J. Aust. Math. Soc. **82** (2007), 123–131

ON THE VALUE SET OF THE CARMICHAEL λ-FUNCTION

JOHN B. FRIEDLANDER✉ and FLORIAN LUCA

(Received 8 April 2005; revised 10 October 2005)

Communicated by W. W. L. Chen

Abstract

In this paper we study the size of the value set of the Carmichael λ-function.

2000 *Mathematics subject classification*: primary 11N25, 11N56.

1. Introduction

Let φ denote the *Euler function*, which, for an integer $n \geq 1$, is defined as usual as the number of elements in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ and hence is given by the product formula

$$\varphi(n) = \prod_{p^\nu \parallel n} p^{\nu-1}(p-1).$$

The *Carmichael function* λ is defined for each integer $n \geq 1$ as the largest order of any element in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. More explicitly, for any prime power p^ν, one has

$$\lambda(p^\nu) = \begin{cases} p^{\nu-1}(p-1) & \text{if } p \geq 3 \text{ or } \nu \leq 2, \\ 2^{\nu-2} & \text{if } p = 2 \text{ and } \nu \geq 3, \end{cases}$$

hence, on prime powers in the first (and more generic) case it coincides with the Euler function, while in the second case it is half as large. Unlike the multiplicative

https://doi.org/10.1017/S144678870001750X Published online by Cambridge University Press

Euler function, the Carmichael function for an arbitrary integer n is given by the least common multiple, rather than the product of, its prime power constituents, that is

$$\lambda(n) = \operatorname{lcm}\left[\lambda(p_1^{\nu_1}), \dots, \lambda(p_k^{\nu_k})\right], \tag{1.1}$$

where $n = p_1^{\nu_1} \cdots p_k^{\nu_k}$ is the prime factorization of n. Note that $\lambda(1) = 1$.

Given a positive integer-valued arithmetic function, it is an interesting question to study the size of its image set. For any subset $\mathscr{A}$ of the positive integers, and for every positive real number x we put $\mathscr{A}(x) = \mathscr{A} \cap [1, x]$. We write

$$\mathscr{L} = \{\lambda(n) : n \geq 1\}$$

and $\mathscr{F}$ for the corresponding image set of φ.

In the case of the Euler function there is a long history of results giving increasingly closer upper and lower bounds and culminating in the result of Ford determining the precise order of magnitude of $\mathscr{F}(x)$. For this and references to the earlier work see [4].

The fact that the Carmichael function is for a general argument given by the least common multiple rather than the product seems to make it more difficult to deal with and consequently quite a bit less is known.

The only lower bound of which we are aware is that of [1]:

$$\#\mathscr{L}(x) \geq \frac{x}{\log x} \exp\left(c(1 + o(1))(\log\log\log x)^2\right),$$

for a suitable positive constant c, which follows from either Theorem 1 or Theorem 2 of that paper. The same expression, with the same constant c, serves as both an upper and a lower bound for $\mathscr{F}(x)$, as was found by Maier and Pomerance [6]. Hence, although we expect that the set $\mathscr{L}(x)$ is rather larger than $\mathscr{F}(x)$, we have not been able to prove this.

The only reference to an upper bound we can find in the literature is contained in the final paragraph of the paper [2] of Erdős, Pomerance and Schmutz, where it is mentioned without proof that a bound of the form $\#\mathscr{L}(x) \ll x/(\log x)^c$ for some $c > 0$ follows from a result of Erdős and Wagstaff [3].

In this paper, we refine the argument of [3] and prove an explicit bound.

THEOREM 1.1. *The inequality*

$$\#\mathscr{L}(x) \ll \frac{x}{(\log x)^\kappa} (\log\log x)^{5/2+\kappa}$$

holds for all $x \geq 3$, where $\kappa = 1 - (e \log 2)/2 = 0.057\dots$.

Actually, as indicated at the end of the proof, the method gives a slightly sharper result, although only so far as to improve the exponent of $\log\log x$.

https://doi.org/10.1017/S144678870001750X Published online by Cambridge University Press

The letters p and q will always denote prime numbers. For a positive integer n, we let $P(n)$, $\omega(n)$ and $\Omega(n)$ denote the largest prime factor, the number of distinct prime factors, and the total number (including multiplicities) of prime factors of n, respectively. If $z > 1$ is any positive real number, we write $\omega_z(n)$ and $\Omega_z(n)$ for the number of distinct prime factors, and the total number of prime factors of n which are $\leq z$, respectively. For any integer $\ell \geq 1$, we write $\log_\ell x$ for the ℓth iterate of the natural logarithm. We shall throughout, without comment, assume that the real variable argument of $\log_\ell$ is sufficiently large that these are defined and positive. Also, throughout the paper the implied constants in symbols 'O' and '$\ll$' will be absolute.

