





Journal of Number Theory 103 (2003) 122-131

http://www.elsevier.com/locate/jnt

Square-free values of the Carmichael function

Francesco Pappalardi,^a Filip Saidak,^b and Igor E. Shparlinski^{c,*}

^a Dipartimento di Matematica, Università degli Studi Roma Tre Largo S.L. Murialdo, 1, Roma 00146, Italy ^b Department of Mathematics, University of Calgary, Calgary, Al., Canada TN2 1N4 ^c Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

Received 13 November 2002; revised 4 February 2003

Communicated by A. Granville

Abstract

We obtain an asymptotic formula for the number of square-free values among p - 1, for primes $p \le x$, and we apply it to derive the following asymptotic formula for L(x), the number of square-free values of the Carmichael function $\lambda(n)$ for $1 \le n \le x$,

$$L(x) = (\kappa + o(1))\frac{x}{\ln^{1-\alpha} x},$$

where $\alpha = 0.37395...$ is the Artin constant, and $\kappa = 0.80328...$ is another absolute constant. © 2003 Elsevier Inc. All rights reserved.

Keywords: Square-free integers; Carmichael function; Wirsing theorem

1. Introduction

Recall that an integer $s \ge 1$ is called *square-free* if it is not divisible by the square of any prime number. We denote by \mathscr{S} the set of square-free positive integers, and let $\varphi(n)$ to be the number of positive $m \le n$, coprime to n.

Clearly, if *n* has at least two odd prime divisors then $4|\varphi(n)$. The same way, if $p^3|n$ for a prime *p* then $p^2|\varphi(n)$. Thus, for $n \ge 5$, $\varphi(n) \in \mathcal{S}$ if and only if *n* is of the form $n = p^2$, $2p^2$, 2p or n = p, where $p \ge 3$ is a prime such that $p - 1 \in \mathcal{S}$. Thus, denoting by

^{*}Corresponding author. Fax: +61-0-9850-9551.

E-mail addresses: pappa@mat.uniroma3.it (F. Pappalardi), filips@math.ucalgary.ca (F. Saidak), igor@ics.mq.edu.au (I.E. Shparlinski).

F(x) the number of positive integers $n \leq x$ for which $\varphi(n) \in \mathcal{S}$, we obtain

$$F(x) = \pi_{\rm sf}(x) + \pi_{\rm sf}(x/2) + O(x^{1/2}/\ln x), \tag{1}$$

where $\pi_{sf}(x)$ is the number of primes $p \leq x$ for which $p - 1 \in \mathcal{S}$.

First, we recall the asymptotic formula $\pi_{sf}(x) \sim \alpha \pi(x)$, see [15] and Lemma 3 below, which shows that the density of primes p with $p - 1 \in \mathcal{S}$ is given by the Artin constant

$$\alpha = \prod_{p} \left(1 - \frac{1}{p(p-1)} \right) = 0.37395...,$$

see [4,12]. Together with (1), this estimate immediately produces an asymptotic formula for F(x).

We recall that the Carmichael function $\lambda(n)$ is defined to be the largest possible order of any element in the unit group of the residue ring modulo $n \ge 1$. More explicitly, for a prime power p^{ν} , we have

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

and for arbitrary $n \ge 2$,

$$\lambda(n) = \operatorname{lcm}(\lambda(p_1^{v_1}), \dots, \lambda(p_v^{v_s})),$$

where $n = p_1^{v_1} \dots p_s^{v_s}$ is the prime factorization of *n*. One also has $\lambda(1) = 1$.

We use the asymptotic formula for F(x) in combination with a theorem of Wirsing in order to derive that $L(x) \sim \kappa x \ln^{\alpha-1} x$, for some constant $\kappa > 0$, where L(x) is the number of positive integers $n \leq x$, for which $\lambda(n) \in \mathcal{S}$.

We remark that various arithmetic properties of $\varphi(n)$ and $\lambda(n)$ have been considered in the literature, see [2,7–10,14] and references therein, but the question about square-freeness appears to be new.

