Turk J Math
33 (2009) , 9 – 16.
© TÜBİTAK
doi:10.3906/mat-0711-38

Values of the Carmichael Function Equal to a Sum of Two Squares

William D. Banks and Ahmet M. Güloğlu

Abstract

In this note, we determine the order of growth of the number of positive integers $n \leqslant x$ such that $\lambda(n)$ is a sum of two square numbers, where $\lambda(n)$ is the Carmichael function.

Key Words: Carmichael function, sum of two squares.

1. Introduction

Let $\lambda(n)$ denote the *Carmichael function*, whose value at the integer $n \geqslant 1$ is defined to be the exponent of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$. More explicitly, for every prime power p^α we have

$$\lambda(p^\alpha) = \begin{cases} p^{\alpha-1}(p-1) & \text{if } p \geqslant 3 \text{ or } \alpha \leqslant 2, \\ 2^{\alpha-2} & \text{if } p = 2 \text{ and } \alpha \geqslant 3, \end{cases}$$

and for an arbitrary integer $n \geqslant 2$ with prime factorization $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ we have

$$\lambda(n) = \operatorname{lcm}\big[\lambda(p_1^{\alpha_1}), \dots, \lambda(p_k^{\alpha_k})\big].$$

Clearly, $\lambda(1) = 1$.

In this note, we study positive integers n with the property that $\lambda(n)$ is the sum of two square numbers. Our main result is the following:

Theorem 1 *Let $\mathcal{S}$ be the set of positive integers m such that $m = a^2 + b^2$ for some integers a and b, and put*

$$S(x) = \#\big\{n \leqslant x \ : \ \lambda(n) \in \mathcal{S}\big\}.$$

Then, there are absolute constants $c_2 > c_1 > 0$ such that the inequalities

$$\frac{c_1\, x}{(\log x)^{3/2}} \leqslant S(x) \leqslant \frac{c_2\, x}{(\log x)^{3/2}}$$

hold for all sufficiently large values of x.

AMS Mathematics Subject Classification: 11N37.

Since $\lambda(p) = p-1$ for every prime p, the lower bound of Theorem 1 follows from the work of Iwaniec [2] (see also [3]), who showed that

$$\#\{p \leqslant x \ : \ p-1 \in \mathcal{S}\} \geqslant \frac{c_1\, x}{(\log x)^{3/2}}$$

holds with some absolute constant $c_1 > 0$ for all sufficiently large values of x. Our proof of the upper bound of Theorem 1 (see Section 4) uses ideas from [1], where similar bounds have been obtained for the *Euler function* $\varphi(n)$ and for the *sum of divisors function* $\sigma(n)$. One difference in our case is that $\lambda(n)$ is *not* a multiplicative function, and this fact necessitates an approach using slightly different sets than those considered in [1] and a special treatment of certain intermediate estimates (see, for example, Lemma 3). Fortunately, the contribution to $S(x)$ coming from integers with a fixed number of prime divisors can be controlled sufficiently well to obtain the required upper bound.

2. Notation

In what follows, the letter p always denotes a *prime number*, and the letter q (with or without subscripts) always denotes an *odd prime power*. As usual, we denote the set of natural numbers by $\mathbb{N}$.

For a positive integer n, we use $\omega(n)$ to denote the number of distinct prime divisors of n; in particular, $\omega(1) = 0$.

Following [1], for a real number $x > 0$ we define $\log x = \max\{\ln x, 2\}$, where $\ln x$ is the natural logarithm, and for every integer $k \geqslant 2$, we use $\log_k x$ to denote the k-th iterate of $\log x$. We recall that $\log x$ is *submultiplicative*:

$$\log(xy) \leqslant (\log x)(\log y) \qquad (x, y > 0). \tag{2.1}$$

Throughout the paper, implied constants in the symbols O, $\gg$ and $\ll$ are *absolute*. We recall that for positive functions f and g, the notations $f = O(g)$, $f \ll g$ and $f \gg g$ are all equivalent to the assertion that $f \leqslant cg$ for some absolute constant $c > 0$.