2. Preliminary results

In this section we prove two lemmas which are needed for the proof of our Theorem 1.1.

LEMMA 2.1. *Let $z > 1$ be any real number. We set α to be a positive real in the interval $(0, 1)$. Let*

$$\mathscr{P}_{z,\alpha} = \{p \text{ prime} : P(p-1) > z,\ P(p-1) \parallel p-1 \text{ and } \omega(p-1) \leq \alpha \log\log p\}.$$

Then the estimate

$$\#\mathscr{P}_{z,\alpha}(t) \ll \frac{t(\log_2 t)^{1/2}}{(\log z)^2 (\log t)^{-\alpha \log(e/\alpha)}}$$

holds uniformly for $t > z > 3$, where the implied constant is absolute.

PROOF. Let $p \in \mathscr{P}_z(t)$, where for simplicity we omit the subscript α. Then $p - 1 = qm$, where $q = P(p-1)$. Clearly, $P(m) < q$. Fix m. By Brun's sieve (see, for example, [5]), the number of primes $p \leq t$ such that $p \equiv 1 \pmod m$ and $(p-1)/m$ is prime is

$$\ll \frac{t}{\phi(m)(\log(t/m))^2}.$$

Since $t/m \geq q = P(p-1) > z$, it follows that the above expression is

$$\ll \frac{t}{\phi(m)(\log z)^2}.$$

Note that m is even and

$$\omega(m) = \omega(p-1) - 1 \leq \alpha \log_2 p \leq \alpha \log_2 t.$$

Put $K = \lfloor \alpha \log_2 t \rfloor$. Summing over all the possible values of m, we get

$$\#\mathscr{P}_z(t) \ll \frac{t}{(\log z)^2} \sum_{k \le K} \sum_{\substack{m \le t \\ \omega(m)=k}} \frac{1}{\phi(m)}.$$

Put $S_k = \sum_{m \le t,\ \omega(m)=k} (1/\phi(m))$. Clearly,

$$S_k \le \frac{1}{k!} \left(\sum_{\substack{2 \le q \le t \\ a \ge 1}} \frac{1}{q^{a-1}(q-1)} \right)^k \le \frac{1}{k!} \left(\log_2 t + O(1)\right)^k.$$

Thus,

$$\#\mathscr{P}_z(t) \ll \frac{t}{(\log z)^2} \sum_{k \le K} S_k \ll \frac{t}{(\log z)^2} \sum_{k \le K} \frac{1}{k!} \left(\log_2 t + O(1)\right)^k.$$

Since $\alpha < 1$, one can easily verify that in the last sum above, the final term is the largest one. Using this observation and Stirling's formula, we get

$$\begin{aligned} \#\mathscr{P}_z(t) &\ll \frac{tK}{(\log z)^2} \frac{1}{K!} \left(\log_2 t + O(1)\right)^K \\ &\ll \frac{t(\log_2 t)^{1/2}}{(\log z)^2} \left(\frac{e \log_2 t + O(1)}{K} \right)^K \\ &\ll \frac{t(\log_2 t)^{1/2}}{(\log z)^2} \left(\frac{e}{\alpha} + O\left(\frac{1}{\log_2 t} \right) \right)^{\alpha \log_2 t} \\ &\ll \frac{t(\log_2 t)^{1/2}}{(\log z)^2 (\log t)^{-\alpha \log(e/\alpha)}}, \end{aligned} \tag{2.1}$$

which completes the proof of the lemma. □

If $1 < y < x$, we write $\Psi(x; y) = \#\{n \le x : P(n) \le y\}$.

LEMMA 2.2. *Let $z > 1$. Let β be a real in the interval* $(0, 1)$. *Put*

$$\mathscr{A}_{z,\beta} = \{n : \omega_z(n) \le \beta \log_2 z\}.$$

Then the estimate

$$\#\mathscr{A}_{z,\beta}(t) \ll \frac{t(\log_2 z)^{3/2}}{(\log z)^{1-\beta \log(e/\beta)}}$$

holds uniformly for $t > z > 3$, where the implied constant is absolute.

