Tabulating Carmichael numbers $n = Pqr$ with P small

Andrew Shallue and Jonathan Webster

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

ANTS 2022, University of Bristol

Outline

Table of Contents

Fermat's Little Theorem

Theorem (Fermat)

If p is prime, then $a^p \equiv a \pmod{p}$.

Theorem (Contrapositive of FLT)

If $a^n \not\equiv a \pmod{n}$, *then n is composite.*

Fermat's Little Theorem

Theorem (Fermat)

If p is prime, then $a^p \equiv a \pmod{p}$.

Theorem (Contrapositive of FLT)

If $a^n \not\equiv a \pmod{n}$, then n is composite.

Definition (Carmichael number)

A Carmichael number is a composite integer n satisfying $a^n \equiv a \pmod{n}$ for any a.

[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 $(p-1)|(n-1)$ 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 $(p-1)|(n-1)$ for all prime divisors p of n.

Example

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

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

The example is the smallest Carmichael number.

OEIS A002997

One may find a tabulation of Carmichael numbers in the OEIS.

The list begins as

$$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041,$$
$$46657, 52633, 62745, 63973, 75361, 101101, 115921, 126217, 162401,$$
$$172081, 188461, 252601, 278545, 294409, 314821, 334153, 340561,$$
$$399001, 410041, 449065, 488881, 512461, \ldots$$

Table of Contents

Problem

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

Problem

Given an integer P (called a pre-product), determine the finite list of prime-pairs (q, r) such that Pqr is Carmichael.

Problem

Determine the computational complexity of either tabulation problem.

Main result

Theorem

The number of $D\Delta$ pairs used to tabulate all Carmichael numbers of the form Pqr with $P < X$ is $O(X^2(\ln X)^2)$.

To turn the above into a time complexity measured in arithmetic operations, multiply by the cost of primality.

Main result

Theorem

The number of $D\Delta$ pairs used to tabulate all Carmichael numbers of the form Pqr with $P < X$ is $O(X^2(\ln X)^2)$.

To turn the above into a time complexity measured in arithmetic operations, multiply by the cost of primality.

For a comparison with previous work, fix a pre-product $P < X$ with $d-2$ unique prime factors.

- Using the *CD* method of Pinch, tabulating Carmichaels with pre-product P requires $O(P^{2-\frac{1}{d-2}} \ln P)$ inner-loop calls.
- Using the $D\Delta$ method, the average number of inner-loop calls is instead $O(P(\ln P)^2)$.

Comparison

Main ideas:

- replace a loop over an interval with a loop over divisors,
- keep average time and space cost low via an incremental sieve

Comparison

Main ideas:

- replace a loop over an interval with a loop over divisors,
- keep average time and space cost low via an incremental sieve

Advantages of the new result:

- Remove the dependence on d.
- Extend the range of pre-products considered "small"
- Enables a hybrid method: size of interval vs. count of divisors.

Motivation

Let $C(x)$ be the count of Carmichael numbers up to x.

Theorem (Harman 2005)

There exists $\beta > 0.33$ such that $C(x) > x^{\beta}$ (for sufficiently large x).

Conjecture (Erdős)

For every $\epsilon > 0$, there exists x such that $C(x) > x^{1-\epsilon}$.

Fact (Pinch, 2006)

$C(x) > x^{0.34}$ *for* $x = 10^{18}$.

Question: For which integer x is $C(x) > x^{0.5}$?

Constructing pseudoprimes

More speculatively, could we get lucky and find a Baillie-PSW pseudoprime?

Unlikely, but techniques for tabulation sometimes apply to other constructions.

Notable that our new method constructs much larger Carmichaels, since it efficiently finds all completions for a given pre-product.

Example

1344142858883969679083454629833201 is Carmichael, found with pre-product 999983

Table of Contents

Pinch's Tabulations $n < B$

In 1993, Richard Pinch published the modern tabulation method. He used it for the following tabulations:

Pinch's Tabulations $n < B$

In 1993, Richard Pinch published the modern tabulation method. He used it for the following tabulations:

- 1993: $n < 10^{15}$
- 1998: $n < 10^{16}$
- 2005: $n < 10^{17}$
- 2006: $n < 10^{18}$
- 2007: $n < 10^{21}$

How do you tabulate?

