HIGHER-ORDER CARMICHAEL NUMBERS

EVERETT W. HOWE

ABSTRACT. We define a Carmichael number of order m to be a composite
integer n such that nth-power raising defines an endomorphism of every $\mathbf{Z}/n\mathbf{Z}$-
algebra that can be generated as a $\mathbf{Z}/n\mathbf{Z}$-module by m elements. We give a
simple criterion to determine whether a number is a Carmichael number of
order m, and we give a heuristic argument (based on an argument of Erdős for
the usual Carmichael numbers) that indicates that for every m there should
be infinitely many Carmichael numbers of order m. The argument suggests a
method for finding examples of higher-order Carmichael numbers; we use the
method to provide examples of Carmichael numbers of order 2.

1. INTRODUCTION

A Carmichael number is defined to be a positive composite integer n that is a
Fermat pseudoprime to every base; that is, a composite n is a Carmichael number
if $a^n \equiv a \bmod n$ for every integer a. Clearly one can generalize the idea of a
Carmichael number by allowing the pseudoprimality test in the definition to vary
over some larger class of tests (perhaps including some of those found in [1], [2],
[4], [6], [8], [9], [11], [16], [19], [26]), and indeed such generalizations have been
considered (see for example [5], [8], [13], [15], [17], [18], [19], [21], [22], [27]). But
there is also a natural algebraic way of generalizing the concept of a Carmichael
number that makes no mention of pseudoprimality. To motivate the definition
we note that (1) an integer $n > 1$ is prime if and only if nth-power raising is
an endomorphism of every $\mathbf{Z}/n\mathbf{Z}$-algebra, and (2) a positive composite integer n
is a Carmichael number if and only if nth-power raising is an endomorphism of
$\mathbf{Z}/n\mathbf{Z}$. So if m is a positive integer, we define a *Carmichael number of order m*
to be a positive composite integer n such that the function $x \mapsto x^n$ defines an
endomorphism of every $\mathbf{Z}/n\mathbf{Z}$-algebra that can be generated as a $\mathbf{Z}/n\mathbf{Z}$-module by
m elements.

Although our definition does not explicitly mention pseudoprimality, a Car-
michael number n of order m will pass many reasonable pseudoprimality tests.
For example, if α is an algebraic integer of degree d with $d \leq m$, then we have

$$\mathrm{Tr}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha^n) \equiv \mathrm{Tr}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha) \bmod n,$$

so n will pass a Dickson-like pseudoprimality test based on the recurrence sequence
of order d consisting of the traces of the powers of α. Also, n will pass the "Frobenius
step" of the Frobenius pseudoprime test of Grantham [8] with respect to every
polynomial of degree at most m.

We will prove the following theorem, which provides a characterization of the Carmichael numbers of order m that generalizes Korselt's criterion [12] for the usual Carmichael numbers:

Theorem 1. *Let m and n be positive integers with n composite. Then n is a Carmichael number of order m if and only if the following two conditions hold*:

(i) *n is squarefree*;

(ii) *for every prime divisor p of n and for every integer r with $1 \leq r \leq m$, there is an integer $i \geq 0$ such that $n \equiv p^i \mod (p^r - 1)$.*

Theorem 1 allows us to formulate a heuristic argument (based on an argument of Erdős [7] for the usual Carmichael numbers, and similar to an argument of Pomerance [25] for the Baillie-PSW pseudoprimes) that indicates that for every m there should be infinitely many Carmichael numbers of order m. The heuristics suggest a method of searching for higher-order Carmichael numbers; we implement this method for the case $m = 2$ and find many examples, some of which we present below. In fact, the numbers n produced by our argument have the property that n is congruent to 1 modulo $p^r - 1$ for every prime divisor p of n and every integer r with $1 \leq r \leq m$. We call such n *rigid* Carmichael numbers of order m, and in Section 5 we show by example that not all higher-order Carmichael numbers are rigid. Our choice of the adjective "rigid" is explained in Section 6, where we prove that a positive composite n is a rigid Carmichael number of order m if and only if nth-power raising is the identity on every finite étale $\mathbf{Z}/n\mathbf{Z}$-algebra that can be generated as a module by m elements.