PROOF. Let $n \in \mathscr{A}_z(t)$, where, again for simplicity, we omit the subscript β. Then $n = uv$, where u and v are coprime, $P(u) \le z$, $\omega(u) \le \beta \log_2 z$, and every prime

https://doi.org/10.1017/S144678870001750X Published online by Cambridge University Press

factor of v exceeds z. We fix u. Then $v \le t/u$ is free of primes $q \le z$. By Brun's sieve, the number of such positive integers is $\ll t/(u \log z)$. Summing over all the possible values of u, we get

$$\# \mathscr{A}_z(t) \ll \frac{t}{\log z} \sum_{\substack{u \le t \\ P(u) \le z \\ \omega(u) \le L}} \frac{1}{u},$$

where $L = \lfloor \beta \log_2 z \rfloor$. Let $T_k = \sum_{u \le t,\, P(u) \le z,\, \omega(u) = k} 1/u$. Clearly,

$$T_k \le \frac{1}{k!} \left(\sum_{\substack{2 \le p \le z \\ a \ge 1}} \frac{1}{p^a} \right)^k \le \frac{1}{k!} \left(\log_2 z + O(1) \right)^k.$$

Thus,

$$\#\mathscr{A}_z(t) \ll \frac{t}{\log z} \sum_{k=0}^{L} \frac{1}{k!} \left(\log_2 z + O(1) \right)^k.$$

Since $\beta < 1$, one can easily verify that in the sum above, the last term is the largest one. Using this observation and Stirling's formula, we obtain

$$\begin{aligned} \text{(2.2)} \qquad \#\mathscr{A}_z(t) &\ll \frac{tL}{\log z} \frac{1}{L!} \left(\log_2 z + O(1) \right)^L \\ &\ll \frac{t (\log_2 z)^{1/2}}{\log z} \left(\frac{e \log_2 z + O(1)}{\beta \log_2 z} \right)^{\beta \log_2 z} \ll \frac{t (\log_2 z)^{1/2}}{(\log z)^{1 - \beta \log(e/\beta)}}, \end{aligned}$$

which completes the proof of the lemma. □

3. The proof of Theorem 1.1

PROOF. Let x be a large positive real number. We put $y = \exp\left(\log x \log_3 x / \log_2 x \right)$, and write $\mathscr{L}_1(x) = \{ m \le x : P(m) \le y \}$. It is well-known (see, for example, [8, Chapter III.5]) that

$$\#\mathscr{L}_1(x) = \Psi(x; y) = x \exp\left(-(1 + o(1)) u \log u \right),$$

where $u = \log x / \log y$. Since $u = \log_2 x / \log_3 x$, a quick calculation shows that

$$\text{(3.1)} \qquad \#\mathscr{L}_1(x) \le \frac{x}{(\log x)^{1 + o(1)}}.$$

We now look at numbers $m = \lambda(n)$, $m \le x$ that are not in $\mathscr{L}_1(x)$. Thus, there exists a prime factor $q > y$ of m. From formula (1.1) for λ, we conclude that either $q^2 | n$,

https://doi.org/10.1017/S144678870001750X Published online by Cambridge University Press

hence $q(q-1)|m$, or there exists a prime number $p|n$ such that $P(p-1)=q>y$. In the first case, denoting the set by $\mathscr{L}_2$, the number of such numbers $m \le x$ does not exceed

$$\#\mathscr{L}_2(x) \le \sum_{q>y} \frac{x}{q(q-1)} \ll x \sum_{q>y} \frac{1}{q^2} \ll \frac{x}{y} = o\left(\frac{x}{\log x}\right).$$

From now on, we need only look at numbers $m \in \mathscr{L}(x)\backslash\mathscr{L}_1(x)$ such that $p-1|m$ for some prime number p with $P(p-1)>y$. Let $q=P(p-1)$. In the case that $q^2|m$, writing $\mathscr{L}_3$ for the set of such m, the number of such numbers $m \le x$ does not exceed

$$\#\mathscr{L}_3(x) \le \sum_{q>y} \frac{x}{q^2} \ll x \sum_{q>y} \frac{1}{q^2} \ll \frac{x}{y} = o\left(\frac{x}{\log x}\right).$$

Hence, from now on we can assume that $q \parallel m$. In particular, $P(p-1) \parallel (p-1)$. Of these remaining $m \le x$, let $\mathscr{L}_4(x)$ be the subset for which we also have $\omega(p-1) < \alpha \log_2 p$, where $\alpha \in (0,1)$ will be fixed later. In this case, $p \in P_y(x)$. Furthermore, since $p-1|m$, the number of such positive integers $m \le x$ does not exceed

$$\sum_{p\in\mathscr{P}_y(x)} \frac{x}{p-1} \ll x \sum_{p\in\mathscr{P}_y(x)} \frac{1}{p}.$$

