine the finite list of R such that $n = PR < B$ is Carmichael.

Motivation

- Tabulating Carmichael numbers is of historical interest.
- More data is helpful in shedding light on various theoretical claims about Carmichael numbers.
- Advances in tabulating Carmichael numbers leads to improvements in constructing other pseudoprimes, e.g. Baillie-PSW pseudoprime.
- Erdős-Shanks debate: For what X will $C(X) > X^{1/2}$?
- Other: “Ours goes to 211," Robert Baillie's check, Sam Wagstaff's search for special Carmichael numbers

Table of Contents

All But One

Prior tabulations constructed Carmichaels prime-by-prime.

If P is small, there exist fast algorithms that can find primes q, r such that Pqr is Carmichael.

- [J1990, P1993] ran efficiently for prime P.
- [SW2022] gave an efficient algorithm for any P.

If P is large, there exist fast algorithms that can find the primes r such that Pr is Carmichael.

- [P1993] trial division to find small factors of $P - 1$.
- [SW2025] utilized the "divisor in residue class" factoring problem.

All But One

Prior tabulations constructed Carmichaels prime-by-prime.

If P is small, there exist fast algorithms that can find primes q, r such that Pqr is Carmichael.

- [J1990, P1993] ran efficiently for prime P.
- [SW2022] gave an efficient algorithm for any P.

If P is large, there exist fast algorithms that can find the primes r such that Pr is Carmichael.

- [P1993] trial division to find small factors of $P - 1$.
- [SW2025] utilized the "divisor in residue class" factoring problem.

The set of P that were improved was asymptotically small.

All But One - Asymptotic Cost

Refer to a preproduct P as the input to a thread, and completions r as the output.

Assuming r is found in polynomial time, the cost to tabulate is proportional to the count of inputs P.

Theorem (SW2025, Theorem 8)

The set of inputs P such that $Pp < B$ is bounded by

$$B \exp\left\{\left(-\frac{1}{\sqrt{2}} + o(1)\right)\sqrt{\log B \log\log B}\right\}.$$

This matches Knödel's bound on the count of Carmichael numbers $C(B)$.

Issue: Prime completion forces a large set of inputs.

Table of Contents

Carmichaels are Easy to Split

Inspiration from Baillie-Wagstaff: let $b \in F(n) \setminus R(n)$, then b can be used to split n (i.e. b is a Fermat liar but not a Rabin liar)

Proof.

Let n' be the odd part of $n-1$, and write $n-1 = 2^e n'$. Let $0 < i \leq e$ be the smallest integer such that $b^{2^i n'} \equiv 1 \pmod{n}$.
Then $b^{2^{i-1} n'} \not\equiv \pm 1 \pmod{n}$, so $(b^{2^{i-1} n'} - 1)(b^{2^{i-1} n'} + 1)$ splits n. □

Carmichaels are Easy to Split

Inspiration from Baillie-Wagstaff: let $b \in F(n) \setminus R(n)$, then b can be used to split n (i.e. b is a Fermat liar but not a Rabin liar)

Proof.

Let n' be the odd part of $n-1$, and write $n-1 = 2^e n'$. Let $0 < i \leq e$ be the smallest integer such that $b^{2^i n'} \equiv 1 \pmod{n}$.
Then $b^{2^{i-1} n'} \not\equiv \pm 1 \pmod{n}$, so $(b^{2^{i-1} n'} - 1)(b^{2^{i-1} n'} + 1)$ splits n. □

Thus we can easily witness n is not Carmichael, or split n if it is.

Usually splitting recursively leads to full factorization, but not this time.

- A composite factor is unlikely to be a Fermat pseudoprime.
- We need to show that any composite factor can be split.

CARMICHAELS is in ZPP

Let n be odd and $n-1 = 2^s n'$ where n' is odd. We can consider a repeated difference of squares factorization:

$$b^{n-1} - 1 = (b^{n'} - 1) \prod_{i=0}^{s-1} (b^{2^i n'} + 1).$$

Rough idea:

1. While there are composite factors m,
2. Generate bases b at random,
3. Check $\gcd(m, b^{2^i n'} + 1)$
4. Correctness confirmed through Korselt

Splitting Picture

Assume n Carmichael with $8 \parallel n-1$. Consider primes $q|n$.