3. Preliminary Estimates

Lemma 1 *Let*

$$\begin{aligned} \mathcal{A} &= \big\{a \in \mathbb{N} \ : \ p \mid a \Rightarrow p \equiv 3 \pmod 4\big\}, \\ \mathcal{B} &= \big\{b \in \mathbb{N} \ : \ p \mid b \Rightarrow p \not\equiv 3 \pmod 4\big\}, \end{aligned}$$

and for any integer $k \geqslant 1$ let $\mathcal{Q}^k$ be the set of ordered k-tuples $(q_1, \ldots, q_k)$ such that each q_i is an odd prime power and $\gcd(q_i, q_j) = 1$ for $i \neq j$. Then, for some absolute constant $C > 0$, the bound

$$\sum_{\substack{(q_1,\ldots,q_k)\in\mathcal{Q}^k \\ q_1\cdots q_k \leqslant x \\ \lambda(q_i)\in a_i\mathcal{B}\ \forall\, i}} \log(q_1 \cdots q_k) \leqslant k^{3/2}\, C^k \left(\prod_{i=1}^{k} \frac{1}{\varphi(a_i)}\right) \frac{x(\log A)^{3/2}}{\sqrt{\log x}} \tag{3.2}$$

holds for all $x > 0$, $k \geqslant 1$, and $a_1, \ldots, a_k \in \mathcal{A}$, where $A = \mathrm{lcm}[a_1, \ldots, a_k]$.

Proof. Since the Euler and Carmichael functions agree on odd prime powers, the bound (3.2) can be proved using an inductive argument similar to the proof of [1, Lemma 5]. The only difference in this case is that we need the uniform upper bound

$$\#\big\{q \leqslant x \ : \ \lambda(q) \in a\mathcal{B}\big\} \ll \frac{x}{\varphi(a)(\log(x/a))^{3/2}} \qquad (a \in \mathcal{A},\ x > 0). \tag{3.3}$$

Since $\lambda(q) \in a\mathcal{B}$ implies $q > a$, it is enough to prove this for $x > a$. In the proof of [1, Lemma 1] it is shown that

$$\#\big\{p \leqslant x \ : \ p-1 \in a\mathcal{B}\big\} \ll \frac{x}{\varphi(a)(\log(x/a))^{3/2}}\,,$$

hence it suffices to consider the contribution to the left side of (3.3) coming from prime powers $q = p^\alpha$ with $\alpha > 1$.

First, we observe that there is at most one prime power p^α such that $\lambda(p^\alpha) \in a\mathcal{B}$, $p \equiv 3 \pmod 4$, and $\alpha > 1$. Indeed, writing

$$p^{\alpha-1}(p-1) = ab \qquad \text{for some } b \in \mathcal{B},$$

it is clear that p is the largest prime divisor of a, and that $p^{\alpha-1} \,\|\, a$; hence p^α is uniquely determined by a. On the other hand, if $p \equiv 1 \pmod 4$, then $\lambda(p^\alpha) \in a\mathcal{B}$ if and only if $p-1 \in a\mathcal{B}$. Therefore,

$$\sum_{\substack{p^\alpha \leqslant x,\ \alpha>1\\ \lambda(p^\alpha)\in a\mathcal{B}}} 1 \leqslant 1 + \sum_{\substack{p \leqslant \sqrt{x}\\ p-1 \in a\mathcal{B}}} \ \sum_{\alpha \leqslant \log x} 1 \ll 1 + \frac{\sqrt{x}\,\log x}{\varphi(a)(\log(\sqrt{x}/a))^{3/2}}\,,$$

and (3.3) follows. To complete the proof of (3.2), it is a straightforward matter to adapt the proofs of [1, Lemmas 3,4,5], making use of the bound (3.3) in place of [1, Lemma 2] together with the fact that $\log(x/A) \geqslant (\log x)/\log A$ by (2.1); the details are omitted. □

Lemma 2 *Uniformly for $n \geqslant 1$, we have*

$$\sum_{p \,|\, n} p^{-1} \ll \log_3 n.$$

Proof. Let $p_1, p_2, \ldots$ be the sequence of consecutive prime numbers, and put $n_k = p_1 \cdots p_k$ for each $k \geqslant 1$. By the *Prime Number Theorem* we have

$$\log n_k = (1 + o(1))\, p_k \qquad (k \to \infty),$$

and by *Mertens' theorem* it follows that

$$\sum_{p \,|\, n_k} p^{-1} = \sum_{p \leqslant p_k} p^{-1} = (1 + o(1))\, \log_2 p_k = (1 + o(1))\, \log_3 n_k.$$

