Constructing a ten billion factor Carmichael number

Steven Hayman and Andrew Shallue  Illinois Wesleyan University

Introduction

We have constructed a Carmichael number with a record number of prime factors. Such constructions are showcases for recent advances in subset-product algorithms that work on problems of very high density [2, 4, 6]. Our new contribution is to show that these techniques can be applied to a subgroup of the natural group that arises from the standard Erdős construction.

Recent records

Here are Carmichael numbers with a record number of prime factors. We start with Löh and Niebuhr [5] since their backtracking algorithm vastly outperformed previous methods.

<table>
<thead>
<tr>
<th>Prime Factors</th>
<th>Date</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>101, 518 primes</td>
<td>1996</td>
<td>Löh and Niebuhr</td>
</tr>
<tr>
<td>10, 333, 229, 305 primes</td>
<td>2011</td>
<td>Alford and Grantham</td>
</tr>
<tr>
<td>10, 021, 449, 117 primes</td>
<td>2012</td>
<td>Hayman and Shallue</td>
</tr>
<tr>
<td>3, 505 prime factors</td>
<td>2012</td>
<td>Hayman and Shallue</td>
</tr>
</tbody>
</table>

(1) In addition, a Carmichael number with k prime factors for all 3 ≤ k ≤ 1005220.
(2) Stored as ASCII with one prime per line, this requires nearly 311 gigabytes.

Erdős construction

A positive integer n is Carmichael if it is a Fermat pseudoprime to the base a for all a coprime to n. For constructions we use the following equivalent definition.

Definition 1 (Korselt criterion): An integer n is Carmichael if it is squarefree and p - 1 | n - 1 for all primes p dividing n.

The following construction of Erdős is widely used in theory [1] and in practice [7].

1. Choose Λ = \prod_{\Phi > 1} q^i, where q₁, ..., qₘ are the first m primes in order and the hᵢ are all at least 1 and non-increasing.
2. Construct the set \mathcal{P} = \{ p \text{ prime} : p = 1 \mod \Lambda \}. Let \mathcal{N} = |\mathcal{P}|.
3. Construct Carmichael n as a product of primes in \mathcal{P} in one of two ways:
   (a) Find a subset S of \mathcal{P} such that \prod_{p \in S} p \equiv 1 \mod \Lambda .
   Then by Definition 1 n = \prod_{p \in \mathcal{P}} p is Carmichael.
   (b) Alternatively, let \ell = \prod_{p \in \mathcal{P}} p and find a subset T of \mathcal{P} such that \prod_{p \in T} p \equiv b \mod \Lambda .
   Then n = \prod_{p \in \mathcal{P} \setminus T} p is Carmichael.

Subset product problem

Let G be an abelian group, and let a₁, ..., aᵣ be elements of G. The subset product problem is to find a subset of the aᵢ that product to the identity in G (more generally, any element of G). Solutions will be rare unless density is greater than 1. Problems with density 1 are the most difficult. Problems with greater density are easier, so the sense in which new algorithms are applicable and in the sense that existing algorithms perform better.

Kuperberg idea

Discovered independently by Flaxman and Przydatek [2], though they didn’t extend to make the best possible improvement.

Assumptions: Group G has a sequence of \sqrt{|\log |G||} subgroups \mathcal{G}ᵣ with factor groups of size 2^{\sqrt{\log |G|}}. Have \mathcal{G}ᵣ distributed independently and symmetrically (i.e. \mathcal{P}[vₜ = x] = \mathcal{P}[vₜ = x^{-1}] in Gₜ) and n > 2^{\sqrt{\log |G|}}.

Algorithm: At level k, let bᵢ ∈ \mathcal{G}ₖ where bᵢ are products of the aᵢ. Pair bᵢ so their products are in \mathcal{G}ₖ₊₁. At level k = \sqrt{|\log |G||}, a product is the identity, and this is the solution.

Complexity: Will succeed with high probability while requiring O(2^{\sqrt{\log |G||}}) group operations and space for O(2^{\sqrt{\log |G||}}) group elements.

New contribution

Inspiration from [5]: elements of \mathcal{P} not uniformly distributed modulo \Lambda. Instead distributed symmetrically, with p ≡ 1 mod \sqrt{\Lambda} more likely. Note the proportion of divisors of \Lambda divisible by \sqrt{\Lambda} is 1/\sqrt{\Lambda}.

Definition 3 Define a subgroup \mathcal{G}' of G as \mathcal{Z}/|\mathcal{Z}|² × \mathcal{Z}/|\mathcal{Z}| with \Lambda = \prod_{p \in \mathcal{P}} p^i, where

\[ m = \min_{j \geq 1} \frac{1}{b_j} \text{ such that } N = \prod_{j \geq 1} b_j^{1/b_j} > (\log |\Lambda|/\log |\Lambda|). \]

While constructing \mathcal{P} we pick out elements in \mathcal{G}', and the claim is that there are enough for the Kuperberg algorithm to still work. Under reasonable assumptions the complexity in terms of N is \[ \geq 2^{\sqrt{\log |\Lambda|/\log |\Lambda|}}. \]

Carmichael with ten billion prime factors

\[ \Lambda = 2^{35} \cdot 3^{19} \cdot 5^{13} \cdot 7^{11} \cdot 11^{7} \cdot 13^{5} \cdot 17^{3} \cdot 19^{2} \cdot 23^{2} \cdot 29^{2} \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \]

With this choice \( N = 10313283024 \). It took 98 seconds to find an appropriate subset of size 819 to exclude. The resulting Carmichael number has 10313283056 prime factors and its decimal expansion would have 230 billion digits.

With \( \Lambda \approx 2^{30} \) applying Kuperberg directly would take approximately \( 2^{34} \) operations. In practice algorithm chose \( m = 17 \) so

\[ \Lambda = 2^{35} \cdot 3^{19} \cdot 5^{13} \cdot 7^{11} \cdot 11^{7} \cdot 13^{5} \cdot 17^{3} \cdot 19^{2} \cdot 23^{2} \cdot 29^{2} \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \]

With \( \Lambda \approx 2^{30} \) we instead anticipate \( 2^{34} \) = \( 2^{14} \) operations. Indeed, the algorithm succeeded with only 16 million primes in \( G' \).

Higher order Carmichael numbers

Holy Grail problem is to construct higher order Carmichael numbers, of which the $620$ problem of Pomerance, Seifard, and Wagstaff is a special case. See [3] for a definition and the following equivalent condition.

Theorem 1 Composite n is a Carmichael of order m if and only if n is square free and for every prime divisor p of n and for every \( 1 \leq r \leq m \), there exists \( s \geq 0 \) with \( n \equiv p^r \mod (p^2 - 1) \).

Build the set \[ S_a(\Lambda) = \{ p \text{ prime}, p^r - 1 \mod \Lambda \text{ for all } 1 \leq r \leq m \} \]

and find a subset to 1 modulo \Lambda. More difficult since density is lower.

References