We construct $n = p_1 p_2 \dots p_d$ in factored form with $d > 2$ prime factors. We let

$$P = \prod_{i=1}^{d-2} p_i, q = p_{d-1}, \text{ and } r = p_d$$

so that $n = Pqr$ is a Carmichael number.

How do you tabulate?

We construct $n = p_1 p_2 \dots p_d$ in factored form with $d > 2$ prime factors. We let

$$P = \prod_{i=1}^{d-2} p_i, q = p_{d-1}, \text{ and } r = p_d$$

so that $n = Pqr$ is a Carmichael number.

There are two cases to consider:

- P is "large" - sieve for q, search for r in an arithmetic progression
- P is "small" - find q and r at the same time

P is "small"

Theorem (Proposition 2 of Pinch)

There are integers $2 \le D < P < C$ *such that, putting* $\Delta = CD - P^2$*, we have*

$$q = \frac{(P-1)(P+D)}{\Delta} + 1, \tag{1}$$

$$r = \frac{(P-1)(P+C)}{\Delta} + 1, \tag{2}$$

$$P^2 < CD < P^2 \left(\frac{p_{d-2}+3}{p_{d-2}+1} \right). \tag{3}$$

Corollary

There are only finitely many Carmichael numbers of the form Pqr *for a given* P.

CD method - Asymptotic cost

Double nested loop on interval $\left[P^2, P^2\left(\frac{p_{d-2}+3}{p_{d-2}+1}\right)\right]$.

With L_p as interval length, cost per D is L_P/D.

The actions inside the inner loop are cheap.

Theorem

Fix a pre-product P. Then all valid C, D pairs may be created in time $O(L_P \ln P) = O(P^{2-\frac{1}{d-2}} \ln P)$.

When $d = 3$, $O(L_P \ln P) = O(P \ln P)$.

Table of Contents

"Small" - Shallue/Webster case

Generate D, Δ pairs to find q and r.

Input: The interval $[P-1, 2P-1]$ with prime factorizations

for $2 \leq D < P$ **do**

  for Δ *divisors of* $(P-1)(P+D)$ **do**

    Check $C = (P^2 + \Delta)/D$ is integral

    Check $q = \frac{(P-1)(P+D)}{\Delta} + 1$ is a prime

    Check $r = \frac{(P-1)(P+C)}{\Delta} + 1$ is an integral prime

    Check $n = Pqr$ passes Korselt's Criterion

  end

end

Generate D, Δ pairs

Can this work? We need to establish two things.

- The expected number of times the inner loop is entered is asymptotically fewer.
- The cost of obtaining the list of divisors is not expensive

Generate D, Δ pairs

Can this work? We need to establish two things.

- The expected number of times the inner loop is entered is asymptotically fewer.
- The cost of obtaining the list of divisors is not expensive

Both of these are met:

- $\tau((P-1)(P+D))$ is often smaller than L_P/D.
- Sieve of Eratosthenes may be modified to factor numbers.

$D\Delta$ method - Asymptotic cost

Theorem

The cost of tabulating all Carmichael number of the form Pqr for $P < X$ is $O(X^2(\ln X)^2)$.

$$\begin{aligned}
\sum_{P<X}\sum_{D=2}^{P-1}\tau\left((P-1)(P+D)\right) &< \left(\sum_{P<X}\tau(P-1)\right)\left(\sum_{D<X}\tau(P+D)\right) \\
&< \left(\sum_{P<X}\tau(P)\right)\left(\sum_{D<2X}\tau(D)\right) \\
&= 2X^2(\ln X)^2 + O(X^2\ln X).
\end{aligned}$$

The average cost per P is $O(P(\ln P)^2)$.

$D\Delta$ method - example

Example

Let $P = 5 \cdot 19 \cdot 23 \cdot 29 = 63365$, then there are four Carmichael numbers of the form Pqr. They are

1. $P \cdot 683 \cdot 2545783 = 110177147679985$
2. $P \cdot 2297 \cdot 36037 = 5245163907985$
3. $P \cdot 37 \cdot 137 = 321197185$
4. $P \cdot 70168253 \cdot 254447257 = 1131326282391998510665$.

