# Algebra & Number Theory

Volume 8

2014

No. 8


## The image of Carmichael's $\lambda$-function


Kevin Ford, Florian Luca and Carl Pomerance



msp

ALGEBRA AND NUMBER THEORY 8:8 (2014)
dx.doi.org/10.2140/ant.2014.8.2009

# The image of Carmichael's λ-function

Kevin Ford, Florian Luca and Carl Pomerance

We show that the counting function of the set of values of Carmichael's λ-function is $x/(\log x)^{\eta+o(1)}$, where $\eta = 1 - (1 + \log\log 2)/(\log 2) = 0.08607\ldots$.

## 1. Introduction

Euler's function $\varphi$ assigns to a natural number $n$ the order of the group of units of the ring of integers modulo $n$. It is of course ubiquitous in number theory, as is its close cousin $\lambda$, which gives the exponent of the same group. Already appearing in Gauss's *Disquisitiones Arithmeticae*, $\lambda$ is commonly referred to as Carmichael's function, after R. D. Carmichael, who studied it about a century ago. (A *Carmichael number* $n$ is composite but nevertheless satisfies $a^n \equiv a \pmod{n}$ for all integers $a$, just as primes do. Carmichael discovered these numbers, which are characterized by the property that $\lambda(n) \mid n-1$.)

It is interesting to study $\varphi$ and $\lambda$ as functions. For example, how easy is it to compute $\varphi(n)$ or $\lambda(n)$ given $n$? It is indeed easy if we know the prime factorization of $n$. Interestingly, we know the converse. By [Miller 1976], given either $\varphi(n)$ or $\lambda(n)$, it is easy to find the prime factorization of $n$.

Within the realm of "arithmetic statistics" one can also ask for the behavior of $\varphi$ and $\lambda$ on typical inputs $n$, and ask how far this varies from their values on average. For $\varphi$, this type of question goes back to the dawn of the field of probabilistic number theory with the seminal paper of Schoenberg [1928], while some results in this vein for $\lambda$ are found in [Erdős et al. 1991].

One can also ask about the value sets of $\varphi$ and $\lambda$. That is, what can one say about the integers which appear as the order or exponent of the groups $(\mathbb{Z}/n\mathbb{Z})^*$?

These are not new questions. Let $V_\varphi(x)$ denote the number of positive integers $n \leqslant x$ for which $n = \varphi(m)$ for some $m$. Pillai [1929] showed $V_\varphi(x) \leqslant x/(\log x)^{c+o(1)}$ as $x \to \infty$, where $c = (\log 2)/e$. On the other hand, since $\varphi(p) = p-1$, $V_\varphi(x)$ is at least $\pi(x+1)$ (the number of primes in $[1, x+1]$), and so $V_\varphi(x) \geqslant (1+o(1))x/\log x$.

---

Ford was supported in part by National Science Foundation grant DMS-1201442. Pomerance was supported in part by NSF grant DMS-1001180.
*MSC2010:* primary 11N64; secondary 11A25, 11N25.
*Keywords:* Carmichael's function, Carmichael's lambda function.

In one of his earliest papers, Erdős [1935] showed that the lower bound is closer to the truth: we have $V_\varphi(x) = x/(\log x)^{1+o(1)}$ as $x \to \infty$. This result has since been refined by a number of authors, including Erdős and Hall, Maier and Pomerance, and Ford; see [Ford 1998] for the current state of the art.

Essentially the same results hold for the sum-of-divisors function $\sigma$, but only recently were we able to show that there are infinitely many numbers that are simultaneously values of $\varphi$ and of $\sigma$ [Ford et al. 2010] , thus settling an old problem of Erdős.

In this paper, we address the range problem for Carmichael's function $\lambda$. From the definition of $\lambda(n)$ as the exponent of the group $(\mathbb{Z}/n\mathbb{Z})^*$, it is immediate that $\lambda(n) \mid \varphi(n)$ and that $\lambda(n)$ is divisible by the same primes as $\varphi(n)$. We also have

$$\lambda(n) = \operatorname{lcm}[\lambda(p^a) : p^a \parallel n],$$

where $\lambda(p^a) = p^{a-1}(p-1)$ for odd primes $p$ with $a \geqslant 1$ or $p = 2$ and $a \in \{1, 2\}$. Further, $\lambda(2^a) = 2^{a-2}$ for $a \geqslant 3$. Put $V_\lambda(x)$ for the number of integers $n \leqslant x$ with $n = \lambda(m)$ for some $m$. Note that since $p - 1 = \lambda(p)$ for all primes $p$, it follows that

$$V_\lambda(x) \geqslant \pi(x+1) = (1+o(1))\frac{x}{\log x} \quad (x \to \infty), \tag{1-1}$$

as with $\varphi$. In fact, one might suspect that the story for $\lambda$ is completely analogous to that of $\varphi$. As it turns out, this is not the case.

It is fairly easy to see that $V_\varphi(x) = o(x)$ as $x \to \infty$, since most numbers $n$ are divisible by many different primes, so most values of $\varphi(n)$ are divisible by a high power of 2. This argument fails for $\lambda$, and in fact it is not immediately obvious that $V_\lambda(x) = o(x)$ as $x \to \infty$. Such a result was first shown in [Erdős et al. 1991], where it was established that there is a positive constant $c$ with $V_\lambda(x) \ll x/(\log x)^c$. In [Friedlander and Luca 2007], a value of $c$ in this result was computed. It was shown there that, as $x \to \infty$,

$$V_\lambda(x) \leqslant \frac{x}{(\log x)^{\alpha+o(1)}} \quad \text{holds with} \quad \alpha = 1 - e(\log 2)/2 = 0.057913\ldots. \tag{1-2}$$

The exponents on the logarithms in the lower and upper bounds (1-1) and (1-2) were brought closer in the recent paper [Luca and Pomerance 2014], where it was shown that, as $x \to \infty$,

$$\frac{x}{(\log x)^{0.359052}} < V_\lambda(x) \leqslant \frac{x}{(\log x)^{\eta+o(1)}} \text{ with } \eta = 1 - \frac{1+\log\log 2}{\log 2} = 0.08607\ldots.$$

In Section 2.1 of that paper, a heuristic was presented suggesting that the correct exponent of the logarithm should be the number $\eta$. In the present paper, we confirm the heuristic from [Luca and Pomerance 2014] by proving the following theorem:

**Theorem 1.** *We have* $V_\lambda(x) = x(\log x)^{-\eta+o(1)}$ *as* $x \to \infty$.

Just as results on $V_\varphi(x)$ can be generalized to similar multiplicative functions, such as $\sigma$, we would expect our result to be generalizable to functions similar to $\lambda$ enjoying the property $f(mn) = \operatorname{lcm}[f(m), f(n)]$ when $m, n$ are coprime.

