Canad. Math. Bull. Vol. **52** (1), 2009 pp. 3–8

Carmichael Numbers with a Square Totient

W. D. Banks

Abstract. Let φ denote the Euler function. In this paper, we show that for all large x there are more than $x^{0.33}$ Carmichael numbers $n \leqslant x$ with the property that $\varphi(n)$ is a perfect square. We also obtain similar results for higher powers.

1 Introduction

A longstanding conjecture in prime number theory asserts the existence of infinitely many primes of the form $m^2 + 1$. Although the problem appears to be intractable at present, there have been a number of partial steps in the direction of this result, for the most part as a consequence of sieve methods. One knows, thanks to Brun, that the number of integers $m^2 + 1 \leqslant x$ that are prime is $O(x^{1/2}/\log x)$. In the opposite direction, Iwaniec [5] has shown that $m^2 + 1$ is the product of at most two primes infinitely often.

For any prime p we have $p = m^2 + 1$ if and only if $\varphi(p) = m^2$, where φ is the Euler function; thus, the $m^2 + 1$ conjecture can be reformulated as the assertion that the set

$$\mathcal{S}_\varphi^{(2)} := \{n \geqslant 1 \,:\, \varphi(n) \text{ is a perfect square}\}$$

contains infinitely many prime numbers. Motivated by this observation, the set of integers with square totients was first studied by Banks, Friedlander, Pomerance, and Shparlinski [3]; they proved that $\bigl|\mathcal{S}_\varphi^{(2)} \cap [1,x]\bigr| \geqslant x^{0.7038}$ for all sufficiently large values of x.

We cannot show that the set $\mathcal{S}_\varphi^{(2)}$ contains infinitely many primes, however it is interesting to ask whether other thin sets of integers enjoy an infinite intersection with $\mathcal{S}_\varphi^{(2)}$. For example, denoting by $\mathcal{P}_2$ the set of integers with at most two prime factors, it may be possible to show using sieve methods that $|\mathcal{S}_\varphi^{(2)} \cap \mathcal{P}_2| = \infty$, a natural analogue of Iwaniec's result. This problem can be restated as follows:

Problem Prove that there exist infinitely many pairs (p,q) of primes such that $(p-1)(q-1)$ is a perfect square.

In this paper, we show that the set $\mathcal{S}_\varphi^{(2)}$ contains infinitely many Carmichael numbers. Moreover, the same is true for all of the sets

$$\mathcal{S}_\varphi^{(N)} := \{n \geqslant 1 \,:\, \varphi(n) = m^N \text{ for some integer } m\} \qquad (N = 2, 3, 4, \ldots).$$

We recall that an integer $n \geqslant 1$ is said to be a *Carmichael number* if n is composite and $n \mid (a^n - a)$ for all integers a.

Received by the editors July 24, 2006; revised October 20, 2006.
AMS subject classification: Primary: 11N25; secondary: 11A25.

By the celebrated work of Alford, Granville, and Pomerance [1], it is known that the set $\mathcal{C}$ of Carmichael numbers is infinite. In fact, the authors have shown that the lower bound $\big|\mathcal{C} \cap [1,x]\big| \geqslant x^{\beta}$ holds for all large x with

$$\beta := \frac{5}{12}\Big(1 - \frac{1}{2\sqrt{e}}\Big) = 0.290306\cdots > \frac{2}{7}.$$

Using a variant of the Alford–Granville–Pomerance construction, Harman [4] has recently established the same result with the constant $\beta := 0.33$; see also the earlier paper of Baker and Harman [2].

The main result of this paper is the following:

Theorem 1 *For every fixed $C < 1$, there is a number $x_0(C)$ such that for all $x \geqslant x_0(C)$ the inequality*

$$\Big|\big\{n \leqslant x \,:\, n \text{ is Carmichael and } \varphi(n) = m^N \text{ for some integer } m\big\}\Big| \geqslant x^{0.33}$$

holds for all positive integers $N \leqslant \exp\big((\log\log x)^C\big)$.

As in [4], the constant 0.33 appearing in Theorem 1 can be replaced by any number $\beta < 0.3322408$.