We would like to replace the heuristic arguments of this paper with actual proofs, but that seems to be difficult; we have been unable to adapt the argument of Alford, Granville, and Pomerance [3] for the infinitude of the usual Carmichael numbers to the case of higher-order Carmichael numbers. However, in a recent paper [10], Hsu proves that there are infinitely many "Carmichael polynomials", which are Drinfeld module analogues of Carmichael numbers and higher-order Carmichael numbers.

We know of only one example of a higher-order Carmichael number other than the ones produced by the computations described in this paper: one finds the number $17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331$, which is a rigid Carmichael number of order 2, on the list of the Carmichael numbers less than 10^{16} that was computed by Richard Pinch (see [23], [24]).

Acknowledgments. The author thanks Dan Gordon, Jon Grantham, Andrew Granville, Hendrik Lenstra, Greg Martin, Carl Pomerance, and Trevor Wooley for their comments. The author is especially grateful to Lenstra for suggesting Lemma 2 and its proof, and for suggesting various ways of defining "finite étale" without using much algebra. The author also thanks the anonymous referee for his or her suggestions for improving the exposition of the material in this paper.

Conventions. All rings in this paper are supposed to be commutative and to have an identity element, and all ring homomorphisms $R \to S$ are supposed to take the identity of R to the identity of S.

2. Proof of Theorem 1

Suppose that n is a Carmichael number of order m. The ring $\mathbf{Z}/n\mathbf{Z}$ is an algebra over itself and is generated by a single element as a module over itself, so $x \mapsto x^n$ must be an endomorphism of this ring. The only endomorphism of $\mathbf{Z}/n\mathbf{Z}$ is the

identity, so we have $x = x^n$ for all x in $\mathbf{Z}/n\mathbf{Z}$. But if n were divisible by the square of a prime p we would have $p^n \not\equiv p \bmod n$, a contradiction. Thus n is squarefree, and condition (i) holds.

Let p be a prime divisor of n and let r be an integer with $1 \leq r \leq m$. The finite field $\mathbf{F}_{p^r}$ is a $\mathbf{Z}/p\mathbf{Z}$-algebra, and is therefore also a $\mathbf{Z}/n\mathbf{Z}$-algebra via the projection $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$. It is clear that $\mathbf{F}_{p^r}$ can be generated as a $\mathbf{Z}/n\mathbf{Z}$-module by m elements, so nth-power raising is an automorphism of $\mathbf{F}_{p^r}$. Every automorphism of $\mathbf{F}_{p^r}$ is of the form $x \mapsto x^{p^i}$ for some i, so there is an integer i such that $x^n = x^{p^i}$ for every $x \in \mathbf{F}_{p^r}$. Since the multiplicative group of $\mathbf{F}_{p^r}$ is cyclic of order $p^r - 1$, we see that $n \equiv p^i \bmod (p^r - 1)$. Thus condition (ii) holds.

Now suppose that conditions (i) and (ii) hold. First we prove the following statement:

Lemma 2. *If r is an integer with $1 \leq r \leq m$, then $\binom{n}{r} \equiv 0 \bmod n$.*

Proof. Since n is assumed to be squarefree, the statement we are to prove is equivalent to the statement that all prime divisors of n are greater than m. Suppose, to obtain a contradiction, that n had a prime divisor q with $q \leq m$. Since n is assumed to be composite as well as squarefree, n must have another prime divisor $p \neq q$. If we apply statement (ii) of the theorem with this p and with $r = q - 1$, we find that there is an $i \geq 0$ such that $n \equiv p^i \bmod (p^{q-1} - 1)$, and since q divides $p^{q-1} - 1$ it follows that $n \equiv p^i \bmod q$. But $q \mid n$, so we find that $q \mid p^i$, a contradiction. $\square$

Now suppose R is a $\mathbf{Z}/n\mathbf{Z}$-algebra that can be generated as a module by m elements. Then R is a finite ring, and so is a product of finite local rings R_i, each of which is a $\mathbf{Z}/n\mathbf{Z}$-algebra that can be generated as a $\mathbf{Z}/n\mathbf{Z}$-module by m elements. If nth-power raising is an endomorphism of each R_i, then it is an endomorphism of R as well, so it suffices to consider the case where R is local. Since n is squarefree, there is a prime divisor p of n such that $pR = 0$, so that R is an $\mathbf{F}_p$-algebra. Let $\mathfrak{p}$ be the maximal ideal of R and let k be the field $R/\mathfrak{p}$. Since R can be generated by m elements as an $\mathbf{F}_p$-module, we see that $[k : \mathbf{F}_p] \leq m$ and that $\mathfrak{p}^m = 0$. Since k is separable over $\mathbf{F}_p$, Hensel's lemma shows that there is a homomorphism $k \to R$ compatible with the reduction map $R \to k$; we view k as a subring of R via this map. We find that every element of R may be written in a unique way as a sum $a + z$ with $a \in k$ and $z \in \mathfrak{p}$.