Since the upper bound in Theorem 1 was proved in [Luca and Pomerance 2014], we need only show that $V_\lambda(x) \geqslant x/(\log x)^{\eta+o(1)}$ as $x \to \infty$. We remark that in our lower bound argument we will count only squarefree values of $\lambda$.

The same number $\eta$ in Theorem 1 appears in an unrelated problem. As shown by Erdős [1960], the number of distinct entries in the multiplication table for the numbers up to $n$ is $n^2/(\log n)^{\eta+o(1)}$ as $n \to \infty$. Similarly, the asymptotic density of the integers with a divisor in $[n, 2n]$ is $1/(\log n)^{\eta+o(1)}$ as $n \to \infty$. See [Ford 2008a; 2008b] for more on these kinds of results. As explained in the heuristic argument presented in [Luca and Pomerance 2014], the source of $\eta$ in the $\lambda$-range problem comes from the distribution of integers $n$ with about $(1/\log 2)\log\log n$ prime divisors: the number of these numbers $n \in [2, x]$ is $x/(\log x)^{\eta+o(1)}$ as $x \to \infty$. Curiously, the number $\eta$ arises in the same way in the multiplication table problem: most entries in an $n$-by-$n$ multiplication table have about $(1/\log 2)\log\log n$ prime divisors (a heuristic for this is given in the introduction of [Ford 2008a]).

We mention two related unsolved problems. Several papers [Banks et al. 2004; Banks and Luca 2011; Freiberg 2012; Pollack and Pomerance 2014] have discussed the distribution of numbers $n$ such that $n^2$ is a value of $\varphi$; in [Pollack and Pomerance 2014] it was shown that the number of such $n \leqslant x$ is between $x/(\log x)^{c_1}$ and $x/(\log x)^{c_2}$, where $c_1 > c_2 > 0$ are explicit constants. Is the count of the form $x/(\log x)^{c+o(1)}$ for some number $c$? The numbers $c_1, c_2$ in [Pollack and Pomerance 2014] are not especially close. The analogous problem for $\lambda$ is wide open. In fact, it seems that a reasonable conjecture (from [Pollack and Pomerance 2014]) is that asymptotically all even numbers $n$ have $n^2$ in the range of $\lambda$. On the other hand, it has not been proved that there is a lower bound of the shape $x/(\log x)^c$ with some positive constant $c$ for the number of such numbers $n \leqslant x$.

## 2. Lemmas

Here we present some estimates that will be useful in our argument. To fix notation, for a positive integer $q$ and an integer $a$, we let $\pi(x; q, a)$ be the number of primes $p \leqslant x$ in the progression $p \equiv a \pmod q$, and put

$$E^*(x; q) = \max_{y \leqslant x} \left| \pi(y; q, 1) - \frac{\operatorname{li}(y)}{\varphi(q)} \right|,$$

where $\operatorname{li}(y) = \int_2^y dt/\log t$.

We also let $P^+(n)$ and $P^-(n)$ denote the largest and smallest prime factors of $n$, respectively, with the convention that $P^-(1) = \infty$ and $P^+(1) = 0$. Let $\omega(m)$ be the number of distinct prime factors of $m$, and let $\tau_k(n)$ be the $k$-th divisor function;

that is, the number of ways to write $n = d_1 \cdots d_k$ with $d_1, \dots, d_k$ positive integers. Let $\mu$ denote the Möbius function.

First, we present an estimate for the sum of reciprocals of integers with a given number of prime factors.

**Lemma 2.1.** *Suppose $x$ is large. Uniformly for $1 \leqslant h \leqslant 2 \log\log x$,*

$$\sum_{\substack{P^+(b) \leqslant x \\ \omega(b)=h}} \frac{\mu^2(b)}{b} \asymp \frac{(\log\log x)^h}{h!}.$$

*Proof.* The upper bound follows very easily from

$$\sum_{\substack{P^+(b) \leqslant x \\ \omega(b)=h}} \frac{\mu^2(b)}{b} \leqslant \frac{1}{h!}\biggl(\sum_{p \leqslant x} \frac{1}{p}\biggr)^h = \frac{(\log\log x + O(1))^h}{h!} \asymp \frac{(\log\log x)^h}{h!}$$

upon using Mertens' theorem and the given upper bound on $h$. For the lower bound, we have

$$\sum_{\substack{P^+(b) \leqslant x \\ \omega(b)=h}} \frac{\mu^2(b)}{b} \geqslant \frac{1}{h!}\biggl(\sum_{p \leqslant x} \frac{1}{p}\biggr)^h \biggl[1 - \binom{h}{2}\biggl(\sum_{p \leqslant x} \frac{1}{p}\biggr)^{-2} \sum_p \frac{1}{p^2}\biggr].$$

Again, the sums of $1/p$ are each $\log\log x + O(1)$. The sum of $1/p^2$ is smaller than 0.46, hence for large enough $x$ the bracketed expression is at least 0.08, and the desired lower bound follows. □

Next, we recall (see e.g., [Davenport 2000, Chapter 28]) the well-known theorem of Bombieri and Vinogradov, and then we prove a useful corollary.

**Lemma 2.2.** *For any number $A > 0$ there is a number $B > 0$ so that for $x \geqslant 2$*

$$\sum_{q \leqslant \sqrt{x}(\log x)^{-B}} E^*(x; q) \ll_A \frac{x}{(\log x)^A}.$$

**Corollary 1.** *For any integer $k \geqslant 1$ and number $A > 0$ we have for all $x \geqslant 2$ that*

$$\sum_{q \leqslant x^{1/3}} \tau_k(q) E^*(x; q) \ll_{k,A} \frac{x}{(\log x)^A}.$$

*Proof.* Apply Lemma 2.2 with $A$ replaced by $2A + k^2$, Cauchy's inequality, the trivial bound $|E^*(x; q)| \ll x/q$ and the easy bound

$$\sum_{q \leqslant y} \frac{\tau_k^2(q)}{q} \ll_k (\log y)^{k^2} \tag{2-1}$$

to get

$$\Big(\sum_{q\leqslant x^{1/3}} \tau_k(q)E^*(x;q)\Big)^2 \leqslant \Big(\sum_{q\leqslant x^{1/3}} \tau_k(q)^2|E^*(x;q)|\Big)\Big(\sum_{q\leqslant x^{1/3}} |E^*(x;q)|\Big)$$

$$\ll_{k,A} x\Big(\sum_{q\leqslant x^{1/3}} \frac{\tau_k(q)^2}{q}\Big)\frac{x}{(\log x)^{2A+k^2}}$$

$$\ll_{k,A} \frac{x^2}{(\log x)^{2A}},$$

which leads to the desired conclusion. □

Finally, we need a lower bound from sieve theory.