Let $\pi(x)$ be the number of primes $p \leqslant x$ and $\pi(x;d,a)$ the number of such primes in the arithmetic progression a modulo d. The following conditional result (compare [1, Theorem 4]) suggests that for every fixed integer $N \geqslant 2$ there are $x^{1+o(1)}$ Carmichael numbers $n \leqslant x$ such that $\varphi(n)$ is a perfect N-th power:

Theorem 2 *Let $\varepsilon > 0$, and suppose that there is a number $x_1(\varepsilon)$ such that for all $x \geqslant x_1(\varepsilon)$, the inequality*

$$\pi(x;d,1) \geqslant \frac{\pi(x)}{2\varphi(d)}$$

holds for all positive integers $d \leqslant x^{1-\varepsilon}$. Then, for every fixed $C < 1$, there is a number $x_2(\varepsilon, C)$ such that for all $x \geqslant x_2(\varepsilon, C)$ the inequality

$$\Big|\big\{n \leqslant x \,:\, n \text{ is Carmichael and } \varphi(n) = m^N \text{ for some integer } m\big\}\Big| \geqslant x^{1-3\varepsilon}$$

holds for all positive integers $N \leqslant \exp\big((\log\log x)^C\big)$.

Both results above follow immediately from Theorem 3 (see Section 2), whose proof relies heavily on ideas from [1, 3, 4].

Throughout the paper, the letters p and q (with or without subscripts) always denote prime numbers, and the letters n and m always represent positive integers.

https://doi.org/10.4153/CMB-2009-001-7 Published online by Cambridge University Press

2 Construction

Fix $\varepsilon > 0$, and let E and B be numbers in the open interval $(0,1)$. Let $y \geqslant 2$ be a parameter, and put

$$\theta := (1-E)^{-1}, \qquad \delta := \frac{\varepsilon\theta}{4B}, \qquad x := \exp(y^{1+\delta}). \tag{1}$$

We shall say that the pair (E,B) is *ε-good* if for all sufficiently large y there exist integers L and k with the following properties:

(i) L is a squarefree product of primes q from the interval $(y^\theta/\log y, y^\theta]$, where each shifted prime $q-1$ is free of prime divisors greater than y;
(ii) $k \leqslant x^{1-B}$ and $\gcd(k,L) = 1$;
(iii) the inequality $|\mathcal{P}| \geqslant x^{EB-\varepsilon/3}$ holds, where

$$\mathcal{P} := \{p \leqslant x \,:\, p = dk+1 \text{ is prime and } d \mid L\}.$$

We shall say that the pair (E,B) is *good* if it is ε-good for every $\varepsilon > 0$.

Theorem 3 *Let (E,B) be a good pair, $C < 1$, and $\varepsilon > 0$. Then, there is a number $X_0 = X_0(E,B,C,\varepsilon)$ such that for all $X \geqslant X_0$ the inequality*

$$\left|\mathcal{S}_\varphi^{(N)} \cap \mathcal{C} \cap [1,X]\right| \geqslant X^{EB-\varepsilon}$$

holds for all positive integers $N \leqslant \exp\big((\log\log x)^C\big)$.

It follows from [4, Theorem 3] that $(0.7039, 0.472)$ is a good pair. Since

$$0.7039 \times 0.472 = 0.3322408 > 0.33,$$

Theorem 1 is an immediate consequence of Theorem 3.

Similarly, let $\mathcal{E}$ and $\mathcal{B}$ be the sets considered in [1]. Arguing as in the proof of [1, Theorem 4.1], it is easy to see that (E,B) is a good pair for any $E \in \mathcal{E}$, $B \in \mathcal{B}$. The hypothesis of Theorem 2 implies that $1-\varepsilon \in \mathcal{B}$, hence by [1, Theorem 3] we have $1-\varepsilon' \in \mathcal{E}$, where $\varepsilon' = \varepsilon/(1-\varepsilon)$; therefore, $(1-\varepsilon', 1-\varepsilon)$ is a good pair. Since $(1-\varepsilon')(1-\varepsilon) - \varepsilon = 1 - 3\varepsilon$, Theorem 2 follows immediately from Theorem 3.

Proof of Theorem 3 Let $y \geqslant 2$ be a parameter, and define θ, δ, x as in (1). Replacing ε by a smaller number if necessary, we can assume that

$$C(1+\delta/2) < 1 + \delta/4. \tag{2}$$

If y is large enough, there are integers L and k satisfying (i)–(iii) above. Let

$$\mathcal{P} := \{p \leqslant x \,:\, p = dk+1 \text{ is prime and } d \mid L\};$$

then the inequality

$$|\mathcal{P}| \geqslant x^{EB-\varepsilon/3}$$

https://doi.org/10.4153/CMB-2009-001-7 Published online by Cambridge University Press

holds by property (iii).

