CARMICHAEL NUMBERS WITH EXACTLY k PRIME FACTORS

W. R. Alford
University of Georgia

Jon Grantham
Institute for Defense Analyses
Center for Computing Sciences

Probable Primes and Pseudoprimes

Fermat's Little Theorem:

If p is prime, then $a^p \equiv a \bmod p$, for all integers a.

The converse doesn't always follow...

$$2^{341} \equiv 2 \bmod 341.$$

A **probable prime to the base** a is a number n such that $a^n \equiv a \bmod n$.

A **pseudoprime to the base** a is a composite probable prime to the base a.

(Sometimes called a **Fermat pseudoprime**.)

There aren't that many pseudoprimes (compared to primes).

Carmichael Numbers

A **Carmichael number** is a pseudoprime to the base a for all integers a.

561 is the first Carmichael number.

Korselt's Criterion:

A composite integer n is a Carmichael number if and only if n is squarefree, and for each prime $p|n$, $p-1|n-1$.

Proof:

Easy.

Theorem and Conjecture

Theorem (Alford, Granville, and Pomerance, 1994):

There are infinitely many Carmichael numbers.

Conjecture:

For every $k \geq 3$, there are infinitely many Carmichael numbers with k prime factors. (In fact, there are $\gg x^{1/k-\epsilon}$ up to x.)

This conjecture follows from Hardy and Littlewood's prime k-tuples conjecture. It has not been proven for any k.

Löh and Niebuhr

In an April 1996 *Math. Comp.* paper, Löh and Niebuhr give an algorithm for finding Carmichael numbers with large numbers of prime factors.

They found a Carmichael number with 1,101,518 prime factors.

They also found Carmichael numbers with k prime factors for $21 \leq k \leq 134$.

Generating the Prime Factors

We use a similar technique as Löh and Niebuhr for generating the prime factors.

Pick a modulus L with many prime factors, for example,

$$L = 2^8 \times 3^4 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19.$$

Find the set S of all primes with $p-1|L$ and $(p, L) = 1$.

Any product n of these primes with $n \equiv 1 \bmod L$ has, for each $p|n$,

$$p - 1|L|n - 1.$$

Thus n is a Carmichael by Korselt's criterion.

How to Find these Primes

Dumb parallelism suffices – e.g., a processor can look for p with $p-1 = 2^3 \times 3^2 \times k$, where $k|(L/2^8 3^4)$.

Cycle through all possibilities, testing each one. A probable prime test does **not** suffice.

Use Pocklington-Lehmer.

Theorem:

Let $n-1 = fu$, where $(f,u) = 1$ and $f > \sqrt{n}$. Then, if for all $p|f$, there is an a_p with $a_p^{n-1} \equiv 1 \bmod n$ and $(a_p^{(n-1)/p} - 1, n) = 1$, then n is prime.

Actual pseudoprimes!

I tried to get by using a probable prime test and later go back and prove primality.

Contrary to conventional wisdom, I got pseudoprimes.

Small numbers? Too many of them?

Open Problem:

Let $B(n)$ be the number of bases b to which n is a pseudoprime to the base b. A number is said to be y-smooth if all of its prime divisors are less than y. Let $\Psi(x, y)$ denote the number of y-smooth numbers less than x. For which y does

$$\frac{(\Sigma_{t<x} B(t)/t)/x}{(\Sigma_{t<x,t\ y-smooth} B(t)/t)/\Psi(x,y)}$$

tend to 0?

Combining the Primes

Löh and Niebuhr:

Find a small subset T of S such that $\prod_{p \in T} p = \prod_{p \in S} p \bmod L$.

Then $\prod_{p \in S-T} p \equiv 1 \bmod L$.

Our strategy:

Find many distinct subsets T_i such that $\prod_{p \in T_i} p \equiv 1 \bmod L$.

Any product of these Carmichaels is also a Carmichael.

Goal: Show that there is a Carmichael number with exactly k prime factors for every k, $3 \leq k \leq B$, where B is really big.

Push Down

So how do we form the sets T_i? For every $p^k|L$, we combine primes in pairs to form products that are 1 modulo p^k. We call this **"pushing down"**.

Example: If we have a prime that is 3 modulo 2^8, we combine it with another prime that is 171 modulo 2^8. The product is then 1 modulo 2^8.

Repeat for each prime power divisor of L. The resulting products will be congruent to 1 modulo L.

They will be Carmichael numbers, and any product of them will be a Carmichael number.

Problems and Solutions

Problem: After we pair up numbers, there will be some left over.

Solution: Before we start pairing up, throw out a number so that the "leftovers" will have product 1 modulo p^k.

Problem: For each prime divisor of L, it seems that we cut the number of products in half.

Solution: We can "look ahead" to the next p^k. (E.g., push down so that the number is 1 mod 2^8 *and* 1 mod 3^4.)

Why Supercomputers Matter

When generating primes, can store in a 64-bit integer by using known form of $p-1$ for a compact representation.

At each step, we need to sort by residue mod p^k. Evenutally, you run out of space on one processor.

Solution: many processors, bucket sort. (1996 technology: Cray T3E)

If you use a Beowulf cluster, you'd need to be more clever (less lazy) about scheduling communication.

Results

In 1998, we found a Carmichael number is divisible by Carmichael numbers with k prime factors for $50 \leq k \leq$244,689.

Last month, we computed a Carmichael number that is divisible by Carmichael numbers with k prime factors for each k in the range 80$\leq k \leq$19,565,220.

It had $19,565,300$, but not all of the intermediate numbers of factors were achievable.

Theorem:

There exist Carmichael numbers with k prime factors for all 3$\leq k \leq$19,565,220.

Onward and Upward

We're not close to running out of memory (by at least a factor of 4).

I generated the primes for a 1 billion factor Carmichael number. I will have to use memory more efficiently or we **will** run out of memory.

When to stop?
1 billion. Or this summer.

The \$620 Problem

A **Fibonacci pseudoprime** is a composite n such that $n | F_{n-\left(\frac{n}{5}\right)}$, where F_k is the k^{th} Fibonacci number.

(Generalizes to Lucas sequences and Lucas pseudoprimes.)

Pomerance, Selfridge and Wagstaff over \$620 for a base-2 pseudoprime that is also a Lucas pseudoprime and is 2 or 3 mod 5.

This is the problem we set out to solve.

Korselt-like criterion:

A composite integer n is worth \$620 if n is squarefree, $n \equiv 2, 3 \bmod 5$, and for each prime $p | n$, $p \equiv 2, 3 \bmod 5$, $p - 1 | n - 1$, and $p + 1 | n + 1$.

Too few primes to "push down".