**Lemma 2.3.** *There are absolute constants $c_1 > 0$ and $c_2 \geqslant 2$ so that for $y \geqslant c_2$, $y^3 \leqslant x$, and any even positive integer $b$, we have*

$$\sum_{\substack{n\in(x,2x]\\ bn+1 \text{ prime}\\ P^-(n)>y}} 1 \geqslant \frac{c_1 bx}{\varphi(b)\log(bx)\log y} - 2\sum_{m\leqslant y^3} 3^{\omega(m)}E^*(2bx;bm).$$

*Proof.* We apply a standard lower bound sieve to the set

$$\mathscr{A} = \Big\{\frac{\ell-1}{b} : \ell \text{ prime},\ \ell\in(bx+1,2bx],\ \ell\equiv 1 \pmod b\Big\}.$$

Letting $\mathscr{A}_d$ be the set of elements of $\mathscr{A}$ divisible by a squarefree integer $d$, we have $|\mathscr{A}_d| = Xg(d)/d + r_d$, where

$$X = \frac{\mathrm{li}(2bx)-\mathrm{li}(bx+1)}{\varphi(b)},\qquad g(d) = \prod_{\substack{p\mid d\\ p\nmid b}} \frac{p}{p-1},\qquad |r_d| \leqslant 2E^*(2bx;db).$$

It follows that for $2\leqslant v<w$,

$$\sum_{v\leqslant p<w} \frac{g(p)}{p}\log p = \log\frac{w}{v} + O(1),$$

the implied constant being absolute. Apply [Halberstam and Richert 1974, Theorem 8.3] with $q=1$, $\xi = y^{3/2}$ and $z=y$, observing that the condition $\Omega_2(1,L)$ on page 142 of that work holds with an absolute constant $L$. With the function $f(u)$ as defined on pages 225–227 there, we have $f(3) = \frac{2}{3}e^{\gamma}\log 2 > \frac{4}{5}$. Then with $B_{19}$ the absolute constant in Theorem 8.3 of that work, we have

$$f(3) - B_{19}\frac{L}{(\log\xi)^{1/14}} \geqslant \frac{1}{2}$$

for large enough $c_2$. We obtain the bound

$$
\begin{aligned}
\#\{x < n \leqslant 2x : bn+1 \text{ prime}, P^-(n) > y\} \\
&\geqslant \frac{X}{2} \prod_{p \leqslant y} \left(1 - \frac{g(p)}{p}\right) - \sum_{m \leqslant \xi^2} 3^{\omega(m)} |r_m| \\
&\geqslant \frac{c_1 bx}{\varphi(b) \log(bx) \log y} - 2 \sum_{m \leqslant y^3} 3^{\omega(m)} E^*(2bx; bm). \quad \square
\end{aligned}
$$

## 3. The set-up

If $n = \lambda(p_1 p_2 \cdots p_k)$, where $p_1, p_2, \ldots, p_k$ are distinct primes, then we have $n = \operatorname{lcm}[p_1 - 1, p_2 - 1, \ldots, p_k - 1]$. If we further assume that $n$ is squarefree and consider the Venn diagram of the sets $S_1, \ldots, S_k$ of the prime factors of $p_1 - 1, \ldots, p_k - 1$, respectively, then this equation gives an ordered factorization of $n$ into $2^k - 1$ factors (some of which may be the trivial factor 1). Here we "see" the shifted primes $p_i - 1$ as products of certain subsequences of $2^{k-1}$ of these factors. Conversely, given $n$ and an ordered factorization of $n$ into $2^k - 1$ factors, we can ask how likely it is for those $k$ products of $2^{k-1}$ factors to all be shifted primes. Of course, this is not likely at all, but if $n$ has many prime factors, and so many factorizations, the odds that there is at least one such "good" factorization improve. For example, when $k = 2$, we factor a squarefree number $n$ as $a_1 a_2 a_3$, and we ask for $a_1 a_2 + 1 = p_1$ and $a_2 a_3 + 1 = p_2$ to both be prime. If so, we would have $n = \lambda(p_1 p_2)$. The heuristic argument from [Luca and Pomerance 2014] was based on this idea. In particular, if a squarefree $n$ is even and has at least $\theta_k \log\log n$ odd prime factors (where $\theta_k > k/\log(2^k - 1)$ is fixed and $\theta_k \to 1/\log 2$ as $k \to \infty$), then there are so many factorizations of $n$ into $2^k - 1$ factors that it becomes likely that $n$ is a $\lambda$-value. The lower bound proof from [Luca and Pomerance 2014] concentrated just on the case $k = 2$, but here we attack the general case. As in that work, we let $r(n)$ be the number of representations of $n$ as the $\lambda$ of a number with $k$ primes. To see that $r(n)$ is often positive, we show that its average value is large, and that the average value of $r(n)^2$ is not much larger. Our conclusion will follow from Cauchy's inequality.

Let $k \geqslant 2$ be a fixed integer, let $x$ be sufficiently large (in terms of $k$), and put

$$
y = \exp\left\{\frac{\log x}{200k \log\log x}\right\}, \qquad l = \left\lfloor \frac{k}{(2^k - 1)\log(2^k - 1)} \log\log y \right\rfloor. \tag{3-1}
$$

For $n \leqslant x$, let $r(n)$ be the number of representations of $n$ of the form

$$
n = \prod_{i=0}^{k-1} a_i \prod_{j=1}^{2^k - 1} b_j, \tag{3-2}
$$

where $P^+(b_j) \leqslant y < P^-(a_i)$ for all $i$ and $j$, where $2 \mid b_{2^k-1}$, where $\omega(b_j) = l$ for each $j$, where $a_i > 1$ for all $i$, and where furthermore $a_i B_i + 1$ is prime for all $i$, where

$$B_i = \prod_{\lfloor j/2^i \rfloor \text{ odd}} b_j. \tag{3-3}$$

Observe that each $B_i$ is even since it is a multiple of $b_{2^k-1}$ (because $\lfloor (2^k-1)/2^i \rfloor = 2^{k-i}-1$ is odd), each $B_i$ is the product of $2^{k-1}$ of the numbers $b_j$, and that every $b_j$ divides $B_0 \cdots B_{k-1}$. Also, if $n$ is squarefree and $r(n) > 0$, then the primes $a_i B_i + 1$ are all distinct, and it follows that

$$n = \lambda\biggl(\prod_{i=0}^{k-1}(a_i B_i + 1)\biggr);$$

therefore such $n \leqslant x$ are counted by $V_\lambda(x)$. We count how often $r(n) > 0$ using Cauchy's inequality in the following standard way:

$$\#\bigl\{2^{-2k}x < n \leqslant x : \mu^2(n) = 1,\ r(n) > 0\bigr\} \geqslant \frac{S_1^2}{S_2}, \tag{3-4}$$

where

$$S_1 = \sum_{2^{-2k}x<n\leqslant x} \mu^2(n) r(n), \qquad S_2 = \sum_{2^{-2k}x<n\leqslant x} \mu^2(n) r^2(n).$$

Our application of Cauchy's inequality is rather sharp, as we will show below that $r(n)$ is approximately 1 on average over the kind of integers we are interested in, both in mean and in mean-square. More precisely, in the next section, we prove

$$S_1 \gg \frac{x}{(\log x)^{\beta_k} (\log\log x)^{O_k(1)}}, \tag{3-5}$$

and in the final section we prove

$$S_2 \ll \frac{x (\log\log x)^{O_k(1)}}{(\log x)^{\beta_k}}, \tag{3-6}$$

where

$$\beta_k = 1 - \frac{k}{\log(2^k-1)}\bigl(1 + \log\log(2^k-1) - \log k\bigr). \tag{3-7}$$

Together, the inequalities (3-4), (3-5) and (3-6) imply that

$$V_\lambda(x) \gg \frac{x}{(\log x)^{\beta_k} (\log\log x)^{O_k(1)}}.$$

We deduce the lower bound of Theorem 1 by noting that $\lim_{k\to\infty} \beta_k = \eta$.