With L and k fixed, consider the group

$$\mathcal{G}_N := (\mathbb{Z}/L\mathbb{Z})^* \times \underbrace{(\mathbb{Z}/N\mathbb{Z})^+ \times \cdots \times (\mathbb{Z}/N\mathbb{Z})^+}_{\kappa \text{ copies}},$$

where $\kappa := \omega(kL)$ is the number of distinct prime divisors of kL. Note that, if y is large enough, we have

$$\kappa \leqslant \log(kL) \leqslant (1-B)\log x + \log L.$$

As in [1], for any finite group G we denote by $n(G)$ the length of the longest sequence of (not necessarily distinct) elements of G such that the product of the elements in any subsequence is different from the identity. Since the maximal order of an element of $\mathcal{G}_N$ is $\lambda(L)N$, where λ is the Carmichael function, and $|\mathcal{G}_N| = \varphi(L)N^\kappa$, we have by [1, Theorem 1.2]:

$$\begin{aligned} n(\mathcal{G}_N) &\leqslant \lambda(L)N\Big(1 + \log\frac{\varphi(L)N^\kappa}{\lambda(L)N}\Big) \leqslant \lambda(L)N\big(1 + \log L + \kappa\log N\big) \\ &\leqslant \lambda(L)N\big(1 + \log L + ((1-B)\log x + \log L)\log N\big). \end{aligned}$$

Taking into account the bounds $\log L \leqslant 2y^\theta$ and $\lambda(L) \leqslant e^{2\theta y}$, which follow from property (i) if y is sufficiently large (see, for example, the proof of [1, Theorem 4.1]), and using the fact that $\log x = y^{1+\delta}$ together with the trivial inequality $2\log N \geqslant 1$ for all $N \geqslant 2$, it follows that

$$n(\mathcal{G}_N) \leqslant e^{2\theta y} N\log N\big(2 + 6y^\theta + (1-B)y^{1+\delta}\big) \leqslant e^{3\theta y} N\log N$$

if y is large enough. In particular,

$$N \leqslant \exp(y^{1+\delta/4}) \quad\Longrightarrow\quad n(\mathcal{G}_N) \leqslant \exp(y^{1+\delta/3}) \tag{3}$$

if y is sufficiently large.

Now let $\mathcal{Q}$ denote the set of primes $q \in (y^\theta/\log y, y^\theta]$, and put $\mathcal{P}' := \mathcal{P} \setminus \mathcal{Q}$. Since $|\mathcal{Q}| \leqslant y^\theta$, we have

$$|\mathcal{P}'| \geqslant x^{EB-\varepsilon/2}$$

for all large y. Consider the multiplicative map ψ from the set of squarefree positive integers coprime to L into the group $\mathcal{G}_N$, defined by

$$\psi(n) := \big(\psi_0(n), \psi_1(n), \ldots, \psi_\kappa(n)\big),$$

where

$$\psi_j(n) := \begin{cases} n \pmod L & \text{if } j = 0; \\ v_{q_j}(\varphi(n)) \pmod N & \text{if } 1 \leqslant j \leqslant \kappa. \end{cases}$$

https://doi.org/10.4153/CMB-2009-001-7 Published online by Cambridge University Press

Here, $q_1 < \cdots < q_\kappa$ are the distinct primes dividing kL, and v_q is the standard q-adic valuation for each prime q. It is easy to see that ψ is injective on $\mathcal{P}'$, hence $\psi(\mathcal{P}')$ is a subset of $\mathcal{G}_N$ with cardinality

$$\big|\psi(\mathcal{P}')\big| = |\mathcal{P}'| \geqslant x^{EB-\varepsilon/2}. \tag{4}$$

Now, if $\mathcal{R}$ is any subset of $\mathcal{P}'$ with more than one element, and

$$\Pi_\psi(\mathcal{R}) := \prod_{p\in\mathcal{R}} \psi(p)$$

is the identity element of $\mathcal{G}_N$, then

$$n_\mathcal{R} := \prod_{p\in\mathcal{R}} p$$

is a Carmichael number, and $\varphi(n_\mathcal{R}) = m^N$ for some positive integer m.

