Higher-order Carmichael numbers

Everett W. Howe

Center for Communications Research, La Jolla

Colorado State University Mathematics Colloquium
6 December 2006

Part I.
Carmichael numbers

Fermat's little theorem

Fermat's little theorem (1640)

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

Definition

A Carmichael number is a composite integer n such that $a^n \equiv a \bmod n$ for all a.

Carmichael numbers exist; the converse of Fermat's theorem is false.

Example (Carmichael, 1910)

Let $n = 561 = 3 \cdot 11 \cdot 17$.
We have $0^n \equiv 0 \bmod n$ and $1^n \equiv 1 \bmod n$. Also,

$2^1 \equiv 2$	$2^8 \equiv 256$	$2^{34} \equiv 412$	$2^{140} \equiv 67$
$2^2 \equiv 4$	$2^{16} \equiv 460$	$2^{35} \equiv 263$	$2^{280} \equiv 1$
$2^4 \equiv 16$	$2^{17} \equiv 359$	$2^{70} \equiv 166$	$2^{560} \equiv 1$

So $2^{561} \equiv 2 \bmod n$.

Repeat with $3, 4, 5, \ldots$

A better way to check for Carmichael numbers

Korselt's criterion (1899)

A composite number n is a Carmichael number if and only if

1. n is squarefree, and
2. for all primes $p \mid n$ we have $n \equiv 1 \bmod (p-1)$.

Example

Again consider $n = 561 = 3 \cdot 11 \cdot 17$. We have

$$561 \equiv 1 \bmod 2$$
$$561 \equiv 1 \bmod 10$$
$$561 \equiv 1 \bmod 16$$

so Korselt's criterion shows that n is Carmichael.

Primality tests

Won't say much about primality tests here. But recall our verification that $2^n \equiv 2 \bmod n$ for $n = 561$:

$2^1 \equiv 2$	$2^8 \equiv 256$	$2^{34} \equiv 412$	$2^{140} \equiv 67$
$2^2 \equiv 4$	$2^{16} \equiv 460$	$2^{35} \equiv 263$	$2^{280} \equiv 1$
$2^4 \equiv 16$	$2^{17} \equiv 359$	$2^{70} \equiv 166$	$2^{560} \equiv 1$

Note that

$$67^2 \equiv 1 \bmod n \quad \text{but} \quad 67 \not\equiv \pm 1 \bmod n.$$

This shows that n is not prime.

Under the Generalized Riemann Hypothesis, tests like this lead to a polynomial-time algorithm to distinguish composites from primes. (Faster than AKS algorithm, which doesn't need GRH.)

Three questions

1. Do Carmichael numbers exist? (Yes.)
2. How can one find or construct them quickly?
3. How many Carmichael numbers are there?

A simple construction

Theorem (Chernick, 1939)

Suppose k is an integer such that $6k+1$, $12k+1$, *and* $18k+1$ *are all prime. Then* $n = (6k+1)(12k+1)(18k+1)$ *is a Carmichael number.*

Proof.

Note that

$$n - 1 = 36k(36k^2 + 11k + 1),$$

and that $p - 1$ divides $36k$ for each prime divisor p of n. □

With $k = 1$, we find that $1729 = 7 \cdot 13 \cdot 19$ is Carmichael.

Remark

A proof of the prime 3-tuple conjecture would thus show that there are infinitely many Carmichael numbers.

Erdős's construction of Carmichael numbers (1956)

Given an integer L, define sets

$$P(L) = \{p \mid p \text{ is prime, } p \nmid L \text{, and } (p-1) \mid L\}$$

$$C(L) = \left\{ n \;\middle|\; \begin{array}{l} n \text{ is squarefree and composite,} \\ \text{all primes dividing } n \text{ lie in } P(L), \\ \text{and } L \mid (n-1). \end{array} \right\}$$

Claim: Every $n \in C(L)$ is Carmicael.

Proof.

If $p \mid n$ then $(p-1) \mid L$.
Since $L \mid (n-1)$, we have $(p-1) \mid (n-1)$.
That is, $n \equiv 1 \bmod (p-1)$. □

How many Carmichael numbers from a given L?