Throughout, constants implied by the symbols $O$, $\ll$, $\gg$, and $\asymp$ may depend on $k$, but not on any other variable.

## 4. The lower bound for $S_1$

For convenience, when using the sieve bound in Lemma 2.3, we consider a slightly larger sum $S_1'$ than $S_1$, namely

$$S_1' := \sum_{n\in\mathcal{N}} r(n),$$

where $\mathcal{N}$ is the set of $n \in (2^{-2k}x, x]$ of the form $n = n_0 n_1$ with $P^+(n_0) \leqslant y < P^-(n_1)$ and $n_0$ squarefree. That is, in $S_1'$ we no longer require the numbers $a_0, \dots, a_{k-1}$ in (3-2) to be squarefree. The difference between $S_1$ and $S_1'$ is very small; indeed, putting $h = 2^k + k - 1$, note that $r(n) \leqslant \tau_h(n)$, so that we have by (3-2) the estimate

$$\begin{aligned} S_1' - S_1 &\leqslant \sum_{\substack{n\leqslant x\\ \exists p>y: p^2\mid n}} \tau_h(n) \leqslant \sum_{p>y} \sum_{\substack{n\leqslant x\\ p^2\mid n}} \tau_h(n) \leqslant \sum_{p>y} \tau_h(p^2) \sum_{m\leqslant x/p^2} \tau_h(m) \\ &\leqslant \sum_{p>y} \tau_h(p^2) \frac{x}{p^2} \sum_{m\leqslant x} \frac{\tau_h(m)}{m} \ll \frac{x(\log x)^h}{y}. \end{aligned} \tag{4-1}$$

Here we have used the inequality $\tau_h(uv) \leqslant \tau_h(u)\tau_h(v)$, as well as the easy bound

$$\sum_{m\leqslant x} \frac{\tau_h(m)}{m} \ll (\log x)^h, \tag{4-2}$$

which is similar to (2-1). By (3-2), the sum $S_1'$ counts the number of $(2^{k-1}+k)$-tuples $(a_0, \dots, a_{k-1}, b_1, \dots, b_{2^k-1})$ satisfying

$$2^{-2k}x < a_0 \cdots a_{k-1} b_1 \cdots b_{2^k-1} \leqslant x \tag{4-3}$$

and with $P^+(b_j) \leqslant y < P^+(a_i)$ for every $i$ and $j$, $b_1 \cdots b_{2^k-1}$ squarefree, $2 \mid b_{2^k-1}$, $\omega(b_j) = l$ for every $j$, $a_i > 1$ for every $i$, and $a_i B_i + 1$ prime for every $i$, where $B_i$ is defined in (3-3). Fix numbers $b_1, \dots, b_{2^k-1}$. Then

$$b_1 \cdots b_{2^k-1} \leqslant y^{(2^k-1)l} \leqslant y^{2\log\log x} = x^{1/100k}. \tag{4-4}$$

In the above, we used the fact that $k \leqslant 2\log(2^k - 1)$. Fix also $A_0, \dots, A_{k-1}$, each a power of 2 exceeding $x^{1/2k}$, such that

$$\frac{x}{2b_1 \cdots b_{2^k-1}} < A_0 \cdots A_{k-1} \leqslant \frac{x}{b_1 \cdots b_{2^k-1}}. \tag{4-5}$$

Then (4-3) holds whenever $A_i/2 < a_i \leqslant A_i$ for each $i$. By Lemma 2.3, using the facts that $B_i/\varphi(B_i) \geqslant 2$ (because $B_i$ is even) and $A_i B_i \leqslant x$ (a consequence of (4-5)), we deduce that the number of choices for each $a_i$ is at least

$$\frac{c_1 A_i}{\log x \log y} - 2 \sum_{m \leqslant y^3} 3^{\omega(m)} E^*(A_i B_i; m B_i).$$

Using the elementary inequality

$$\prod_{j=1}^{k} \max(0, x_j - y_j) \geqslant \prod_{j=1}^{k} x_j - \sum_{i=1}^{k} y_i \prod_{j \neq i} x_j,$$

valid for any nonnegative real numbers $x_j$, $y_j$, we find that the number of admissible $k$-tuples $(a_0, \dots, a_{k-1})$ is at least

$$\frac{c_1^k A_0 \cdots A_{k-1}}{(\log x \log y)^k} - \frac{2 c_1^{k-1} A_0 \cdots A_{k-1}}{(\log x \log y)^{k-1}} \sum_{i=0}^{k-1} \frac{1}{A_i} \sum_{m \leqslant y^3} 3^{\omega(m)} E^*(A_i B_i; m B_i) \\ = M(\boldsymbol{A}, \boldsymbol{b}) - R(\boldsymbol{A}, \boldsymbol{b}),$$

say. By symmetry and (4-5),

$$\sum_{\boldsymbol{A}, \boldsymbol{b}} R(\boldsymbol{A}, \boldsymbol{b}) \\ \ll \frac{x}{(\log x \log y)^{k-1}} \sum_{\boldsymbol{b}} \frac{1}{b_1 \cdots b_{2^k - 1}} \sum_{\boldsymbol{A}} \frac{1}{A_0} \sum_{m \leqslant y^3} 3^{\omega(m)} E^*(A_0 B_0; m B_0), \quad (4\text{-}6)$$

where the sum on $\boldsymbol{b}$ is over all $(2^k - 1)$−tuples satisfying $b_1 \cdots b_{2^k - 1} \leqslant x^{1/100k}$. Write $b_1 \cdots b_{2^k - 1} = B_0 B_0'$, where $B_0' = b_2 b_4 \cdots b_{2^k - 2}$. Given $B_0$ and $B_0'$, the number of corresponding tuples $(b_1, \dots, b_{2^k - 1})$ is at most $\tau_{2^{k-1}}(B_0) \tau_{2^{k-1}-1}(B_0')$. Suppose $D/2 < B_0 \leqslant D$, where $D$ is a power of 2. Since $E^*(x; q)$ is an increasing function of $x$, $E^*(A_0 B_0; m B_0) \leqslant E^*(A_0 D; m B_0)$. Also, $3^{\omega(m)} \leqslant \tau_3(m)$ and

$$\sum_{B_0' \leqslant x} \frac{\tau_{2^{k-1}-1}(B_0')}{B_0'} \ll (\log x)^{2^{k-1}-1}$$