Throughout the paper, the implied constants in symbols 'O' and ' \ll ' may depend, where obvious, on a certain parameter A > 0, and are absolute otherwise (we recall that $U \ll V$ is equivalent to U = O(V)). As usual, p always denotes a prime number, and $\pi(x)$ is the number of primes $p \leqslant x$.

2. Necessary tools

Our results depend on some analytic results.

We recall that an arithmetic function f(n) is called *multiplicative* if f(nm) = f(n)f(m) for any integers *n* and *m* with gcd(n,m) = 1. Then the theorem of Wirsing [20] can be formulated as follows.

Lemma 1. Assume that a real-valued multiplicative function f(n) satisfies the following conditions:

- $f(n) \ge 0, n = 1, 2, ...;$
- $f(p^{\nu}) \leq c_1 c_2^{\nu}, \nu = 2, 3, ..., for some constants c_1, c_2 with c_2 < 2;$
- there exists a constant $\tau > 0$ such that

$$\sum_{p \leqslant x} f(p) = (\tau + o(1)) \frac{x}{\ln x}$$

Then for any $x \ge 0$ *,*

$$\sum_{n \leqslant x} f(n) = \left(\frac{1}{e^{\gamma \tau} \Gamma(\tau)} + o(1)\right) \frac{x}{\ln x} \prod_{p \leqslant x} \sum_{\nu=0}^{\infty} \frac{f(p^{\nu})}{p^{\nu}},$$

where γ is the Euler constant, and

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$$

is the gamma function.

Finally, we use partial summation in the following form.

Lemma 2. For any function g(t), having a continuous derivative in the interval [1, n], and any sequence a_1, \ldots, a_n , we have

$$\sum_{k=1}^{n} a_k g(k) = A(n)g(n) - \int_1^n A(t)g'(t) \, dt,$$

where

$$A(T) = \sum_{1 \leqslant k \leqslant T} a_k.$$

The following result has appeared already, without a proof, in [15]. A proof, however, can easily be obtained from the representation

$$\begin{split} \psi_{\rm sf}(x) &= \sum_{1 \leqslant m \leqslant x^{1/2}} \mu(m) \psi(x, m^2, 1) \\ &= \sum_{1 \leqslant m \leqslant x^{1/5}} \mu(m) \psi(x, m^2, 1) + \sum_{x^{1/5} < m \leqslant x^{1/2}} \mu(m) \psi(x, m^2, 1), \end{split}$$

where

$$\psi_{\mathrm{sf}}(x) = \sum_{\substack{1 \leqslant n \leqslant x \\ n \in \mathscr{S}}} \Lambda(n) \quad \mathrm{and} \quad \psi(x,k,l) = \sum_{\substack{1 \leqslant n \leqslant x \\ n \equiv l \; (\mathrm{mod}\; k)}} \Lambda(n)$$

and $\Lambda(n)$ is the von Mangoldt function, that is, $\Lambda(n) = \ln p$ if *n* is a power of a prime *p* and $\Lambda(n) = 0$ otherwise. Now one can apply the Bombieri–Vinogradov theorem, see [5] to the first sum and the trivial bound $\psi(x, k, l) \leq xk^{-1} \ln x$ to the second sum. Finally, partial summation produces the following statement.

Lemma 3. For any constant A > 0 we have

$$\pi_{\rm sf}(x) = \alpha \pi(x) + O\left(\frac{x}{\ln^A x}\right).$$

In particular, from (1), Lemma 3 and the prime number theorem we conclude that

$$F(X) = \frac{3\alpha}{2}\pi(x) + O(x\ln^{-2} x).$$

Now we establish an analogue of the Mertens formula.

Lemma 4. There exists an absolute constant η such that

$$\prod_{\substack{p \le x\\p-1 \in \mathscr{S}}} \left(1 + \frac{1}{p} + \frac{1}{p^2} \right) = \eta \ln^{\alpha} x + O(\ln^{\alpha - 1} x).$$
(2)

Proof. In view of the fact that

$$\ln\left(1+\frac{1}{p}+\frac{1}{p^2}\right) = \frac{1}{p} + O\left(\frac{1}{p^2}\right),$$

it is equivalent to prove that there exists an absolute constant ζ such that

$$\rho_{\mathrm{sf}}(x) = \sum_{\substack{p \leqslant x \\ p-1 \in \mathscr{S}}} \frac{1}{p} = \alpha \ln \ln x + \zeta + O(\ln^{-1} x).$$