Now, for an arbitrary integer n with $\omega(n) = k$, we have

$$\sum_{p \,|\, n} p^{-1} \leqslant \sum_{p \,|\, n_k} p^{-1} \ll \log_3 n_k \leqslant \log_3 n,$$

which is the desired bound. □

Lemma 3 *For some absolute constant $C_1 > 0$, we have the uniform bound:*

$$\sum_{\substack{(n_1,\ldots,n_k)\in\mathbb{N}^k\\ \mathrm{lcm}[n_1,\ldots,n_k]=n}} \left(\prod_{i=1}^{k} \frac{1}{\varphi(n_i)}\right) \ll \frac{k^{\omega(n)}(\log_2 n)^{C_1 k}}{n} \qquad (k,n\in\mathbb{N}). \tag{3.4}$$

Proof. For each fixed k, let $F_k(n)$ be the arithmetic function defined by the left side of (3.4). It is easy to see that $F_k(n)$ is multiplicative; thus,

$$F_k(1) = 1 \qquad \text{and} \qquad F_k(n) = \prod_{p^\alpha \,\|\, n} F_k(p^\alpha) \qquad (n \geqslant 2).$$

For every prime power p^α, we have

$$F_k(p^\alpha) = G_k(p^\alpha) - G_k(p^{\alpha-1}),$$

where

$$G_k(m) = \sum_{\substack{(d_1,\ldots,d_k)\in\mathbb{N}^k\\ \mathrm{lcm}[d_1,\ldots,d_k]\,|\,m}} \left(\prod_{i=1}^{k} \frac{1}{\varphi(d_i)}\right) = \left(\sum_{d\,|\,m} \frac{1}{\varphi(d)}\right)^k \qquad (m\in\mathbb{N}).$$

Hence, writing

$$g = \frac{1}{\varphi(p^\alpha)} \qquad \text{and} \qquad h = \sum_{d\,|\,p^{\alpha-1}} \frac{1}{\varphi(d)},$$

we have

$$F_k(p^\alpha) = (g+h)^k - h^k = k\int_h^{g+h} t^{k-1}\,dt \leqslant kg(g+h)^{k-1}.$$

Also,

$$g+h = \sum_{d\,|\,p^\alpha} \frac{1}{\varphi(d)} = 1 + \frac{p^{\alpha+1}-p}{p^\alpha(p-1)^2} = 1 + O(p^{-1}).$$

Putting everything together, we derive that

$$\begin{aligned}\ln F_k(n) &\leqslant \sum_{p^\alpha \,\|\, n} \ln\left(\frac{k}{\varphi(p^\alpha)}\left(1+O(p^{-1})\right)^{k-1}\right)\\ &= \omega(n)\ln k - \ln\varphi(n) + O\left(k\sum_{p\,|\,n} p^{-1}\right).\end{aligned}$$

Using Lemma 2 together with the lower bound

$$\varphi(n) \gg \frac{n}{\log_2 n} \qquad (n\in\mathbb{N}),$$

we obtain the stated result. □

Lemma 4 *The following bound holds:*

$$\sum_{k=1}^{\infty} \frac{k^n}{k!} \ll n^n \qquad (n \in \mathbb{N}).$$

Proof. If n is large, then

$$\sum_{k>n} \frac{k^n}{k!} < \sum_{k>n} \frac{n^k}{k!} < \sum_{k=0}^{\infty} \frac{n^k}{k!} = e^n.$$

Since $k! \sim \sqrt{2\pi}\, k^{k+1/2} e^{-k}$ as $k \to \infty$, we also have

$$\sum_{k=1}^{n} \frac{k^n}{k!} \ll \sum_{k=1}^{n} \frac{k^n e^k}{k^k} \leqslant \frac{n\kappa^n e^\kappa}{\kappa^\kappa},$$

where κ is the real number at which the function $f(x) = x^n e^x x^{-x}$ takes its maximum value. It is easy to check that κ satisfies the equation $\kappa \ln \kappa = n$, hence $\kappa \sim n/\log n$ as $n \to \infty$, and we derive the estimate

$$\frac{n\kappa^n e^\kappa}{\kappa^\kappa} = \exp(n \log n - n \log_2 n + O(n)).$$