(this is (4-2) with $h$ replaced by $2^{k-1} - 1$). We therefore deduce that

$$\sum_{\boldsymbol{A}, \boldsymbol{b}} R(\boldsymbol{A}, \boldsymbol{b}) \\ \ll \frac{x (\log x)^{2^{k-1}-1}}{(\log x \log y)^{k-1}} \sum_{\boldsymbol{A}} \frac{1}{A_0} \sum_{D} \frac{1}{D} \sum_{\substack{D/2 < B_0 \leqslant D \\ m \leqslant y^3}} \tau_3(m) \tau_{2^{k-1}}(B_0) E^*(A_0 D; m B_0),$$

with the sum taken over $(A_0, \dots, A_{k-1}, D)$, each a power of 2, $D \leqslant x^{1/100k}$, $A_i \geqslant x^{1/2k}$ for each $i$ and $A_0 \cdots A_{k-1} D \leqslant x$. With $A_0$ and $D$ fixed, the number of choices for $(A_1, \dots, A_{k-1})$ is $\ll (\log x)^{k-1}$. Writing $q = mB_0$, we obtain

$$\begin{aligned}\sum_{A,b} R(A, b) \\ &\ll x\frac{(\log x)^{2^{k-1}-1}}{(\log y)^{k-1}} \sum_{D\leqslant x^{1/100k}} \sum_{x^{1/2k}<A_0\leqslant x/D} \frac{1}{A_0 D} \sum_{q\leqslant y^3 x^{1/100k}} \tau_{2^{k-1}+3}(q) E^*(A_0 D; q) \\ &\ll \frac{x}{(\log x)^{\beta_k+1}},\end{aligned}$$

where we used Corollary 1 in the last step, with $A = 2^{k-1} - k + 4 + \beta_k$.

For the main term, by (4-5), given any $b_1, \dots, b_{2^{k-1}}$, the product $A_0 \cdots A_{k-1}$ is determined (and larger than $\frac{1}{2}x^{1-1/100k}$ by (4-4)), so there are $\gg (\log x)^{k-1}$ choices for the $k$-tuple $A_0, \dots, A_{k-1}$. Hence,

$$\sum_{A,b} M(A, b) \gg \frac{x}{(\log y)^k \log x} \sum_{b} \frac{1}{b_1 \cdots b_{2^k-1}}.$$

Let $b = b_1 \cdots b_{2^k-1}$. Given an even, squarefree integer $b$, the number of ordered factorizations of $b$ as $b = b_1 \cdots b_{2^k-1}$, where each $\omega(b_i) = l$ and $b_{2^k-1}$ is even, is equal to

$$\frac{((2^k-1)l)!}{(2^k-1)(l!)^{2^k-1}}.$$

Let $b' = b/2$, so $h := \omega(b') = (2^k-1)l - 1 = k(\log\log y)/\log(2^k-1) + O(1)$. Applying Lemma 2.1, Stirling's formula and the fact that $(2^k-1)l = h + O(1)$ produces

$$\begin{aligned}\sum_{b} \frac{1}{b_1 \cdots b_{2^k-1}} &\geqslant \frac{((2^k-1)l)!}{2(2^k-1)(l!)^{2^k-1}} \sum_{\substack{P^+(b')\leqslant y \\ \omega(b')=h}} \frac{\mu^2(b')}{b'} \\ &\gg \frac{((2^k-1)l)!}{(l!)^{2^k-1}} \frac{(\log\log y)^h}{h!} = \frac{(\log\log y)^h}{(l!)^{2^k-1}} (\log\log x)^{O(1)} \\ &= \left[\frac{(2^k-1)e\log(2^k-1)}{k}\right]^{(2^k-1)l} (\log\log x)^{O(1)} \\ &= (\log y)^{\frac{k}{\log(2^k-1)}\log\left[\frac{(2^k-1)e\log(2^k-1)}{k}\right]} (\log\log x)^{O(1)} \\ &= (\log y)^{k-\beta_k+1} (\log\log x)^{O(1)}.\end{aligned}$$

Invoking (3-1), we obtain that

$$\sum_{A,b} M(A, b) \geqslant \frac{x}{(\log x)^{\beta_k} (\log\log x)^{O(1)}}. \tag{4-7}$$

Inequality (3-5) now follows from estimate (4-7) and our earlier estimates (4-1) of $S_1' - S_1$ and (4-6) of $\sum_{A,b} R(A, b)$.

## 5. A multivariable sieve upper bound

Here we prove an estimate from sieve theory that will be useful in our treatment of the upper bound for $S_2$.

**Lemma 5.1.** *Suppose that*:

- $y, x_1, \ldots, x_h$ *are reals with* $3 < y \leqslant 2\min\{x_1, \ldots, x_h\}$.
- $I_1, \ldots, I_k$ *are nonempty subsets of* $\{1, \ldots, h\}$.
- $b_1, \ldots, b_k$ *are positive integers such that if* $I_i = I_j$, *then* $b_i \neq b_j$.

*For* $\boldsymbol{n} = (n_1, \ldots, n_h)$ *a vector of positive integers and for* $1 \leqslant j \leqslant k$, *let* $N_j = N_j(\boldsymbol{n}) = \prod_{i \in I_j} n_i$. *Then*

$$\#\bigl\{\boldsymbol{n} : x_i < n_i \leqslant 2x_i \ (1 \leqslant i \leqslant h),\ P^-(n_1 \cdots n_h) > y,\ b_j N_j + 1 \text{ prime } (1 \leqslant j \leqslant k)\bigr\} \ll_{h,k} \frac{x_1 \cdots x_h}{(\log y)^{h+k}} (\log\log(3b_1 \cdots b_k))^k.$$

*Proof.* Throughout this proof, all Vinogradov symbols $\ll$ and $\gg$ as well as the Landau symbol $O$ depend on both $h$ and $k$. Without loss of generality, suppose that $y \leqslant (\min(x_i))^{1/(h+k+10)}$. Since $n_i > x_i \geqslant y^{h+k+10}$ for every $i$, we see that the number of $h$-tuples in question does not exceed

$$S := \#\{\boldsymbol{n} : x_i < n_i \leqslant 2x_i \ (1 \leqslant i \leqslant h),\ P^-(n_1 \cdots n_h(b_1N_1 + 1) \cdots (b_kN_k + 1)) > y\}.$$