A given q will divide the factor under the divisibility given

$$\underbrace{(b^{8n'}-1)}_{2,4,8 \parallel (q-1)} = \underbrace{(b^{4n'}+1)\overbrace{(b^{4n'}-1)}^{2,4 \parallel (q-1)}}_{8 \parallel (q-1)}$$

$$= \underbrace{(b^{4n'}+1)\overbrace{(b^{2n'}+1)\underbrace{(b^{n'}+1)(b^{n'}-1)}_{2 \parallel (q-1)}}^{4 \parallel (q-1)}}_{8 \parallel (q-1)}$$

Arbitrary Completions

Given input P, apply CARMICHAELS oracle to every element in

$$P(r^\star + k\lambda(P)),$$

where $r^\star$ denotes the least positive residue of $P^{-1} \pmod{\lambda(P)}$.

Example

Let $P = 101 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127$ and $B = 10^{24}$.

1. Prime-by-prime appending in $7 \leq d \leq 11$ tabulations:
   - There are 2455149 candidates to consider.
2. There are only 8431 candidates $n = P(r^\star + k\lambda(P)) < B$.

Arbitrary Completions

Given input P, apply CARMICHAELS oracle to every element in

$$P(r^\star + k\lambda(P)),$$

where $r^\star$ denotes the least positive residue of $P^{-1} \pmod{\lambda(P)}$.

Example

Let $P = 101 \cdot 103 \cdot 107 \cdot 109 \cdot 113 \cdot 127$ and $B = 10^{24}$.

1. Prime-by-prime appending in $7 \leq d \leq 11$ tabulations:
   - There are 2455149 candidates to consider.
2. There are only 8431 candidates $n = P(r^\star + k\lambda(P)) < B$.

We can now ensure that arithmetic progressions are neither too long nor too short, and we have flexibility in parallelization.

Bounds on $C(B)$

Theorem (Erdős-PSW bound - 1956, 1980)

The count of Carmichael numbers less than B is bounded above by

$$B \exp\left\{\frac{-(1-\epsilon)\log B \log\log\log B}{\log\log B}\right\},$$

Let $\mathcal{E}(B)$ denote this bound.

Conjecture: $\mathcal{E}(B)$ is also the lower bound on $C(B)$

Best provable lower bound is $B^{0.3389}$.

Optimal Algorithm

We realize $\mathcal{E}(B)$ by following the proof of Erdős-PSW.

There are three sets of inputs:

1. For $n < B^{1-\delta}$, we find these by recursion.
2. For $B^{1-\delta} < n \leq B$, where n has a prime factor $p \geq B^{\delta}$.
   Create via prime sieve on $[B^{\delta}, B^{1/2})$.
3. For $B^{1-\delta} < n \leq B$ that are B^{δ}-smooth.
   Create via prime-by-prime approach, primes in $[3, B^{\delta})$

Overall, we generate inputs efficiently, outputs corresponding to (3) drive the asymptotic result.

Optimal Algorithm Claims

1. The algorithm is unconditionally correct.
2. The algorithm has running time $\mathcal{E}(B)$ (conditional or probabalistic)
3. The algorithm is optimal, if the conjecture is true that $\mathcal{E}(B)$ is also the lower bound on $C(B)$.

Conclusion: using composite completions is the correct high-level approach to tabulating Carmichael numbers.

Data

There are 308279939 Carmichaels up to 10^{24}.

We now have $C(10^{24}) > (10^{24})^{0.35}$. Compare to Pinch's 0.34 and the provable asymptotic lower bound of 0.3389.

Smallest Carmichael with 60 prime factors is

$$4873238546962513658336860441886028167519866613$$
$$9693740524180635022932074776729658715802049771$$
$$7656753159476851881490172492035557403703360001$$

Thank you!