Observe that

$$\sum_{\substack{p \leq x \\ p-1 \in \mathscr{S}}} \frac{\ln p}{p} = \frac{\pi_{\rm sf}(x) \ln x}{x} + \int_2^x \frac{\ln t - 1}{t^2} \pi_{\rm sf}(t) \, dt = \alpha \int_2^x \frac{\ln t - 1}{t^2} \pi(t) \, dt + O(1).$$

The same arguments also imply that

$$\sum_{p \leq x} \frac{\ln p}{p} = \int_2^x \frac{\ln t - 1}{t^2} \pi(t) \, dt + O(1)$$

and the Mertens theorem, see Theorem 3.1 of Chapter 1 in [19], yields

$$\vartheta_{\mathrm{sf}}(x) = \sum_{\substack{p \leqslant x \\ p-1 \in \mathscr{S}}} \frac{\ln p}{p} = \alpha \ln x + r(x),$$

where r(x) = O(1). Applying Lemma 2 we derive

$$\rho_{\rm sf}(x) = \frac{9_{\rm sf}(x)}{\ln x} + \int_2^x \frac{9_{\rm sf}(x)}{t \ln^2 t} dt$$

= $\frac{\alpha \ln x + r(x)}{\ln x} + \int_2^x \frac{\alpha \ln t + r(t)}{t \ln^2 t} dt$
= $\alpha \ln \ln x - \alpha \ln \ln 2 + \alpha + \int_2^x \frac{r(t)}{t \ln^2 t} dt + O(\ln^{-1} x)$
= $\alpha \ln \ln x - \alpha \ln \ln 2 + \alpha + \int_2^\infty \frac{r(t)}{t \ln^2 t} dt + O(\ln^{-1} x)$

(here the existence of the improper integral follows from r(t) = O(1)). \Box

3. Square-free values of the Carmichael function

We note that $\lambda(n) \in \mathcal{S}$ if and only if $\lambda(p_i^{v_i}) \in \mathcal{S}$ for every i = 1, ..., s, where $n = p_1^{v_1} \dots p_v^{v_s}$ is the prime factorization of n. Hence $\lambda(n) \in \mathcal{S}$ if and only if n is not divisible by 16 and is not divisible by p^3 for $p \ge 3$ and is composed of primes p with $p - 1 \in \mathcal{S}$. Thus Lemmas 1 and 3 imply an asymptotic result concerning L(x).

Theorem 5. Let $\kappa = 15\eta/14e^{\gamma\alpha}\Gamma(\alpha)$ where α is the Artin constant, γ is the Euler constant and η is defined in Lemma 4. Then

$$L(x) = (\kappa + o(1)) \frac{x}{\ln^{1-\alpha} x}.$$

Proof. Let us consider the multiplicative function f(n) for which $f(p^2) = f(p) = 1$ if $p - 1 \in \mathcal{S}$ and $f(p^v) = 0$ if either $v \ge 3$ or $p - 1 \notin \mathcal{S}$, for each odd prime p. We also put f(2) = f(4) = f(8) = 1 and $f(2^v) = 0$ if $v \ge 4$.

126

Therefore, for $n \ge 5$, $\lambda(n) \in \mathscr{S}$ if and only if f(n) = 1. From Lemma 3 we see that the conditions of Lemma 1 are satisfied with $\tau = \alpha$, so we have

$$\begin{split} L(x) &= \sum_{n \leq x} f(n) + O(1) = \left(\frac{1}{e^{\gamma \alpha} \Gamma(\alpha)} + o(1)\right) \frac{x}{\ln x} \prod_{p \leq x} \sum_{\nu=0}^{\infty} \frac{f(p^{\nu})}{p^{\nu}} \\ &= \left(\frac{1}{e^{\gamma \alpha} \Gamma(\alpha)} + o(1)\right) \frac{15x}{8 \ln x} \prod_{\substack{3 \leq p \leq x\\ p-1 \in \mathscr{S}}} \left(1 + \frac{1}{p} + \frac{1}{p^2}\right) \\ &= \left(\frac{1}{e^{\gamma \alpha} \Gamma(\alpha)} + o(1)\right) \frac{15x}{14 \ln x} \prod_{\substack{2 \leq p \leq x\\ p-1 \in \mathscr{S}}} \left(1 + \frac{1}{p} + \frac{1}{p^2}\right). \end{split}$$