If $a \in k$ and $z \in \mathfrak{p}$, then we have

$$(a + z)^n = \sum_{r=0}^{n} \binom{n}{r} a^{n-r} z^r = a^n,$$

where the second equality is obtained from the facts that $z^r = 0$ when $r \geq m$ and $\binom{n}{r} = 0$ in R when $1 \leq r \leq m$. But since $n \equiv p^i \bmod (p^{[k:\mathbf{F}_p]} - 1)$ we see that $(a+z)^n = a^{p^i}$, so nth-power raising on R is simply the reduction map to k followed by the automorphism $x \mapsto x^{p^i}$ followed by the lifting map $k \to R$. In particular, nth-power raising is a homomorphism. Thus, n is a Carmichael number of order m. This completes the proof of Theorem 1.

3. A CONSTRUCTION AND HEURISTICS

Let $m > 0$ be given. In this section we will give a construction that associates to every positive integer L a (possibly empty) set $C(m, L)$ of Carmichael numbers

of order m. We will also give a heuristic argument that indicates that one should be able to find values of L that will make $\#C(m, L)$ as large as one pleases. The construction and argument generalize those of Erdős [7] for the usual Carmichael numbers; Pomerance uses a similar argument in [25] to show that there should be infinitely many Baillie-PSW pseudoprimes.

First, the construction. Let $P(m, L)$ be the set of prime numbers p that do not divide L and that have the property that for every positive integer $r \leq m$, the integer $p^r - 1$ divides L. Let $C(m, L)$ be the set of squarefree integers $n > 1$ that are congruent to 1 modulo L and whose prime divisors all lie in $P(m, L)$. We claim that the elements of $C(m, L)$ are Carmichael numbers of order m. For suppose n is an element of $C(m, L)$, suppose r is an integer with $1 \leq r \leq m$, and suppose p is a prime divisor of n. Then $p^r - 1$ divides L, and L divides $n - 1$, so $n \equiv p^0 \bmod (p^r - 1)$. By Theorem 1, the integer n is a Carmichael number of order m.

Our heuristic argument for the existence of L for which $\#C(m, L)$ is large depends on the following assumption (in addition to the usual assumptions and approximations made in such arguments):

Assumption. *Suppose f is an element of $\mathbf{Z}[x]$ with $f(0) \neq 0$. Then there exist real numbers u and v with $1 < v < u$ such that for all sufficiently large y, there are at least y^v primes q less than y^u such that $f(q)$ is y-smooth.*

(Recall that an integer z is said to be *y-smooth* if all of its prime divisors are less than or equal to y.) Note that this assumption is in fact true if f is a product of linear elements of $\mathbf{Z}[x]$, as is shown by Theorem 4 of [20].

Let f be the least common multiple of the polynomials $x^r - 1$ for $1 \leq r \leq m$, and apply the above assumption to this f to obtain real numbers u and v with the properties mentioned in the assumption. For every y let L be the least common multiple of the prime powers p^e such that $p < y$ and $p^e < y^{mu}$. We will argue that one should expect $\log \#C(m, L) \gg y^v$.

Let us estimate the cardinality of the set $S(y, u)$ of primes q between y and y^u such that $f(q)$ is y-smooth. By our choice of u and v, when y is sufficiently large there are y^v primes q less than y^u such that $f(q)$ is y-smooth. Since there are fewer than y primes less than y, we find that $\#S(y, u) \gg y^v$.

Suppose q is an element of $S(y, u)$ and let r be an integer with $1 \leq r \leq m$. Since $f(q)$ is y-smooth, we see that all of the prime factors of $q^r - 1$ are less than y. Suppose p is a prime divisor of $q^r - 1$ and suppose p^e is the largest power of p that divides $q^r - 1$. Then certainly $p^e \leq q^r - 1 < q^m \leq y^{mu}$, so p^e divides L. It follows that $q^r - 1$ divides L. Thus $S(y, u)$ is contained in $P(m, L)$, and $\#P(m, L) \gg y^v$.