$P(L) = \{\text{primes } p \text{ coprime to } L \text{ with } (p-1) \mid L\}$

$C(L) = \{\text{squarefree composite } n \equiv 1 \bmod L \text{ built from primes in } P(L)\}$

Heuristics

- About $2^{\#P(L)}$ squarefree composite n built from $p \in P(L)$.
- "Each such n has $1/\varphi(L)$ chance of being 1 modulo L."
- So we expect $\#C(L) \approx 2^{\#P(L)}/\varphi(L)$.

Goal: Find L with $\#P(L)$ very large.

Alford (circa 1990)

Found an L for which he could show that

$$\#C(L) \geq 2^{\text{very big exponent}}.$$

Shame your colleagues to success!

Denote by $c(x)$ the number of Carmichael numbers less than x.

Theorem (Alford, Granville, Pomerance 1992)

When $x \gg 0$, we have $c(x) \geq x^{2/7}$.

Harman (2005) has improved the exponent to just under $1/3$.

But what do we expect to be true?

Erdős (1956): Heuristic argument predicting that for every $\varepsilon > 0$, we have

$$c(x) > x^{1-\varepsilon} \quad \text{when} \quad x \gg 0.$$

A more precise heuristic

Heuristic (Pomerance, Selfridge, Wagstaff 1980)

For every $\varepsilon > 0$, when $x \gg 0$ we have

$$c(x) > xe^{(-2+\varepsilon)\frac{\log x \log\log\log x}{\log\log x}}.$$

Define a function $k(x)$ by requiring that

$$c(x) = xe^{-k(x)\frac{\log x \log\log\log x}{\log\log x}}.$$

Pomerance, Selfridge, and Wagstaff prove that

$$\liminf k(x) \geq 1$$

and conjecture that

$$\limsup k(x) \leq 2.$$

Evidence?

Pinch's computations

n	$k(10^n)$	n	$k(10^n)$	n	$k(10^n)$
3	2.93319	9	1.87989	15	1.86301
4	2.19547	10	1.86870	16	1.86406
5	2.07632	11	1.86421	17	1.86472
6	1.97946	12	1.86377	18	1.86522
7	1.93388	13	1.86240	19	1.86565
8	1.90495	14	1.86293	20	1.86598

Part II.
Higher-order Carmichael numbers

Primes vs. Carmichaels

Convention: All rings are commutative, with identity.

Fact #1

An integer n is prime if and only if
$x \mapsto x^n$ is an endomorphism of every $(\mathbb{Z}/n\mathbb{Z})$-algebra.

(For 'if' direction, consider the polynomial ring $(\mathbb{Z}/n\mathbb{Z})[x]$.)

Fact #2

A composite integer n is Carmichael if and only if
$x \mapsto x^n$ is an endomorphism of $(\mathbb{Z}/n\mathbb{Z})$.

Carmichael numbers of order m

Let $m > 0$ be an integer.

Definition

A composite integer n is a Carmichael number of order m if $x \mapsto x^n$ gives an endomorphism of every $(\mathbb{Z}/n\mathbb{Z})$-algebra that can be generated as a $(\mathbb{Z}/n\mathbb{Z})$-module by m elements.

Theorem

A composite n is a Carmichael number of order m if and only if

1. *n is squarefree, and*
2. *for all primes $p \mid n$ and for all positive integers $r \leq m$, there is an integer i such that $n \equiv p^i \bmod (p^r - 1)$.*

Example

Take

$$\begin{aligned} n &= 443372888629441 \\ &= 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331. \end{aligned}$$

Then for all $p \mid n$ we have

$$n \equiv 1 \bmod (p-1)$$
$$n \equiv 1 \bmod (p^2-1)$$

so n is a Carmichael number of order 2.

This is the only example less than 10^{16}.
(There are 246683 Carmichael numbers less than 10^{16}.)

Proof of $\Longrightarrow$ direction

1. n is squarefree, and
2. for all primes $p \mid n$ and for all $r \le m$, there is an i such that $n \equiv p^i \bmod (p^r - 1)$.

Suppose n is a Carmichael number of order m.

Proof of (1)

Only endomorphism of $\mathbb{Z}/n\mathbb{Z}$ is the identity, so $a^n \equiv a \bmod n$.
Suppose $p \mid n$. Then $p = (p, n) = (p^n, n)$, so $p^2 \nmid n$.