By estimate (2.1) and partial summation, we get

$$\begin{aligned}
\sum_{p\in\mathscr{P}_y(x)} \frac{1}{p} &\ll \frac{P_y(x)}{x} + \int_y^x \frac{P_y(t)}{t^2}\,dt \\
&\ll \frac{(\log_2 x)^{1/2}}{(\log y)^2(\log x)^{-\alpha\log(e/\alpha)}} + \int_y^x \frac{(\log_2 t)^{1/2}}{(\log y)^2(\log t)^{-\alpha\log(e/\alpha)}}\frac{dt}{t} \\
&\ll \frac{(\log_2 x)^{1/2}}{(\log y)^2(\log x)^{-\alpha\log(e/\alpha)}} + \frac{(\log_2 x)^{1/2}}{(\log y)^2(\log x)^{-1-\alpha\log(e/\alpha)}} \\
&\ll \frac{(\log_2 x)^{5/2}}{(\log x)^{1-\alpha\log(e/\alpha)}(\log_3 x)^2}.
\end{aligned}$$

Hence,

$$\#\mathscr{L}_4(x) \ll \frac{x(\log_2 x)^{5/2}}{(\log x)^{1-\alpha\log(e/\alpha)}(\log_3 x)^2}. \tag{3.2}$$

Let $\mathscr{L}_5(x)$ be the set of those $m \in \mathscr{L}(x)$ not yet considered and such that there exists a prime $p \le x$ with $p-1|m$ and $m/(p-1) \in \mathscr{A}_y$, for some value of β to be fixed later. Lemma 2.2 tells us that for p a given prime, the number of such $m \in \mathscr{L}_5(x)$ is

$$\leq \#\mathscr{A}_y\left(\frac{x}{p-1}\right) \ll \frac{x(\log_2 y)^{3/2}}{p(\log y)^{1-\beta\log(e/\beta)}}.$$

Summing this inequality over all possible values of p, we get

$$\begin{aligned}(3.3)\qquad \#\mathscr{L}_5(x) &\ll \frac{x(\log_2 x)^{3/2}}{(\log y)^{1-\beta\log(e/\beta)}}\sum_{p\leq x}\frac{1}{p} \ll \frac{x(\log_2 x)^{5/2}}{(\log y)^{1-\beta\log(e/\beta)}}\\ &= \frac{x(\log_2 x)^{5/2+1-\beta\log(e/\beta)}}{(\log x)^{1-\beta\log(e/\beta)}(\log_3 x)^{1-\beta\log(e/\beta)}}.\end{aligned}$$

Finally, we let $\mathscr{L}_6(x)$ denote the set of remaining $m \in \mathscr{L}(x)$. Such positive integers m have the property that $p-1|m$ holds with some prime p such that $P(p-1) > y$, $\omega(p-1) \geq \alpha\log_2 p$, and furthemore, $\omega_p(m/(p-1)) \geq \beta\log_2 p$. This implies that

$$\Omega(m) \geq \omega(p-1) + \omega_p(m/p-1) \geq (\alpha+\beta)\log_2 p \geq (\alpha+\beta)\log_2 y.$$

Note that $\log_2 y = \log\left(\log x\log_3 x/\log_2 x\right) = \log_2 x - \log_3 x + \log_4 x$. Put

$$\delta(x) = \frac{(\alpha+\beta)\log_2 y}{\log_2 x} = (\alpha+\beta)\left(1 - \frac{\log_3 x}{\log_2 x} + \frac{\log_4 x}{\log_2 x}\right).$$

We have $\mathscr{L}_6(x) \subset \{m \leq x : \Omega(m) > \delta(x)\log_2 x\}$. We shall choose our constants so that $\alpha+\beta > 1$ and this will make the latter set small. Specifically, a result of Norton [7] shows that

$$\#\mathscr{L}_6(x) \ll \frac{x}{(\log_2 x)^{1/2}}\exp\left(-(1-\delta(x)\log(e/\delta(x)))\log_2 x\right).$$