Consider the map from the power set of $P(m, L)$ to $(\mathbf{Z}/L\mathbf{Z})^*$ defined by sending a subset of $P(m, L)$ to the residue modulo L of the product of its elements. It seems reasonable to assume that the elements of $(\mathbf{Z}/L\mathbf{Z})^*$ will each have roughly the same number of preimages in the power set of $P(m, L)$, so we expect that there should be roughly $2^{\#P(m,L)}/\varphi(L)$ subsets X of $P(m, L)$ such that the product of the elements of X is 1 modulo L. In other words, we expect

$$\log \#C(m, L) \approx \#P(m, L) \log 2 - \log \varphi(L).$$

Now, $\log \varphi(L)$ is less than $\log L$, and $\log L \ll y$. It follows that we should have $\log \#C(m, L) \gg y^v$, and so we expect to be able to find integers L for which $\#C(m, L)$ is as large as we like.

4. Constructing Carmichael numbers of order 2

The argument given in Section 3 suggests a method for finding Carmichael numbers of order m: Find a value of L for which $\#P(m,L)\log 2 - \log\varphi(L)$ is large, and then search for subsets of $P(m,L)$ the products of whose elements are 1 modulo L. Only about 1 out of every $\varphi(L)$ subsets of $P(m,L)$ will have the desired property, so if L is too large we will have trouble finding such subsets. If m is greater than 2, we must take L to be extremely large in order for our heuristics to predict that $C(m,L)$ is nonempty, so examples of Carmichael numbers of order 3 or more seem to be out of reach for the moment. However, as we will show in this section, it is possible to use the above method to find Carmichael numbers of order 2.

Let us define the *fecundity* of a number L to be

$$F(L) = \#P(2,L) - (\log\varphi(L))/\log 2,$$

so that we expect $C(2,L)$ to contain about $2^{F(L)}$ elements. When L does not have too many divisors, one can compute the set $P(2,L)$ naïvely by listing the divisors d of L and searching for those d such that $d+1$ is the square of a prime. We computed $F(L)$ by this method for many L built up of primes less than or equal to 37, and we found several L with positive fecundity. For example, let

$$L_1 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29$$

and

$$L_2 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31.$$

Then $\#P(2,L_1) = 45$ and $\#P(2,L_2) = 58$, so that $F(L_1) \approx 8.039$ and $F(L_2) \approx 16.132$.

We calculated the entire set $C(2,L_1)$, and found many elements of the set $C(2,L_2)$, by using a modified "meet-in-the-middle" approach written using the mathematics package MAGMA and run on one 195-MHz MIPS R10000 IP27 processor of a Silicon Graphics Origin 2000 computer. Before we give the details of our computation, let us first describe an unmodified meet-in-the-middle algorithm for computing $C(2,L)$.

Let L be given. Suppose we divide the set $P(2,L)$ into two disjoint subsets S_1 and S_2 of roughly equal size, and for each $i = 1,2$ let m_i be the product of the primes in S_i. We can then calculate the set X of multiplicative inverses of the residues (modulo L) of the $2^{\#S_1}$ divisors of m_1 and the set Y of the residues (modulo L) of the $2^{\#S_2}$ divisors of m_2. For every element x in the intersection $X \cap Y$, we can then find all divisors e of m_1 such that $e \equiv x^{-1} \bmod L$ and all divisors f of m_2 such that $f \equiv x \bmod L$. For each such pair (e,f) the product ef is congruent to 1 modulo L, and is therefore an element of $C(2,L)$ (unless $e = f = 1$). This gives a reasonably efficient method for computing $C(2,L)$, but it requires that we store about $2^{\#P(2,L)/2}$ numbers of size about L. We used a slightly different method that reduces the storage requirements at the expense of reducing the efficiency of the algorithm.