Proof of (2)

Given p and r, consider $\mathbb{F}_{p^r}$. Note $\mathbb{Z}/n\mathbb{Z} \to \mathbb{F}_p \to \mathbb{F}_{p^r}$.
Endomorphisms of $\mathbb{F}_{p^r}$ are powers of Frobenius, so for some i we have $x^n = x^{p^i}$ for all $x \in \mathbb{F}_{p^r}$.
Since $\mathbb{F}_{p^r}^*$ is cyclic of order $p^r - 1$, item (2) follows.

A lemma

1. n is squarefree, and
2. for all primes $p \mid n$ and for all $r \le m$, there is an i such that $n \equiv p^i \bmod (p^r - 1)$.

For the other implication, we need a lemma.

Lemma

If (1) and (2), then $\forall s$ with $1 \le s \le m$ we have $\binom{n}{s} \equiv 0 \bmod n$. That is, if $q \mid n$ then $q > m$.

Proof.

Suppose there's a $q \mid n$ with $q \le m$. Choose $p \mid n$ with $p \ne q$. Apply (2) with $r = q - 1$ to get

$$n \equiv p^i \bmod (p^{q-1} - 1).$$

□

A lemma

1. n is squarefree, and
2. for all primes $p \mid n$ and for all $r \leq m$, there is an i such that $n \equiv p^i \bmod (p^r - 1)$.

For the other implication, we need a lemma.

Lemma

If (1) and (2), then $\forall s$ with $1 \leq s \leq m$ we have $\binom{n}{s} \equiv 0 \bmod n$. That is, if $q \mid n$ then $q > m$.

Proof.

Suppose there's a $q \mid n$ with $q \leq m$. Choose $p \mid n$ with $p \neq q$. Apply (2) with $r = q - 1$ to get

$$n \equiv p^i \bmod q.$$

□

A lemma

1. n is squarefree, and
2. for all primes $p \mid n$ and for all $r \leq m$, there is an i such that $n \equiv p^i \bmod (p^r - 1)$.

For the other implication, we need a lemma.

Lemma

If (1) and (2), then $\forall s$ with $1 \leq s \leq m$ we have $\binom{n}{s} \equiv 0 \bmod n$. That is, if $q \mid n$ then $q > m$.

Proof.

Suppose there's a $q \mid n$ with $q \leq m$. Choose $p \mid n$ with $p \neq q$. Apply (2) with $r = q - 1$ to get

$$0 \equiv p^i \bmod q,$$

□

A lemma

1. n is squarefree, and
2. for all primes $p \mid n$ and for all $r \leq m$, there is an i such that $n \equiv p^i \bmod (p^r - 1)$.

For the other implication, we need a lemma.

Lemma

If (1) and (2), then $\forall s$ with $1 \leq s \leq m$ we have $\binom{n}{s} \equiv 0 \bmod n$. That is, if $q \mid n$ then $q > m$.

Proof.

Suppose there's a $q \mid n$ with $q \leq m$. Choose $p \mid n$ with $p \neq q$. Apply (2) with $r = q - 1$ to get

$$0 \equiv p^i \bmod q,$$

contradiction. □

Proof of $\Longleftarrow$ direction

1. n is squarefree, and
2. for all primes $p \mid n$ and for all $r \leq m$, there is an i such that $n \equiv p^i \bmod (p^r - 1)$.

Suppose (1) and (2) hold.
Suppose R is a $(\mathbb{Z}/n\mathbb{Z})$-algebra generated as a module by m elements. Then

$$R \cong R_1 \times R_2 \times \cdots \times R_t$$

with each R_i *local* and gen'd by m elts.

If $x \mapsto x^n$ is endomorphism of each R_i, then it's an endomorphism of R.

Suffices to consider case where R is local.

Proof of $\Longleftarrow$ direction, continued

1. n is squarefree, and
2. for all primes $p \mid n$ and for all $r \leq m$, there is an i such that $n \equiv p^i \bmod (p^r - 1)$.

Suppose (1) and (2) hold, and R is a local $(\mathbb{Z}/n\mathbb{Z})$-algebra generated as a module by m elements.

Let $\mathfrak{p}$ be the maximal ideal of R, and $k = R/\mathfrak{p}$ the residue field.

We know $\mathfrak{p}^m = (0)$ and $[k : \mathbb{F}_p] \leq m$.