Using (2) we derive the result. \Box

We now derive an upper bound for the number of square-free values of $\lambda(n)$ in a short interval. Let L(x, y) denote the number of positive integers $x - y \le n \le x$, for which the Carmichael function $\lambda(n) \in \mathcal{S}$.

Theorem 6. For any x > y > 1 we have

$$L(x,y) \ll \frac{y}{\ln^{1-\alpha} y}.$$

Proof. We merely drop the condition that relevant values of *n* must not be divisible by a cube of a prime and write $L(x, y) \leq S(x, y)$, where S(x, y) is the number of positive integers $x - y \leq n \leq x$ such that gcd(n, p) = 1 for any *p* with $p - 1 \notin \mathcal{S}$. Combining the first bound of Corollary 4 with Corollary 2.3.1 in Section 2.6 of [11] we finish the proof. \Box

4. Calculations

Unfortunately, it seems that there are no closed form analytic expressions for the constants α , η and κ .

Using PARI [3], and Lemma 4 (with primes up to $4 \cdot 10^8$) we have obtained the following approximation for η :

$$\tilde{\eta} = \frac{1}{(\ln 4 \cdot 10^8)^{\alpha}} \prod_{\substack{p \le 4 \cdot 10^8 \\ p-1 \in \mathscr{S}}} \left(1 + \frac{1}{p} + \frac{1}{p^2} \right) = 2.1171 \dots$$

which implies

$$\tilde{\kappa} = \frac{15\tilde{\eta}}{14e^{\gamma\alpha}\Gamma(\alpha)} = 0.80328\dots$$
 (3)

We have also computed (in a rather straightforward fashion, without any serious efforts to optimize the calculations) $\tilde{\kappa}(x) = L(x)x^{-1}\ln^{1-\alpha}x$ which exhibits a rather slow convergence to κ :

x	$\widetilde{\kappa}(x)$	x	$\widetilde{\kappa}(x)$	x	$\widetilde{\kappa}(x)$
107	0.8585513	$6 \cdot 10^{7}$	0.8518393	$20 \cdot 10^{7}$	0.8482225
$2 \cdot 10^{7}$	0.8556957	$7 \cdot 10^{7}$	0.8513639	$30 \cdot 10^{7}$	0.8471133
$3 \cdot 10^{7}$	0.8542084	8 · 10 ⁷	0.8508742	$40 \cdot 10^{7}$	0.8463676
$4 \cdot 10^{7}$	0.8531435	$9 \cdot 10^{7}$	0.8505291		
$5 \cdot 10^{7}$	0.8524153	$10 \cdot 10^{7}$	0.8502255		

Furthermore, we have also computed

$$\tilde{\kappa}(x,y) = (L(x+y) - L(x))((x+y)\ln^{\alpha-1}(x+y) - x\ln^{\alpha-1}x)^{-1},$$

where the convergence to the value (3) seems somewhat faster.

у	$\widetilde{\kappa}(10^{20}, y)$	У	$\widetilde{\kappa}(10^{20}, y)$	У	$\widetilde{\kappa}(10^{20}, y)$
10 ⁶	0.8215991	$5 \cdot 10^{6}$	0.8194758	9 · 10 ⁶	0.8186230
$2 \cdot 10^{6}$	0.8203167	$6 \cdot 10^{6}$	0.8191755	$10 \cdot 10^{6}$	0.8188303
$3\cdot 10^6$	0.8190902	$7 \cdot 10^{6}$	0.8193178	$11 \cdot 10^{6}$	0.8188164
$4 \cdot 10^{6}$	0.8183822	$8 \cdot 10^6$	0.8189953	$12 \cdot 10^{6}$	0.8186914