To calculate $C(2,L_1)$, we divided the set $P(2,L_1)$ into three disjoint subsets S_1, S_2, and S_3 with $\#S_1 = \#S_2 = 19$ and $\#S_3 = 7$, and for each $i = 1,2,3$ we let m_i be the product of the primes in S_i. We calculated the sets X and Y associated to S_1 and S_2 as above, and for every one of the 2^7 divisors d of m_3 we calculated the set $Y_d = \{dy : y \in Y\}$. For every element x in the intersection $X \cap Y_d$, we found all divisors e of m_1 such that $e \equiv x^{-1} \bmod L_1$ and all divisors f of m_2 such that

$df \equiv x \bmod L_1$. For each such triple (d, e, f) the product def is congruent to 1 modulo L_1, and so is an element of $C(2, L_1)$ (unless $d = e = f = 1$). We found that $\#C(2, L_1) = 246$, whereas our heuristic argument suggested that there would be approximately $2^{F(L_1)} \approx 263$ elements in this set. The two elements of $C(2, L_1)$ with the smallest number of prime divisors are

$$31 \cdot 37 \cdot 101 \cdot 103 \cdot 109 \cdot 199 \cdot 419 \cdot 449 \cdot 521 \cdot 571 \cdot 911 \cdot 2089 \cdot 2551 \cdot 5851 \cdot 11969$$

and

$$41 \cdot 67 \cdot 79 \cdot 181 \cdot 199 \cdot 233 \cdot 239 \cdot 307 \cdot 449 \cdot 521 \cdot 1217 \cdot 1871 \cdot 4159 \cdot 5851 \cdot 9281.$$

We used a similar method to construct elements of $C(2, L_2)$. We divided the set $P(2, L_2)$ into the set S_1 of its 20 smallest members, the set S_2 of the 20 smallest elements not in S_1, and the set S_3 of the remaining 18 elements, and we defined the m_i as before. We expect that there are about $2^{F(L_2)} \approx 2^{16.132}$ elements in $C(2, L_2)$, so we expect that for every 4 divisors d of m_3 we should find one element in $X \cap Y_d$. This expectation is borne out by experimentation. For example, of the 18 prime divisors of m_3, four give rise to Carmichael numbers of order 2; these Carmichael numbers are

$$23 \cdot 43 \cdot 59 \cdot 61 \cdot 79 \cdot 89 \cdot 113 \cdot 131 \cdot 151 \cdot 191 \cdot 307 \cdot 311 \cdot 373$$
$$\cdot\, 419 \cdot 433 \cdot 463 \cdot 701 \cdot 1217 \cdot 2551,$$
$$23 \cdot 53 \cdot 59 \cdot 79 \cdot 89 \cdot 101 \cdot 109 \cdot 113 \cdot 131 \cdot 181 \cdot 199 \cdot 233 \cdot 307$$
$$\cdot\, 349 \cdot 433 \cdot 701 \cdot 911 \cdot 1217 \cdot 4523,$$
$$61 \cdot 67 \cdot 71 \cdot 89 \cdot 101 \cdot 103 \cdot 113 \cdot 151 \cdot 181 \cdot 191 \cdot 199 \cdot 233$$
$$\cdot\, 239 \cdot 271 \cdot 307 \cdot 419 \cdot 463 \cdot 521 \cdot 571 \cdot 701 \cdot 911 \cdot 5279,$$

and

$$41 \cdot 43 \cdot 53 \cdot 61 \cdot 89 \cdot 103 \cdot 113 \cdot 151 \cdot 191 \cdot 311 \cdot 349$$
$$\cdot\, 373 \cdot 419 \cdot 433 \cdot 463 \cdot 521 \cdot 571 \cdot 701 \cdot 929 \cdot 15313.$$

5. EXAMPLES OF NON-RIGID CARMICHAEL NUMBERS

Let m be a positive integer. Recall that we defined a rigid Carmichael number of order m to be a Carmichael number n of order m such that for every prime divisor p of n and every integer r with $1 \le r \le m$ we have $n \equiv 1 \bmod (p^r - 1)$. We see that every element of the set $C(m, L)$ from Section 3 is a rigid Carmichael number of order m. It is natural to ask whether all Carmichael numbers of order m are rigid. The answer is no; we prove this by producing several Carmichael numbers n of order 2 each having a prime divisor p with $n \not\equiv 1 \bmod (p^2 - 1)$.