Indeed, to see that $n_\mathcal{R}$ is Carmichael we apply:

Korselt's criterion. *$a^n \equiv a \pmod n$ for all integers a if and only if n is squarefree and $p-1$ divides $n-1$ for every prime p dividing n.*

Since $\psi(n_\mathcal{R}) = \Pi_\psi(\mathcal{R})$ is the identity of $\mathcal{G}_N$, it follows that $n_\mathcal{R} \equiv 1 \mod L$. As $p \equiv 1 \pmod k$ for every prime p dividing $n_\mathcal{R}$, and $\gcd(k, L) = 1$, we further have $n_\mathcal{R} \equiv 1 \pmod{kL}$. Thus, $p - 1 \mid kL \mid n_\mathcal{R} - 1$ for every prime p dividing $n_\mathcal{R}$, and therefore $n_\mathcal{R}$ is a Carmichael number by Korselt's criterion.

To see that $\varphi(n_\mathcal{R}) = m^N$ for some positive integer m, we observe that the only primes which can divide $\varphi(n_\mathcal{R})$ are those primes $q_1, \ldots, q_\kappa$ that divide kL. Since $\psi(n_\mathcal{R})$ is the identity of $\mathcal{G}_N$, we have $v_{q_j}(\varphi(n_\mathcal{R})) \equiv 0 \pmod N$ for $1 \leqslant j \leqslant \kappa$, and the result follows.

Now let $t := \exp(y^{1+\delta/2})$. By [1, Proposition 1.2], the number of subsets $\mathcal{R} \subset \mathcal{P}'$ with $|\mathcal{R}| \leqslant t$, and such that $\Pi_\psi(\mathcal{R})$ is the identity of $\mathcal{G}_N$, is at least

$$\binom{|\mathcal{P}'|}{\lfloor t\rfloor} \Big/ \binom{|\mathcal{P}'|}{n(\mathcal{G}_N)} \geqslant \Big(\frac{|\mathcal{P}'|}{\lfloor t\rfloor}\Big)^{\lfloor t\rfloor} |\mathcal{P}'|^{-n(\mathcal{G}_N)} \geqslant \big(x^{EB-\varepsilon/2}\big)^{\lfloor t\rfloor - n(\mathcal{G}_N)} \lfloor t\rfloor^{-\lfloor t\rfloor},$$

where we have used (4) for the second inequality. Using (3), we see that the last number exceeds $x^{t(EB-\varepsilon)}$ if $N \leqslant \exp(y^{1+\delta/4})$ and y is sufficiently large. For any such $\mathcal{R}$ we have $n_\mathcal{R} \leqslant x^t$; therefore, setting $X := x^t$ we see that there are more than $X^{EB-\varepsilon}$ Carmichael numbers $n \leqslant X$ with $\varphi(n) = m^N$ provided that $N \leqslant \exp(y^{1+\delta/4})$. Since $X = \exp(y^{1+\delta}\exp(y^{1+\delta/2}))$, we have by our assumption (2):

$$C\log\log\log X = C(1+\delta/2+o(1))\log y \leqslant (1+\delta/4)\log y$$

if y is large enough, and thus

$$\exp((\log\log X)^C) \leqslant \exp(y^{1+\delta/4}).$$

Since y can be determined uniquely from X, this completes the proof. ∎

Acknowledgments The author would like to thank Igor Shparlinski for useful conversations and for pointing out the relevance of [4] to the present work, and the anonymous referee for the suggestion of Theorem 2. This paper was written during a visit by the author to Macquarie University; the hospitality and support of this institution are gratefully acknowledged.

References

[1] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers.* Ann. of Math. (2) **139**(1994), no. 3, 703–722.
[2] R. Baker and G. Harman, *Shifted primes without large prime factors.* Acta Arith. **83**(1998), no. 4, 331–361.
[3] W. Banks, J. B. Friedlander, C. Pomerance and I. E. Shparlinski, *Multiplicative structure of values of the Euler function.* In: High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun. 41, American Mathematical Society, Providence, RI, 2004, pp. 29–47.
[4] G. Harman, *On the number of Carmichael numbers up to x.* Bull. London Math. Soc. **37**(2005), no. 5, 641–650.
[5] H. Iwaniec, *Almost-primes represented by quadratic polynomials.* Invent. Math. **47**(1978), no. 2, 171–188.

Department of Mathematics, University of Missouri, Columbia, MO 65211 USA
e-mail: bbanks@math.missouri.edu

https://doi.org/10.4153/CMB-2009-001-7 Published online by Cambridge University Press