The result follows. □

Lemma 5 *The following bound holds:*

$$\omega(n) \leqslant \frac{\log n}{\log_2 n} \left(1 + O\left(\frac{1}{\log_2 n}\right)\right) \qquad (n \in \mathbb{N}).$$

Proof. As in the proof of Lemma 2, it suffices to prove this bound for integers of the form $n_k = p_1 \cdots p_k$, where $p_1, p_2, \ldots$ is the sequence of consecutive prime numbers. Using [4, Theorem 4] we see that

$$\log n_k = \sum_{p \leqslant p_k} \log p = p_k \left(1 + O\left(\frac{1}{\log p_k}\right)\right),$$

and by [4, Theorem 3] we have

$$p_k = k(\log k + \log_2 k) + O(k);$$

therefore,

$$\log n_k = k(\log k + \log_2 k) \left(1 + O\left(\frac{1}{\log k}\right)\right)$$

and

$$\log \log n_k = (\log k + \log_2 k) \left(1 + O\left(\frac{\log_2 k}{(\log k)^2}\right)\right).$$

Since $\log k \sim \log_2 n_k$ as $k \to \infty$, it follows that

$$\omega(n_k) = k = \frac{\log n_k}{\log_2 n_k}\left(1 + O\left(\frac{1}{\log_2 n_k}\right)\right).$$

This completes the proof. □

4. Proof of the Upper Bound

Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{Q}^k$ be defined as in Lemma 1. For every $a \in \mathcal{A}$, let

$$\mathcal{N}(a;x) = \big\{\text{odd } n \leqslant x \ : \ \lambda(n) \in a\mathcal{B}\big\} \qquad (x \geqslant 1).$$

Our first goal is to establish an upper bound on sums of the form

$$L_k(a;x) = \sum_{\substack{n \in \mathcal{N}(a;x)\\ \omega(n)=k}} \log n \qquad (k \in \mathbb{N},\ a \in \mathcal{A},\ x \geqslant 1).$$

Factoring each n as a product of odd prime powers, we have

$$L_k(a;x) = \frac{1}{k!} \sum_{\substack{(q_1,\ldots,q_k)\in\mathcal{Q}^k\\ q_1\cdots q_k \in \mathcal{N}(a;x)}} \log(q_1\cdots q_k),$$

Every k-tuple $(q_1,\ldots,q_k) \in \mathcal{Q}^k$ determines a unique k-tuple $(a_1,\ldots,a_k) \in \mathcal{A}^k$ such that

$$\lambda(q_i) \in a_i\mathcal{B} \qquad (i = 1,\ldots,k).$$

Moreover, since $\gcd(q_i,q_j) = 1$ for $i \neq j$, the condition $\lambda(q_1\cdots q_k) \in a\mathcal{B}$ is equivalent to $\operatorname{lcm}[a_1,\ldots,a_k] = a$. Therefore, the preceding sum can be expressed in the form

$$L_k(a;x) = \frac{1}{k!} \sum_{\substack{(a_1,\ldots,a_k)\in\mathcal{A}^k\\ \operatorname{lcm}[a_1,\ldots,a_k]=a}} \ \sum_{\substack{(q_1,\ldots,q_k)\in\mathcal{Q}^k\\ q_1\cdots q_k\leqslant x\\ \lambda(q_i)\in a_i\mathcal{B}\ \forall\, i}} \log(q_1\cdots q_k).$$

Inserting the bounds of Lemmas 1 and 3, we derive that

$$L_k(a;x) \ll \frac{k^{\omega(a)+3/2}\big(C(\log_2 a)^{C_1}\big)^k}{k!}\,\frac{(\log a)^{3/2}}{a}\,\frac{x}{\sqrt{\log x}}. \tag{4.5}$$

Next, we need an upper bound on sums of the form

$$s(a) = \sum_{k=1}^{\infty} \frac{k^{\omega(a)+3/2}\big(C(\log_2 a)^{C_1}\big)^k}{k!}$$

in the special case that a is a *square number*. For our purposes below, the following bound suffices:

$$s(a) \ll \frac{\sqrt{a}}{(\log a)^{7/2}}\,. \tag{4.6}$$

To prove (4.6), we begin by applying Cauchy's inequality to the sum $s(a)$, obtaining

$$s(a)^2 \leqslant \exp\big(C^2(\log_2 a)^{2C_1}\big)\sum_{k=1}^\infty \frac{k^{2\,\omega(a)+3}}{k!}\,. \tag{4.7}$$