Let L_0 be a positive integer and let p_0 be a prime number that does not divide L_0 and such that $\gcd(L_0, p_0^2 - 1)$ divides $p_0 - 1$. Let $P(2, L_0)$ be as in Section 3, and let $C(2, L_0, p_0)$ denote the set of integers of the form $p_0 n_0$, where n_0 is a squarefree integer, all of whose prime factors lie in $P(2, L_0)$, such that $n_0 \equiv 1 \bmod (p_0^2 - 1)$ and $p_0 n_0 \equiv 1 \bmod L_0$. (Our assumption on $\gcd(L_0, p_0^2 - 1)$ ensures that such n_0 are not barred from existence by congruence conditions.) Then for every n in $C(2, L_0, p_0)$ and every prime divisor p of n we have

$$n \equiv \begin{cases} 1 \bmod (p^2 - 1) & \text{if } p \ne p_0, \\ p \bmod (p^2 - 1) & \text{if } p = p_0. \end{cases}$$

Since such an n is squarefree, Theorem 1 shows that it is a Carmichael number of order 2, but it certainly is not a rigid Carmichael number of order 2.

If L_0 and p_0 are as above, let L be the least common multiple of L_0 and $p_0^2 - 1$. Heuristics as in Section 3 indicate that we should expect there to be about $2^{\#P(2,L_0)}/\varphi(L)$ elements in the set $C(2, L_0, p_0)$.

For example, suppose we take L_0 to be $2^7 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31$ (the number called L_2 in Section 4), and suppose we let $p_0 = 1153$ (the smallest prime that does not divide L_0 and that satisfies the gcd condition mentioned above). Since $\#P(2, L_0) = 58$ and $\log \varphi(L)/\log 2 \approx 52$, we expect there to be about 64 integers in $C(2, L_0, p_0)$. We used a slightly modified version of the technique described in the preceding section to search for elements of $C(2, L_0, p_0)$. (We chose the subsets S_1 and S_2 of $P(2, L_0)$ so that they each contained only quadratic residues modulo 5 — this allowed us to immediately disregard those divisors of m_3 that are quadratic residues modulo 5, since we were trying to find a divisor of $m_1 m_2 m_3$ that is congruent modulo L to a quadratic nonresidue modulo 5.) We found there to be 53 elements in $C(2, L_0, p_0)$; the smallest of these is

$$23 \cdot 67 \cdot 71 \cdot 89 \cdot 109 \cdot 113 \cdot 191 \cdot 199 \cdot 233 \cdot 239 \cdot 271 \cdot 307 \cdot 373$$
$$\cdot 419 \cdot 521 \cdot 911 \cdot 929 \cdot 1153 \cdot 1217 \cdot 1429 \cdot 2089 \cdot 2729 \cdot 23561,$$

and the largest is

$$23 \cdot 37 \cdot 43 \cdot 53 \cdot 59 \cdot 61 \cdot 67 \cdot 71 \cdot 89 \cdot 103 \cdot 109 \cdot 113 \cdot 131 \cdot 181 \cdot 191 \cdot 199 \cdot 239 \cdot 271$$
$$\cdot 311 \cdot 373 \cdot 379 \cdot 419 \cdot 433 \cdot 463 \cdot 521 \cdot 683 \cdot 701 \cdot 911 \cdot 929 \cdot 991 \cdot 1153 \cdot 1429$$
$$\cdot 2089 \cdot 2551 \cdot 3191 \cdot 4159 \cdot 5279 \cdot 11969 \cdot 15809 \cdot 23561 \cdot 23869 \cdot 244529.$$

6. FINITE ÉTALE ALGEBRAS

In this section we will show that the rigid Carmichael numbers have a natural interpretation in terms of finite étale algebras, an interpretation that explains our choice of the term "rigid".

For the benefit of those readers unfamiliar with finite étale R-algebras, we present a definition equivalent to the usual one (found for example in Section I.3 of [14]) that is applicable when R is a finite product of local rings. First suppose that R is itself a local ring — that is, a ring with a unique maximal ideal. Then an R-algebra S is *finite étale* if it is free of finite rank as an R-module and if for some (or equivalently, every) R-module basis $\{e_1, \ldots, e_n\}$ of S, the determinant of the n-by-n matrix $[\mathrm{Tr}_{S/R}(e_i e_j)]$ is a unit of R; here $\mathrm{Tr}_{S/R}$ is the trace map from S to R. Now suppose that R is equal to $R_1 \times \cdots \times R_m$, where the R_i are local. Then an R-algebra S is *finite étale* if it is of the form $S = S_1 \times \cdots \times S_m$, where each S_i is a finite étale R_i-algebra. (Note that the zero ring is a finite étale R_i-algebra, so some of the S_i may be zero.) Since every finite ring is a finite product of local rings, our definition can be used when R is finite. We see, for example, that if n is a squarefree integer then a finite étale $\mathbf{Z}/n\mathbf{Z}$-algebra is simply a finite product of finite fields, each of whose characteristics divides n.