У	$\widetilde{\kappa}(10^{30}, y)$	<i>y</i>	$\widetilde{\kappa}(2\cdot 10^{30},y)$	<i>y</i>	$\widetilde{\kappa}(3\cdot 10^{30},y)$
107	0.8144590	107	0.8137660	107	0.8139725
$2 \cdot 10^7$	0.8142472	$2 \cdot 10^{7}$	0.8138552	$2 \cdot 10^{7}$	0.8146238
$3 \cdot 10^{7}$	0.8145223	$3 \cdot 10^{7}$	0.8140572	$3 \cdot 10^{7}$	0.8138039
$4 \cdot 10^{7}$	0.8145319	$4 \cdot 10^{7}$	0.8140761	$4 \cdot 10^{7}$	0.8136268

We remark that observing how calculations behave, we give much more trust to the numerical value of κ which follows from (3) rather than to the approximations from the above tables.

5. k-Free values of the Carmichael function

We recall that an integer is said to be k-free if it is not divisible by the kth power of any prime number.

The feature of the Carmichael function that allowed us to prove Theorem 5 is that the arithmetic function $\mu^2(\lambda(n))$ is multiplicative. The same fact holds for k-free values of $\lambda(n)$. More precisely, if \mathscr{S}_k is the set of integers which are k-free, then $\lambda(n) \in \mathscr{S}_k$ if and only if $\lambda(p_i^{k_1}) \in \mathscr{S}_k$ for every i = 1, ..., v where $n = p_1^{k_1} ... p_v^{k_v}$.

128

One observes that the same arguments which give Lemma 3, which has been outlined in Section 2, gives for any A > 0,

$$#\{p \leq x \mid p \in \mathscr{S}_k\} = \alpha_k \pi(x) + O\left(\frac{x}{\ln^A x}\right),$$

where

$$\alpha_k = \prod_p \left(1 - \frac{1}{p^{k-1}(p-1)} \right).$$
(4)

Accordingly, we obtain

$$\prod_{\substack{p \leq x\\p-1 \in \mathscr{S}_k}} \ln\left(1 + \frac{1}{p} + \dots + \frac{1}{p^k}\right) = \eta_k \ln^{\alpha_k} x + O\left(\ln^{\alpha_k - 1} x\right).$$
(5)

Next one notices that, if p > 3, then $\lambda(p^m) \in \mathscr{S}_k$ if and only if $m \leq k$ and $p - 1 \in \mathscr{S}_k$ while $\lambda(2^m) \in \mathscr{S}_k$ if and only if m < k + 3. Now the application of the Wirsing theorem given in Lemma 1 yields:

Theorem 7. Let

$$\kappa_k = \frac{2^{k+2}-1}{2^{k+2}-2} \cdot \frac{\eta_k}{e^{\gamma \alpha_k} \Gamma(\alpha_k)};$$

where α_k is defined in (4) and η_k is defined by (5). Then

$$L_k(x) = (\kappa_k + o(1))x \ln^{1-\alpha_k} x.$$

Interestingly, the problem of enumerating the k-free values of the Euler function for $k \ge 3$ seems to be more involved than in the case k = 2. For example, the corresponding *n* may have a more complicated structure with up to k prime divisors *p*, for which the arithmetic structure of p - 1 must be studied simultaneously.

6. Remarks

The proof of Lemma 3 which we have indicated uses only a fraction of the power of the Bombieri–Vinogradov theorem because we estimate the sums over perfect squares of a given interval by the sum over all integers of that interval. In fact, there is a seemingly more suitable form of the Bombieri–Vinogradov theorem where the summation is taken over any polynomial sequence of moduli, see [6]. Unfortunately, it does not seem to improve the error terms in our results. On the other hand, it is clear that the Extended Riemann Hypothesis implies a much better error in Lemma 3. Indeed, using the bound

$$\psi(x, m^2, 1) = \frac{x}{\varphi(m^2)} + O(x^{1/2} \ln^2 x)$$

(for example, see (1.32) in Chapter 1 of [4] or (5.12) in Chapter 7 of [19]) for $m \le x^{1/4}$; and $\psi(x,k,l) \le xk^{-1} \ln x$, for $m > x^{1/4}$; we obtain an error term of order $x^{3/4+\varepsilon}$ for any $\varepsilon > 0$.