We estimate $S$ in the usual way with sieve methods, although this is a bit more general than the standard applications and we give the proof in some detail (the case $h = 1$ being completely standard). Let $\mathscr{A}$ denote the multiset

$$\mathscr{A} = \left\{ n_1 \cdots n_h \prod_{j=1}^{k} (b_j N_j + 1) \ :\ x_j < n_j \leqslant 2x_j \ (1 \leqslant j \leqslant h) \right\}.$$

For squarefree $d \leqslant y^2$ composed of primes $\leqslant y$, we have by a simple counting argument

$$|\mathscr{A}_d| := \#\{a \in \mathscr{A} : d \mid a\} = \frac{\nu(d)}{d^h} X + r_d,$$

where $X = x_1 \cdots x_h$, $\nu(d)$ is the number of solution vectors $\boldsymbol{n}$ modulo $d$ of the congruence

$$n_1 \cdots n_h \prod_{j=1}^{k} (b_j N_j + 1) \equiv 0 \pmod{d},$$

and the remainder term satisfies, for $d \leqslant \min(x_1, \dots, x_h)$,

$$|r_d| \leqslant \nu(d) \sum_{i=1}^{h} \prod_{\substack{1 \leqslant l \leqslant h \\ l \neq i}} \left( \left\lfloor \frac{x_l}{d} \right\rfloor + 1 \right) \leqslant \nu(d) \sum_{i=1}^{h} \frac{(x_1+d)\cdots(x_h+d)}{(x_i+d)d^{h-1}}$$
$$\ll \frac{\nu(d)X}{d^{h-1}\min(x_i)}.$$

The function $\nu(d)$ is clearly multiplicative and satisfies the global upper bound $\nu(p) \leqslant (h+k)p^{h-1}$ for every $p$. If $\nu(p) = p^h$ for some $p \leqslant y$, then clearly $S=0$. Otherwise, the hypotheses of [Halberstam and Richert 1974, Theorem 6.2] (Selberg's sieve) are clearly satisfied, with $\kappa = h+k$, and we deduce that

$$S \ll X \prod_{p \leqslant y} \left(1 - \frac{\nu(p)}{p^h}\right) + \sum_{\substack{d \leqslant y^2 \\ P^+(d) \leqslant y}} \mu^2(d) 3^{\omega(d)} |r_d|.$$

By our initial assumption about the size of $y$,

$$\sum_{d \leqslant y^2} \mu^2(d) 3^{\omega(d)} |r_d| \ll \frac{X}{\min(x_i)} \sum_{d \leqslant y^2} (3k+3h)^{\omega(d)} \ll \frac{Xy^3}{\min(x_i)} \ll \frac{X}{y}.$$

For the main term, consideration only of the congruence $n_1 \cdots n_h \equiv 0 \pmod p$ shows that

$$\nu(p) \geqslant h(p-1)^{h-1} = hp^{h-1} + O(p^{h-2})$$

for all $p$. On the other hand, suppose that $p \nmid b_1 \cdots b_k$ and furthermore that $p \nmid (b_i - b_j)$ whenever $I_i = I_j$. Each congruence $b_j N_j + 1 \equiv 0 \pmod p$ has $p^{h-1} + O(p^{h-2})$ solutions with $n_1 \dots n_h \not\equiv 0 \pmod p$, and any two of these congruences have $O(p^{h-2})$ common solutions. Hence, $\nu(p) = (h+k)p^{h-1} + O(p^{h-2})$. In particular,

$$\frac{h}{p} + O\left(\frac{1}{p^2}\right) \leqslant \frac{\nu(p)}{p^h} \leqslant \frac{h+k}{p} + O\left(\frac{1}{p^2}\right). \tag{5-1}$$

Further, writing $E = b_1 \cdots b_k \prod_{i \neq j} |b_i - b_j|$, the upper bound (5-1) above is in fact an equality except when $p \mid E$. We obtain

$$\prod_{p \leqslant y} \left(1 - \frac{\nu(p)}{p^h}\right) \ll \prod_{p \leqslant y} \left(1 - \frac{1}{p}\right)^{k+h} \prod_{p \mid E} \left(1 - \frac{1}{p}\right)^{-k} \ll \frac{(E/\varphi(E))^k}{(\log y)^{h+k}} \ll \frac{(\log\log 3E)^k}{(\log y)^{h+k}}$$

and the desired bound follows. □

## 6. The upper bound for $S_2$

Here, $S_2$ is the number of solutions of

$$n = \prod_{i=0}^{k-1} a_i \prod_{j=1}^{2^k-1} b_j = \prod_{i=0}^{k-1} a_i' \prod_{j=1}^{2^k-1} b_j', \tag{6-1}$$

with $2^{-2k}x < n \leqslant x$, $n$ squarefree,

$$P^+(b_1 b_1' \cdots b_{2^k-1} b_{2^k-1}') \leqslant y < P^-(a_0 a_0' \cdots a_{k-1} a_{k-1}'),$$

$\omega(b_j) = \omega(b_j') = l$ for every $j$, $a_i > 1$ for every $i$, $2 \mid b_{2^k-1}$, $2 \mid b_{2^k-1}'$, and $a_i B_i + 1$ and $a_i' B_i' + 1$ prime for $0 \leqslant i \leqslant k-1$, where $B_i'$ is defined analogously to $B_i$ (see (3-3)). Trivially, we have

$$a := \prod_{i=0}^{k-1} a_i = \prod_{i=0}^{k-1} a_i', \qquad b := \prod_{j=1}^{2^k-1} b_j = \prod_{j=1}^{2^k-1} b_j'. \tag{6-2}$$

We partition the solutions of (6-1) according to the number of the primes $a_i B_i + 1$ that are equal to one of the primes $a_j' B_j' + 1$, a number which we denote by $m$. By symmetry (that is, by appropriate permutation of the vectors $(a_0, \ldots, a_{k-1})$, $(a_0', \ldots, a_{k-1})$, $(b_1, \ldots, b_{2^k-1})$ and $(b_1', \ldots, b_{2^k-1}')$[1]), without loss of generality we may suppose that $a_i B_i = a_i' B_i'$ for $0 \leqslant i \leqslant m-1$ and that

$$a_i B_i \neq a_j B_j \quad (i \geqslant m,\ j \geqslant m). \tag{6-3}$$

Consequently,

$$a_i = a_i' \quad \text{and} \quad B_i = B_i' \quad (0 \leqslant i \leqslant m-1). \tag{6-4}$$

Now fix $m$ and all the $b_j$ and $b_j'$. For $0 \leqslant i \leqslant m-1$, place $a_i$ into a dyadic interval $(A_i/2, A_i]$, where $A_i$ is a power of 2. The primality conditions on the remaining variables are now coupled with the condition

$$a_m \cdots a_{k-1} = a_m' \cdots a_{k-1}'.$$

[1]The permutations may be described explicitly. Suppose that $m \leqslant k-1$ and that we wish to permute $(b_1, \ldots, b_{2^k-1})$ such that $B_{i_1}, \ldots, B_{i_m}$ become $B_0, \ldots, B_{m-1}$, respectively. Let $S_i = \{1 \leqslant j \leqslant 2^k - 1 : \lfloor j/2^i \rfloor \text{ odd}\}$. The Venn diagram for the sets $S_{i_1}, \ldots, S_{i_m}$ has $2^m - 1$ components of size $2^{k-m-1}$ and one component of size $2^{k-m-1} - 1$, and we map the variables $b_j$ with $j$ in a given component to the variables whose indices are in the corresponding component of the Venn diagram for $S_0, \ldots, S_{m-1}$.