Theorem 3. *Let m and n be positive integers with n composite.*

(a) *The integer n is a Carmichael number of order m if and only if nth-power raising is an endomorphism of every finite étale $\mathbf{Z}/n\mathbf{Z}$-algebra that can be generated as a $\mathbf{Z}/n\mathbf{Z}$-module by m elements.*

(b) *The integer n is a rigid Carmichael number of order m if and only if nth-power raising is the identity map on every finite étale $\mathbf{Z}/n\mathbf{Z}$-algebra that can be generated as a $\mathbf{Z}/n\mathbf{Z}$-module by m elements.*

Proof. Let us prove the "if" parts of statements (a) and (b). Suppose nth-power raising is an endomorphism of every finite étale $\mathbf{Z}/n\mathbf{Z}$-algebra that can be generated as a $\mathbf{Z}/n\mathbf{Z}$-module by m elements. Since $\mathbf{Z}/n\mathbf{Z}$ is a finite étale $\mathbf{Z}/n\mathbf{Z}$-algebra, the argument that we gave in the first paragraph of the proof of Theorem 1 shows that n is squarefree. Now let p be a prime divisor of n and let r be an integer with $1 \leq r \leq m$. By the comment just before the statement of the theorem, the finite field $\mathbf{F}_{p^r}$ is a finite étale $\mathbf{Z}/n\mathbf{Z}$-algebra, so the argument that we gave in the second paragraph of the proof of Theorem 1 shows that there is an integer i such that $n \equiv p^i \bmod (p^r - 1)$; furthermore, we have $n \equiv 1 \bmod (p^r - 1)$ if nth-power raising is the identity on $\mathbf{F}_{p^r}$. Thus n satisfies the two conditions of Theorem 1, so n is a Carmichael number of order m, and n is rigid if nth-power raising is the identity on every finite étale $\mathbf{Z}/n\mathbf{Z}$-algebra that can be generated as a $\mathbf{Z}/n\mathbf{Z}$-module by m elements.

The "only if" part of statement (a) is obvious. Let us prove the "only if" part of statement (b). If n is a rigid Carmichael number of order m, then Theorem 1 shows that n is squarefree. It is immediate from the definition of rigidity that nth-power raising is the identity map on every finite étale $\mathbf{Z}/n\mathbf{Z}$-algebra of the form $\mathbf{F}_{p^r}$, where p is a prime divisor of n and $1 \leq r \leq m$. But every finite étale $\mathbf{Z}/n\mathbf{Z}$-algebra R that can be generated as a $\mathbf{Z}/n\mathbf{Z}$-module by m elements is a product of algebras of the form $\mathbf{F}_{p^r}$ with $1 \leq r \leq m$, so nth-power raising is the identity on every such R as well. $\qquad\square$

References

[1] W. W. Adams: Characterizing pseudoprimes for third-order linear recurrences, *Math. Comp.* **48** (1987), 1–15. MR **87k:**11014

[2] W. W. Adams and D. Shanks: Strong primality tests that are not sufficient, *Math. Comp.* **39** (1982), 255–300. MR **84c:**10007

[3] W. R. Alford, A. Granville, and C. Pomerance: There are infinitely many Carmichael numbers, *Ann. of Math. (2)* **139** (1994), 703–722. MR **95k:**11114

[4] R. Baillie and S. S. Wagstaff, Jr.: Lucas pseudoprimes, *Math. Comp.* **35** (1980), 1391–1417. MR **81j:**10005

[5] A. Di Porto and P. Filipponi: Generating M-strong Fibonacci pseudoprimes, *Fibonacci Quart.* **30** (1992), 339–343. MR **93i:**11013

[6] A. Di Porto, P. Filipponi, and E. Montolivo: On the generalized Fibonacci pseudoprimes, *Fibonacci Quart.* **28** (1990), 347–354. MR **91m:**11007

[7] P. Erdős: On pseudoprimes and Carmichael numbers, *Publ. Math. Debrecen* **4** (1956), 201–206. MR **18:**18e

[8] J. Grantham: Frobenius pseudoprimes, *Math. Comp.* (to appear).