It is also clear that the above method can be used to count square-free and, more generally, k-free values among p + a, for any integer a.

We remark that the regular behavior of $\tilde{\kappa}(x) - \kappa$, exhibited in Section 4 may suggest the existence of the second main term in the asymptotic formula for L(x). Maybe more detailed calculations, in a wide range, may help to clarify this matter.

Finally, it would be interesting to study how often the multiplicative order $l_g(n)$ of a given integer $g \ge 2$ is square-free. The number of prime divisors and the largest prime divisor of $l_g(n)$ have been studied in [16,18,1,19], respectively. An asymptotic formula for the number of primes $p \le x$ for which $(p-1)/l_g(p)$ is square-free is given in [17]. Some arithmetic properties of $\lambda(n)/l_g(n)$ have been studied in [13].

Acknowledgments

The authors thank Andrew Granville for careful reading of the manuscript, for several helpful observations and for pointing out an error in the original version of the paper.

References

- [1] W. Banks, I.E. Shparlinski, Smooth values of the Euler function, preprint 2002, 1-11.
- [2] N.L. Bassily, I. Kátai, M. Wijsmuller, On the prime power divisors of the iterates of the Euler- ϕ function, Publ. Math. Debrecen 55 (1999) 17–32.
- [3] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, GP/PARI CALCULATOR Version 2.1.4. UltraSpare (MicroSpare kernel) 32-bit version, 2002.
- [4] R. Crandall, C. Pomerance, Prime Numbers: A Computational Perspective, Springer, Berlin, 2001.
- [5] H. Davenport, Multiplicative Number Theory, 2nd Edition, Springer, New York, 1980.
- [6] P.D.T.A. Elliott, Primes in short arithmetic progressions with rapidly increasing differences, Trans. Amer. Math. Soc. 353 (2001) 2705–2724.
- [7] P. Erdős, A. Granville, C. Pomerance, C. Spiro, On the normal behaviour of the iterates of some arithmetic functions, in: B.C. Berndt, H.G. Diamond, H. Halberstam, A. Hildebrand (Eds.), Analytic Number Theory, Birkhäuser, Boston, 1990, pp. 165–204.
- [8] P. Erdős, C. Pomerance, On the normal number of prime factors of $\varphi(n)$, Rocky Mountain J. Math. 15 (1985) 343–352.
- [9] P. Erdős, C. Pomerance, E. Schmutz, Carmichael's lambda function, Acta Arith. 58 (1991) 363–385.
- [10] J.B. Friedlander, C. Pomerance, I.E. Shparlinski, Period of the power generator and small values of Carmichael's function, Math. Comp. 70 (2001) 1591–1605.
- [11] H. Halberstam, H.-E. Richert, Sieve Methods, Academic Press, London, 1974.

130

- [12] C. Hooley, On Artin's conjecture, J. Reine Angew. Math. 225 (1967) 209-220.
- [13] S. Li, C. Pomerance, On generalizing Artin's conjecture on primitive roots to composite moduli, J. Reine Angew. Math. 556 (2003) 205–224.
- [14] F. Luca, C. Pomerance, On some problems of Mąkowski–Schinzel and Erdős concerning the arithmetical functions φ and σ , Colloq. Math. 92 (2002) 111–130.
- [15] L. Mirsky, The number of representations of an integer as the sum of a prime and a k-free integer, Amer. Math. Monthly 56 (1949) 17–19.
- [16] M.R. Murty, F. Saidak, Non-abelian generalizations of the Erdős–Kac theorem, Canad. J. Math., to appear.
- [17] F. Pappalardi, On Hooley's theorem with weights, Rend. Sem. Mat. Univ. Pol. Torino 53 (1995) 375–388.
- [18] C. Pomerance, I.E. Shparlinski, Smooth orders and cryptographic applications, Lecture Notes in Comptuer Science, Springer, Berlin, Vol. 2369, 2002, pp. 338–348.
- [19] K. Prachar, Primzahlverteilung, Springer, Berlin, 1957.
- [20] E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen, Math. Ann. 143 (1961) 75–102.