The third number is the smallest Carmichael number with exactly six prime factors. Generating these four numbers requires checking about 9 million $D\Delta$ pairs or about 2.8 billion CD pairs.

What about $d = 3$?

The new $D\Delta$ method is better if $d > 3$. For $d = 3$:

- CD method - costs $O(P \ln P)$.
- $D\Delta$ method - average cost $O(P(\ln P)^2)$.

Timing tests verify that the CD method is faster. We employ a hybrid approach:

For each D, compare $\tau((P-1)(P+D))$ versus L_p/D.

Hybrid - Example

Example

Let $P = 65003$ a prime, the resulting Carmichael numbers are

1. $P \cdot 384226823 \cdot 1387549787527 = 34655299431568422859575163$
2. $P \cdot 260009 \cdot 149569603 = 2527930457246474281$
3. $P \cdot 4485139 \cdot 1443304409 = 420791778351741348553$
4. $P \cdot 4255030921 \cdot 605229266867 = 16740022672059541638033852 1$
5. $P \cdot 2145067 \cdot 123503801 = 17220850085262054001$
6. $P \cdot 11960369 \cdot 628504339 = 488636899246608538273$
7. $P \cdot 845027 \cdot 27300841 = 1499615814744258121$
8. $P \cdot 3073667 \cdot 36326833 = 7258013177193134833$
9. $P \cdot 260009 \cdot 845027 = 14282109784670729$
10. $P \cdot 845027 \cdot 1950061 = 107115466344644941$

The average value of $\tau((P-1)(P+D)/2)$ is around 45 and $\lfloor L_P/D \rfloor = 45$ when $D = 2827$.

Faster $d = 3$ case - heuristic

Conjecture

When P is a prime, all Carmichael numbers of the form Pqr may be found in time $O(P \ln\ln P)$. As a corollary, all Carmichael numbers up to B with three prime factors may be tabulated in time $O(B^{2/3})$.

Use $D\Delta$ method when D is small and CD method when D is large.

Crossover on average: $D = \frac{P}{(\ln P)^2}$

With average value of τ, get:

$$\sum_{D=2}^{\frac{P}{(\ln P)^2}} (\ln P)^2 + \sum_{D=\frac{P}{(\ln P)^2}}^{P-1} 2P/D = P + 2P \ln\ln P = O(P \ln\ln P).$$

Timings - CD versus $D\Delta$

Pre-product bound	$D\Delta$ (seconds)	CD (seconds)	Hybrid (seconds)
$10 \cdot 10^4$	21	81	10
$20 \cdot 10^4$	92	553	50
$30 \cdot 10^4$	231	1730	124
$40 \cdot 10^4$	430	3778	233
$50 \cdot 10^4$	697	7017	395
$60 \cdot 10^4$	983	11455	568
$70 \cdot 10^4$	1425	17281	795
$80 \cdot 10^4$	1898	23806	1072
$90 \cdot 10^4$	2425	33288	1386

Timings for P a prime

Prime pre-product bound	$D\Delta$ (sec)	CD (sec)	Hybrid (sec)
$10 \cdot 10^4$	9	1	1
$20 \cdot 10^4$	36	6	3
$30 \cdot 10^4$	83	15	8
$40 \cdot 10^4$	151	26	14
$50 \cdot 10^4$	237	41	22
$60 \cdot 10^4$	348	60	31
$70 \cdot 10^4$	470	80	41
$80 \cdot 10^4$	619	103	53
$90 \cdot 10^4$	738	125	64
$100 \cdot 10^4$	939	159	81
$110 \cdot 10^4$	1170	193	97
$120 \cdot 10^4$	1328	221	110

Future/Continuing Work

- Complete a tabulation for pre-products $P < 10^8$.
- Complete a Carmichael tabulation up to 10^{24}.

Future/Continuing Work

- Complete a tabulation for pre-products $P < 10^8$.
- Complete a Carmichael tabulation up to 10^{24}.

Thank you!