[9] S. Gurak: Cubic and biquadratic pseudoprimes of Lucas type, pp. 330–347 in *Théorie des nombres (Quebec, PQ, 1987)* (J.-M. De Koninck and C. Levesque, eds.), de Gruyter, Berlin-New York, 1989. MR **90k:**11166

[10] C.-N. Hsu: On Carmichael polynomials, *J. Number Theory* **71** (1998), 257–274. MR **99i:**11116

[11] I. Joó: On generalized Lucas pseudoprimes, *Acta. Math. Hungar.* **55** (1990), 279–284. MR **92f:**11004

[12] A. Korselt: Problème chinois, *L'Intermédiaire des Mathématiciens* **6** (1899), 142–143.

[13] G. Kowol: On strong Dickson pseudoprimes, *Appl. Algebra Engrg. Comm. Comput.* **3** (1992), 129–138. MR **96g:**11005

[14] J. S. Milne: *Étale Cohomology*, Princeton University Press, Princeton, NJ, 1980. MR **81j:**14002

[15] R. LIDL AND W. B. MÜLLER: A note on strong Fibonacci pseudoprimes, pp. 311–317 in *Advances in cryptology — AUSCRYPT '90* (J. Seberry and J. Pieprzyk, eds.), Lecture notes in computer science **453**, Springer, Berlin, 1990. MR **91k:**11012

[16] R. LIDL AND W. B. MÜLLER: Generalizations of the Fibonacci pseudoprimes test, *Discrete Math.* **92** (1991), 211–220. MR **93g:**11010

[17] R. LIDL AND W. B. MÜLLER: Primality testing with Lucas functions, *Advances in cryptology — AUSCRYPT '92* (J. Seberry and Y. Zheng, eds.), Lecture notes in computer science **718**, Springer, Berlin, 1993. MR **95j:**11121

[18] R. LIDL, W. B. MÜLLER, AND A. OSWALD: Some remarks on strong Fibonacci pseudoprimes, *Appl. Algebra Engrg. Comm. Comput.* **1** (1990), 59–65. MR **95k:**11015

[19] F. MARKO: A note on pseudoprimes with respect to abelian linear recurring sequence, *Math. Slovaca* **46** (1996), 173–176. MR **97k:**11009

[20] G. MARTIN: Lower bounds for the number of smooth values of a polynomial, electronic preprint available online at `http://xxx.lanl.gov/abs/math.NT/9807102`, 1998.

[21] S. M. S. MÜLLER: Carmichael numbers and Lucas tests, pp. 193–202 in *Finite Fields: Theory, Applications, and Algorithms* (R. C. Mullin and G. L. Mullen, eds.), Contemp. Math. **225**, American Mathematical Society, Providence, RI 1998. MR **99m:**11008

[22] W. B. MÜLLER AND A. OSWALD: Generalized Fibonacci pseudoprimes and probable primes, pp. 459–464 in *Applications of Fibonacci numbers, Vol.* 5 (G. E. Bergum, A. N. Philippou, and A. F. Horadam, eds.), Kluwer, Dordrecht, 1993. MR **95f:**11105

[23] R. G. E. PINCH: The Carmichael numbers up to 10^{15}, *Math. Comp.* **61** (1993), 381–391. MR **93m:**11137

[24] R. G. E. PINCH: Compressed text file `carmichael-16.gz`, available by anonymous ftp at `ftp://ftp.dpmms.cam.ac.uk/pub/rgep/Carmichael`, 1992.

[25] C. POMERANCE: Are there counterexamples to the Baillie-PSW primality test?, *Dopo le Parole* (H. W. Lenstra, Jr., J. K. Lenstra, and P. Van Emde Boas, eds.), privately published, Amsterdam, 1984.

[26] G. SZEKERES: Higher order pseudoprimes in primality testing, pp. 451–458 in *Combinatorics, Paul Erdős is eighty, Vol.* 2 (*Keszthely,* 1993) (D. Miklós, V. T. Sós and T. Szőnyi, eds.), Bolyai Soc. Math. Stud. **2**, János Bolyai Math. Soc., Budapest, 1996. MR **97c:**11113

[27] H. C. WILLIAMS: On numbers analogous to the Carmichael numbers, *Canad. Math. Bull.* **20** (1977), 133–143. MR **56:**5414

CENTER FOR COMMUNICATIONS RESEARCH, 4320 WESTERRA COURT, SAN DIEGO, CA 92121-1967, USA

E-mail address: `however@alumni.caltech.edu`

URL: `http://alumni.caltech.edu/~however/`