To aid the bookkeeping, let $\alpha_{i,j} = \gcd(a_i, a'_j)$ for $m \leqslant i, j \leqslant k-1$. Then

$$a_i = \prod_{j=m}^{k-1} \alpha_{i,j}, \qquad a'_j = \prod_{i=m}^{k-1} \alpha_{i,j}. \tag{6-5}$$

As each $a_i > 1, a'_j > 1$, each product above contains at least one factor that is greater than 1. Let $I$ denote the set of pairs of indices $(i, j)$ such that $\alpha_{i,j} > 1$, and fix $I$. For $(i, j) \in I$, place $\alpha_{i,j}$ into a dyadic interval $(A_{i,j}/2, A_{i,j}]$, where $A_{i,j}$ is a power of 2 and $A_{i,j} \geqslant y$. By the assumption on the range of $n$, we have

$$A_0 \cdots A_{m-1} \prod_{(i,j)\in I} A_{i,j} \asymp \frac{x}{b}. \tag{6-6}$$

For $0 \leqslant i \leqslant m-1$, we use Lemma 5.1 (with $h = 1$) to deduce that the number of $a_i$ with $A_i/2 < a_i \leqslant A_i$, $P^-(a_i) > y$ and $a_i B_i + 1$ prime is

$$\ll \frac{A_i \log\log B_i}{\log^2 y} \ll \frac{A_i (\log\log x)^3}{\log^2 x}. \tag{6-7}$$

Counting the vectors $(\alpha_{i,j})_{(i,j)\in I}$ subject to the conditions

- $A_{i,j}/2 < \alpha_{i,j} \leqslant A_{i,j}$ and $P^-(\alpha_{i,j}) > y$ for $(i, j) \in I$;
- $a_i B_i + 1$ prime $(m \leqslant i \leqslant k-1)$;
- $a'_j B'_j + 1$ prime $(m \leqslant j \leqslant k-1)$;
- condition (6-5)

is also accomplished with Lemma 5.1, this time with $h = |I|$ and with $2(k-m)$ primality conditions. The hypothesis in the lemma concerning identical sets $I_i$, which may occur if $\alpha_{i,j} = a_i = a'_j$ for some $i$ and $j$, is satisfied by our assumption (6-3), which implies in this case that $B_i \neq B'_j$. The number of such vectors is at most

$$\ll \frac{\prod_{(i,j)\in I} A_{i,j} (\log\log x)^{2k-2m}}{(\log y)^{|I|+2k-2m}} \ll \frac{\prod_{(i,j)\in I} A_{i,j} (\log\log x)^{|I|+4k-4m}}{(\log x)^{|I|+2k-2m}}. \tag{6-8}$$

Combining the bounds (6-7) and (6-8), and recalling (6-6), we see that the number of possibilities for the $2k$-tuple $(a_0, \dots, a_{k-1}, a'_0 \dots, a'_{k-1})$ is at most

$$\ll \frac{x (\log\log x)^{O(1)}}{b (\log x)^{|I|+2k}}.$$

With $I$ fixed, there are $O((\log x)^{|I|+m-1})$ choices for $A_0, \dots, A_{m-1}$ and $A_{i,j}$ subject to (6-6), and there are $O(1)$ possibilities for $I$. We infer that with $m$ and all of the

$b_j, b'_j$ fixed, the number of possible $(a_0, \dots, a_{k-1}, a'_0 \dots, a'_{k-1})$ is at most

$$\ll \frac{x(\log\log x)^{O(1)}}{b(\log x)^{2k+1-m}}.$$

We next prove that the identities in (6-4) imply that

$$B_{\boldsymbol{v}} = B'_{\boldsymbol{v}} \quad (\boldsymbol{v} \in \{0,1\}^m), \tag{6-9}$$

where $B_{\boldsymbol{v}}$ is the product of all $b_j$ where the $m$ least significant base-2 digits of $j$ are given by the vector $\boldsymbol{v}$, and $B'_{\boldsymbol{v}}$ is defined analogously. Fix $\boldsymbol{v} = (v_0, \dots, v_{m-1})$. For $0 \leqslant i \leqslant m-1$, let $C_i = B_i$ if $v_i = 1$ and $C_i = b/B_i$ if $v_i = 0$, and define $C'_i$ analogously. By (3-3), each number $b_j$ where the last $m$ base-2 digits of $j$ are equal to $\boldsymbol{v}$ divides every $C_i$, and no other $b_j$ has this property. By (6-4), $C_i = C'_i$ for each $i$ and thus

$$C_0 \cdots C_{m-1} = C'_0 \cdots C'_{m-1}.$$

As the numbers $b_j$ are pairwise coprime, in the above equality the primes having exponent $m$ on the left are exactly those dividing $B_{\boldsymbol{v}}$, and similarly the primes on the right side having exponent $m$ are exactly those dividing $B'_{\boldsymbol{v}}$. This proves (6-9).

Say $b$ is squarefree. We count the number of dual factorizations of $b$ compatible with both (6-2) and (6-9). Each prime dividing $b$ first "chooses" which $B_{\boldsymbol{v}} = B'_{\boldsymbol{v}}$ to divide. Once this choice is made, there is the choice of which $b_j$ to divide and also which $b'_j$. For the $2^m - 1$ vectors $\boldsymbol{v} \neq \boldsymbol{0}$, $B_{\boldsymbol{v}} = B'_{\boldsymbol{v}}$ is the product of $2^{k-m}$ numbers $b_j$ and also the product of $2^{k-m}$ numbers $b'_j$. Similarly, $B_{\boldsymbol{0}}$ is the product of $2^{k-m} - 1$ numbers $b_j$ and $2^{k-m} - 1$ numbers $b'_j$. Thus, ignoring that $\omega(b_j) = \omega(b'_j) = l$ for each $j$ and that $b_{2^k-1}$ and $b'_{2^k-1}$ are even, the number of dual factorizations of $b$ is at most

$$\big((2^m - 1)(2^{k-m})^2 + (2^{k-m} - 1)^2\big)^{\omega(b)} = (2^{2k-m} - 2^{k+1-m} + 1)^{\omega(b)}. \tag{6-10}$$