Since n is squarefree, $\mathbb{F}_p \subseteq R$.

Hensel: Can embed $k \hookrightarrow R$ so that $k \hookrightarrow R \xrightarrow{\text{red}} k$ is identity.

Proof of $\Longleftarrow$ direction, concluded

R is a local ring containing residue field $k = R/\mathfrak{p}$. We have $\mathfrak{p}^m = (0)$ and $[k : \mathbb{F}_p] \leq m$.
To show: $x \mapsto x^n$ is an endomorphism of R.

Given $x \in R$, we may write $x = a + z$ with $a \in k$ and $z \in \mathfrak{p}$.

$$x^n = \sum_{s=0}^{n} \binom{n}{s} a^{n-s} z^s = a^n + \sum_{s=1}^{n} \binom{n}{s} a^{n-s} z^s.$$

But $\binom{n}{s} = 0$ if $1 \leq s \leq m$ and $z^s = 0$ if $s \geq m$, so $x^n = a^n$.

So $x \mapsto x^n$ in R is the composition of

- reduction $R \to k$ $x \mapsto a$
- automorphism $k \to k$ $a \mapsto a^{p^i} = a^n$
- inclusion $k \to R$ $a^n \mapsto a^n$.

Variant of Erdős's construction

Given m and L, define sets

$$P(m, L) = \left\{ p \;\middle|\; \begin{array}{l} p \text{ is prime, } p \nmid L \text{, and for all} \\ \text{positive } r \leq m \text{ we have } (p^r - 1) \mid L. \end{array} \right\}$$

$$C(m, L) = \left\{ n \;\middle|\; \begin{array}{l} n \text{ is squarefree and composite,} \\ \text{all primes dividing } n \text{ lie in } P(m, L), \\ \text{and } L \mid (n-1). \end{array} \right\}$$

Suppose $n \in C(m, L)$ and $p \mid n$.

For all $r \leq m$ we have $(p^r - 1) \mid L$ and $L \mid (n - 1)$, so

$$n \equiv 1 = p^0 \bmod (p^r - 1).$$

So every $n \in C(m, L)$ is a Carmichael number of order m.

Example

$P(m, L) = \{\text{primes } p \text{ coprime to } L \text{ with } (p^r - 1) \mid L \text{ for all } r \le m\}$

$C(m, L) = \{\text{squarefree composite } n \equiv 1 \bmod L \text{ built from primes in } P(m, L)\}$

With $m = 2$, take $L = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29$.

Then $\#P(m, L) = 45$, and we expect about $2^{45}/\varphi(L) \approx 263$ elements in $C(m, L)$.

In fact, $\#C(m, L) = 246$.

Example

The smallest element of $C(m, L)$ is $59 \cdot 67 \cdot 71 \cdot 79 \cdot 89 \cdot 101 \cdot 113 \cdot 191 \cdot 233 \cdot 239 \cdot 307 \cdot 349 \cdot 379 \cdot 911 \cdot 2089 \cdot 5279$.

How to compute $C(m, L)$

$P(m, L) = \{\text{primes } p \text{ coprime to } L \text{ with } (p^r - 1) \mid L \text{ for all } r \le m\}$

$C(m, L) = \{\text{squarefree composite } n \equiv 1 \bmod L \text{ built from primes in } P(m, L)\}$

In the preceding example, $\#P(2, L) = 45$.
Don't enumerate 2^{45} integers to find ones that are 1 modulo L!

A 'meet-in-the-middle' approach

- Write $P(2, L) = P \cup Q$ with $\#P = 23$ and $\#Q = 22$.
- Calculate
  $X = \{(a \bmod L) : a \text{ squarefree, built from primes in } P\}$.
- Calculate
  $Y = \{(b \bmod L)^{-1} : b \text{ squarefree, built from primes in } Q\}$.
- Calculate $X \cap Y$.
- If $(a \bmod L) = (b \bmod L)^{-1}$ then $ab \equiv 1 \bmod L$ and ab is squarefree, built from primes in $P(2, L)$.

Open questions and problems

Heuristic (à la Erdős): For every m, there should be infinitely many Carmichael numbers of order m.

Open problems

1. Are there infinitely many Carmichael numbers of order 2?
2. What are the first 3 Carmichael numbers of order 2?
3. Give an example of a Carmichael number of order 3.