Since a is a square number, Lemma 5 implies that

$$2\,\omega(a)+3 = 2\,\omega(\sqrt{a}\,)+3 \leqslant \frac{\log a}{\log_2 a}\left(1+O\left(\frac{1}{\log_2 a}\right)\right).$$

Setting $n = 2\,\omega(a)+3$, it follows that

$$n\log n \leqslant \frac{\log a}{\log_2 a}\,(\log_2 a - \log_3 a + O(1)),$$

hence by Lemma 4 we have

$$\sum_{k=1}^\infty \frac{k^{2\,\omega(a)+3}}{k!} = \sum_{k=1}^\infty \frac{k^n}{k!} \ll \exp(n\log n) \leqslant a\,\exp\left(-\frac{\log a}{\log_2 a}\,(\log_3 a + O(1))\right).$$

Inserting this bound into (4.7) and extracting a square-root, we immediately obtain (4.6) for all square numbers $a \in \mathcal{A}$.

Using (4.5) and (4.6), we now derive that

$$\sum_{n\in\mathcal{N}(a;x)} \log n \leqslant \sum_{k=1}^\infty L_k(a,x) \ll \frac{s(a)(\log a)^{3/2}}{a}\frac{x}{\sqrt{\log x}} \ll \frac{1}{\sqrt{a}\,(\log a)^2}\frac{x}{\sqrt{\log x}}\,.$$

Let

$$\mathcal{L}(x) = \big\{\text{odd } n \leqslant x \ :\ \lambda(n) \in \mathcal{S}\big\} \qquad (x \geqslant 1),$$

where $\mathcal{S}$ is defined as in the statement of Theorem 1. Since $\mathcal{S}$ is the disjoint union:

$$\mathcal{S} = \dot{\bigcup_{d\in\mathcal{A}}} d^2\mathcal{B},$$

we have

$$\sum_{n\in\mathcal{L}(x)} \log n = \sum_{d=1}^\infty \sum_{n\in\mathcal{N}(d^2;x)} \log n \ll \frac{x}{\sqrt{\log x}} \sum_{d=1}^\infty \frac{1}{d\,(\log d)^2} \ll \frac{x}{\sqrt{\log x}}\,.$$

By partial summation, it follows that

$$\#\mathcal{L}(x) \ll \frac{x}{(\log x)^{3/2}}\,.$$

Finally, for an odd integer n, we have $\lambda(n) \in \mathcal{S}$ if and only if $\lambda(2^\alpha n) \in \mathcal{S}$ for all $\alpha \geqslant 0$; therefore,

$$S(x) = \#\big\{n \leqslant x \ : \ \lambda(n) \in \mathcal{S}\big\} = \sum_{\alpha \geqslant 0} \#\mathcal{L}(x/2^\alpha)$$

$$\ll \sum_{\alpha \geqslant 0} \frac{x}{2^\alpha (\log(x/2^\alpha))^{3/2}} \leqslant \frac{x}{(\log x)^{3/2}} \sum_{\alpha \geqslant 0} \frac{(\log 2^\alpha)^{3/2}}{2^\alpha} \ll \frac{x}{(\log x)^{3/2}},$$

which is the required upper bound for $S(x)$.

Acknowledgements

The authors thank Florian Luca, Igor Shparlinski and the referee for helpful comments which led to several improvements in the exposition of the paper.

References

[1] Banks, W.D., Luca, F., Saidak, F., Shparlinski, I.E.: Values of arithmetical functions equal to a sum of two squares. Q. J. Math. 56, no. 2, 123–139, (2005).

[2] Iwaniec, H.: Primes of the type $\varphi(x, y) + A$ where φ is a quadratic form. Acta Arith., 21, 203–234, (1972).

[3] Iwaniec, H.: Primes represented by quadratic polynomials in two variables. Acta Arith., 24, 435–459, (1974).

[4] Rosser, J.B., Schoenfeld, L., Approximate formulas for some functions of prime numbers. Illinois J. Math., 6, 64–94, (1962).

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

Received 29.11.2007

Ahmet M. GÜLOĞLU
Department of Mathematics
University of Missouri
Columbia, MO 65211 USA
e-mail: ahmet@math.missouri.edu