Again, let

$$h = \omega(b) = (2^k - 1)l = \frac{k}{\log(2^k - 1)} \log\log y + O(1),$$

as in Section 4. Lemma 2.1 and Stirling's formula give

$$\sum_{\substack{P^+(b) \leqslant y \\ \omega(b) = h}} \frac{\mu^2(b)}{b} \ll \frac{(\log\log y)^h}{h!} \ll (e \log(2^k - 1)/k)^h.$$

Combined with our earlier bound (6-10) for the number of admissible ways to dual factor each $b$, we obtain

$$S_2 \ll \frac{x(\log\log x)^{O(1)}}{\log x}(e\log(2^k-1)/k)^h \times \sum_{m=0}^{k} (\log y)^{m-2k+\frac{k}{\log(2^k-1)}\log(2^{2k-m}-2^{k+1-m}+1)}. \quad (6\text{-}11)$$

For real $t \in [0,k]$, let $f(t) = k\log(2^{2k-t}-2^{k+1-t}+1) - (2k-t)\log(2^k-1)$. We have $f(0) = f(k) = 0$ and

$$f''(t) = \frac{k(\log 2)^2(2^{2k}-2^{k+1})2^{-t}}{(2^{2k-t}-2^{k+1-t}+1)^2} > 0.$$

Hence, $f(t) < 0$ for $0 < t < k$. Thus, the sum on $m$ in (6-11) is $O(1)$, and (3-6) follows.

Theorem 1 is therefore proved.

## Acknowledgements

Part of this work was done while Ford and Luca visited Dartmouth College in Spring 2013. They thank the people there for their hospitality. Pomerance gratefully acknowledges a helpful conversation with Andrew Granville in which the heuristic argument behind our proof first arose. The authors also thank one of the referees for constructive comments which improved the paper.

## References

[Banks and Luca 2011] W. D. Banks and F. Luca, "Power totients with almost primes", *Integers* **11**:3 (2011), 307–313. MR 2988064 Zbl 1268.11141

[Banks et al. 2004] W. D. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, "Multiplicative structure of values of the Euler function", pp. 29–47 in *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, edited by A. van der Poorten and A. Stein, Fields Inst. Commun. **41**, Amer. Math. Soc., Providence, RI, 2004. MR 2005f:11217 Zbl 1099.11055

[Davenport 2000] H. Davenport, *Multiplicative number theory*, 3rd ed., Graduate Texts in Mathematics **74**, Springer, New York, 2000. MR 2001f:11001 Zbl 1002.11001

[Erdős 1935] P. Erdős, "On the normal number of prime factors of $p-1$ and some related problems concerning Euler's $\varphi$-function", *Q. J. Math., Oxf. Ser.* **6** (1935), 205–213. Zbl 0012.14905

[Erdős 1960] P. Erdős, "Об одном асимптотическом неравенстве в теории чисел (An asymptotic inequality in number theory)", *Vestnik Leningrad. Univ.* **15**:13 (1960), 41–49. MR 23 #A3720 Zbl 0104.26804

[Erdős et al. 1991] P. Erdős, C. Pomerance, and E. Schmutz, "Carmichael's lambda function", *Acta Arith.* **58**:4 (1991), 363–385. MR 92g:11093 Zbl 0734.11047

[Ford 1998] K. Ford, "The distribution of totients", *Ramanujan J.* **2**:1-2 (1998), 67–151. Updated version on the author's web page. MR 99m:11106 Zbl 0914.11053

[Ford 2008a] K. Ford, "The distribution of integers with a divisor in a given interval", *Ann. of Math.* (2) **168**:2 (2008), 367–433. MR 2009m:11152 Zbl 1181.11058

[Ford 2008b] K. Ford, "Integers with a divisor in $(y, 2y]$", pp. 65–80 in *Anatomy of integers*, edited by J.-M. De Koninck et al., CRM Proc. Lecture Notes **46**, Amer. Math. Soc., Providence, RI, 2008. MR 2009i:11113 Zbl 1175.11053

[Ford et al. 2010] K. Ford, F. Luca, and C. Pomerance, "Common values of the arithmetic functions $\phi$ and $\sigma$", *Bull. Lond. Math. Soc.* **42**:3 (2010), 478–488. MR 2011m:11191 Zbl 1205.11010

[Freiberg 2012] T. Freiberg, "Products of shifted primes simultaneously taking perfect power values", *J. Aust. Math. Soc.* **92**:2 (2012), 145–154. MR 2999152 Zbl 06124076

[Friedlander and Luca 2007] J. B. Friedlander and F. Luca, "On the value set of the Carmichael $\lambda$-function", *J. Aust. Math. Soc.* **82**:1 (2007), 123–131. MR 2008c:11124 Zbl 1146.11046

[Halberstam and Richert 1974] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs **4**, Academic Press, London, New York, 1974. MR 54 #12689 Zbl 0298.10026

[Luca and Pomerance 2014] F. Luca and C. Pomerance, "On the range of Carmichael's universal-exponent function", *Acta Arith.* **162**:3 (2014), 289–308. MR 3173026 Zbl 1292.11109

[Miller 1976] G. L. Miller, "Riemann's hypothesis and tests for primality", *J. Comput. System Sci.* **13**:3 (1976), 300–317. MR 58 #470a Zbl 0349.68025

[Pillai 1929] S. S. Pillai, "On some functions connected with $\phi(n)$", *Bull. Amer. Math. Soc.* **35**:6 (1929), 832–836. MR 1561819 Zbl 55.0710.02

[Pollack and Pomerance 2014] P. Pollack and C. Pomerance, "Square values of Euler's function", *Bull. Lond. Math. Soc.* **46**:2 (2014), 403–414. MR 3194758 Zbl 1297.11125

[Schoenberg 1928] I. Schoenberg, "Über die asymptotische Verteilung reeller Zahlen mod 1", *Math. Z.* **28**:1 (1928), 171–199. MR 1544950 Zbl 54.0212.02

Communicated by Andrew Granville
Received 2014-06-23 Revised 2014-09-04 Accepted 2014-10-09

ford@math.uiuc.edu — *Department of Mathematics, University of Illinois at Urbana–Champaign, 1409 West Green Street, Urbana, IL 61801, United States*

florian.luca@wits.ac.za — *School of Mathematics, University of the Witwatersrand, P.O. Box Wits 2050, Johannesburg, South Africa*

*Instituto de Matématicas, UNAM Juriquilla, Santiago de Querétaro, 76230, Querétaro de Arteaga, México*

carl.pomerance@dartmouth.edu — *Mathematics Department, Dartmouth College, Kemeny Hall, Hanover, NH 03755, United States*

# Algebra & Number Theory

msp.org/ant





See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2014 is US $225/year for the electronic version, and $400/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

**mathematical sciences publishers**

**nonprofit scientific publishing**

http://msp.org/

# Algebra & Number Theory

Volume 8 No. 8 2014





1937-0652(2014)8:8;1-3