If we set $\eta(x) = (\log_3 x - \log_4 x)/\log_2 x$, we then have

$$\begin{aligned}\delta(x)\log(e/\delta(x)) &= (\alpha+\beta)(1-\eta(x))\log\left(\frac{e}{\alpha+\beta}\left(1+\eta(x)+O(\eta(x)^2)\right)\right)\\ &= (\alpha+\beta)(1-\eta(x))\left(\log\left(\frac{e}{\alpha+\beta}\right)+\eta(x)+O(\eta(x)^2)\right)\\ &= (\alpha+\beta)\log\left(\frac{e}{\alpha+\beta}\right)+\gamma\eta(x)+O(\eta(x)^2),\end{aligned}$$

where we have set $\gamma = (\alpha+\beta-\log(e/(\alpha+\beta)))$. We get that

$$\begin{aligned}&\left(1-\delta(x)\log\left(\frac{e}{\delta(x)}\right)\right)\log_2 x\\ &\quad = \left(1-(\alpha+\beta)\log\left(\frac{e}{\alpha+\beta}\right)\right)\log_2 x - \gamma(\log_3 x - \log_4 x) + o(1),\end{aligned}$$

https://doi.org/10.1017/S144678870001750X Published online by Cambridge University Press

therefore

$$\#\mathscr{L}_6(x) \ll \frac{x(\log_2 x)^{-1/2+\gamma}}{(\log x)^{1-(\alpha+\beta)\log(e/(\alpha+\beta))}(\log_3 x)^\gamma}. \tag{3.4}$$

Optimizing the exponent of $\log x$ among $\#\mathscr{L}_4(x)$, $\#\mathscr{L}_5(x)$ and $\#\mathscr{L}_6(x)$ (see (3.2)–(3.4)), we get $\alpha = \beta$ and $1 - \alpha\log(e/\alpha) = 1 - (\alpha+\beta)\log(e/(\alpha+\beta))$. This gives $\alpha = e/4$, $\gamma = e/2 - \log 2 = .66599\ldots$, $1 - \alpha\log(e/\alpha) = 1 - e\log 2/2 = 0.0579\ldots$, leading to the bound

$$\#\mathscr{L}_6(x) \ll \frac{x(\log_2 x)^{-1/2+e/2-\log 2}}{(\log x)^{1-e\log 2/2}(\log_3 x)^{e/2-\log 2}}.$$

The theorem now follows from estimates (3.2)–(3.4) and the stronger bounds for $\mathscr{L}_1$, $\mathscr{L}_2$, $\mathscr{L}_3$, in fact in the slightly sharper form

$$\#\mathscr{L}(x) \ll \frac{x}{(\log x)^\kappa}(\log\log x)^{5/2+\kappa}(\log\log\log x)^{-\kappa},$$

where κ was defined in the statement of the theorem. □

In conclusion we remark that there was no necessity to choose α and β to be fixed. By slightly perturbing the above choices by a function of x tending to zero as x approaches infinity, one can obtain a very minor improvement sharpening slightly the exponent $5/2 + \kappa$ of $\log\log x$.

Acknowledgments

Most of this paper was written during a very enjoyable visit by the first author to the Mathematical Institute of the UNAM in Morelia, Mexico. This author wishes to express his thanks to that institution for the hospitality and support. Research of J. F. is also partially supported by NSERC grant A5123 and a Killam Research Fellowship.

References

[1] W. D. Banks, J. B. Friedlander, F. Luca, F. Pappalardi and I. E. Shparlinski, 'Coincidences in the values of the Euler and Carmichael functions', *Acta Arith.* **122** (2006), 207–234.

[2] P. Erdős, C. Pomerance and E. Schmutz, 'Carmichael's lambda function', *Acta Arith.* **58** (1991), 363–385.

[3] P. Erdős and S. S. Wagstaff Jr., 'The fractional parts of the Bernoulli numbers', *Illinois J. Math.* **24** (1980), 104–112.

[4] K. Ford, 'The distribution of totients', *Ramanujan J.* **2** (1998), 67–151.

[5] H. Halberstam and H.-E. Richert, *Sieve methods* (Academic Press, London, UK, 1974).
[6] H. Maier and C. Pomerance, 'On the number of distinct values of Euler's ϕ function', *Acta Arith.* **49** (1988), 263–275.
[7] K. K. Norton, 'On the number of restricted prime factors of an integer. I', *Illinois J. Math.* **20** (1976), 681–705.
[8] G. Tenenbaum, *Introduction to analytic and probabilistic number theory* (University Press, Cambridge, UK, 1985).

Department of Mathematics
University of Toronto
Toronto, Ontario M5S 3G3
Canada
e-mail: frdlndr@math.toronto.edu

Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán
México
e-mail: fluca@matmor.unam.mx

https://doi.org/10.1017/S144678870001750X Published online by Cambridge University Press