

Arithmetic properties of [Formel] and the structure of the multiplicative group modulo n

Autor(en): **Banks, William / Luca, Florian / Shparlinski, Igor E.**

Objektyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **81 (2006)**

PDF erstellt am: **11.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-1149>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Arithmetic properties of $\varphi(n)/\lambda(n)$ and the structure of the multiplicative group modulo n

William D. Banks, Florian Luca and Igor E. Shparlinski

Abstract. For a positive integer n , we let $\varphi(n)$ and $\lambda(n)$ denote the Euler function and the Carmichael function, respectively. We define $\xi(n)$ as the ratio $\varphi(n)/\lambda(n)$ and study various arithmetic properties of $\xi(n)$.

Mathematics Subject Classification (2000). 11A25.

Keywords. Euler function, Carmichael function.

1. Introduction and notation

Let $\varphi(n)$ denote the *Euler function*, which is defined as usual by

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \prod_{p^v \parallel n} p^{v-1}(p-1), \quad n \geq 1.$$

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

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

and for an arbitrary integer $n \geq 2$,

$$\lambda(n) = \text{lcm}(\lambda(p_1^{v_1}), \dots, \lambda(p_k^{v_k})),$$

where $n = p_1^{v_1} \dots p_k^{v_k}$ is the prime factorization of n . Clearly, $\lambda(1) = 1$.

Despite their many similarities, the functions $\varphi(n)$ and $\lambda(n)$ often exhibit remarkable differences in their arithmetic behavior, and a vast number of results about the growth rate and various arithmetical properties of $\varphi(n)$ and $\lambda(n)$ have been obtained; see for example [4], [5], [7], [8], [9], [11], [15]. In this paper, we consider the

arithmetical function defined by

$$\xi(n) = \frac{\varphi(n)}{\lambda(n)}, \quad n \geq 1,$$

and we study some of its arithmetic properties.

In particular, letting $P(k)$ denote the largest prime factor of a positive integer k (with the convention that $P(1) = 1$), we study the behavior of $P(\xi(n))$. Our results imply that typically $\xi(n)$ is much “smoother” than a random integer k of the same size. To make this comparison, it is useful to recall that Theorem 2 of [9] implies that the estimate

$$\xi(n) = \exp(\log_2 n \log_3 n + C \log_2 n + o(\log_2 n)) \quad (1)$$

holds on a set of positive integers n of asymptotic density 1 with some absolute constant $C > 0$. Here, and in the sequel, for a real number $z > 0$ and a natural number ℓ , we write $\log_\ell z$ for the recursively defined function given by $\log_1 z = \max\{\log z, 1\}$, where $\log z$ denotes the natural logarithm of z , and $\log_\ell z = \max\{\log(\log_{\ell-1} z), 1\}$ for $\ell > 1$. When $\ell = 1$, we omit the subscript (however, we still assume that all the logarithms that appear below are at least 1). Of course, when z is sufficiently large, then $\log_\ell z$ is nothing more than the ℓ -fold composition of the natural logarithm evaluated at z .

We also use $\Omega(n)$ and $\omega(n)$ with their usual meanings: $\Omega(n)$ denotes the total number of prime divisors of $n > 1$ counted with multiplicity, while $\omega(n)$ is the number of distinct prime factors of $n > 1$; as usual, we put $\Omega(1) = \omega(1) = 0$. In this paper, we also study the functions $\Omega(\xi(n))$ and $\omega(\xi(n))$.

Observe that a prime p divides $\xi(n)$ if and only if the p -Sylow subgroup of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is not cyclic. Thus, $P(\xi(n))$ and $\omega(\xi(n))$ can be viewed as measures of “non-cyclicity” of this group. In particular, $\omega(\xi(n))$ is the number of non-cyclic Sylow subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$.

We also remark that any prime $p \mid \xi(n)$ has that property that $p^2 \mid \varphi(n)$. Thus, while studying the prime factors of $\xi(n)$, one is naturally lead to an associated question concerning the difference $\Omega(\varphi(n)) - \omega(\varphi(n))$, a question that we address here as well.

As usual, for a large number x , $\pi(x)$ denotes the number of primes $p \leq x$, and for positive integers a, k with $\gcd(a, k) = 1$, $\pi(x; k, a)$ denotes the number of primes $p \leq x$ with $p \equiv a \pmod{k}$.

We use the Vinogradov symbols \gg, \ll, \asymp as well as the Landau symbols O and o with their usual meanings. The implied constants in the symbols O, \gg, \ll and \asymp are always absolute unless indicated otherwise.

Finally, we say that a certain property holds for “almost all” n if it holds for all $n \leq x$ with at most $o(x)$ exceptions, as $x \rightarrow \infty$.

Acknowledgements. The authors wish to thank Carl Pomerance for suggesting the statement of Theorem 9 and for some useful references. During the preparation of this paper, W. B. was supported in part by NSF grant DMS-0070628, F. L. was supported in part by grants SEP-CONACYT 37259-E and 37260-E, and I. S. was supported in part by ARC grant DP0211459.

2. Distribution of $P(\xi(n))$, $\omega(\xi(n))$ and $\Omega(\xi(n))$

In what follows, let us call a real-valued function $\varepsilon(x)$ *admissible* if

- $\varepsilon(x)$ is a decreasing function, with limit 0 as $x \rightarrow \infty$;
- $\varepsilon(x) \log_2 x$ is an increasing function, tending to ∞ as $x \rightarrow \infty$.

We begin with the following statement, which may be of independent interest.

Lemma 1. *For any admissible function $\varepsilon(x)$ and any prime $q \leq \varepsilon(x) \log_2 x$, every positive integer $n \leq x$ has at least $(\log_2 n)/2q$ distinct prime factors $p \equiv 1 \pmod{q}$, with at most $o(x)$ exceptions.*

Proof. Let $\omega(n, q)$ denote the number of distinct prime factors p of n such that $p \equiv 1 \pmod{q}$. For any real number $y \geq 1$ and integer $a \geq 1$, put

$$S(y, a) = \sum_{\substack{p \leq y \\ p \equiv 1 \pmod{a}}} \frac{1}{p}. \tag{2}$$

It is known (see Theorem 1 in [18] or Lemma 6.3 in [17]) that

$$S(y, a) = \frac{\log_2 y}{\varphi(a)} + O(1). \tag{3}$$

In particular, the estimate

$$S(n, q) = \frac{\log_2 n}{q-1} + O(1) \gg \varepsilon(x)^{-1}$$

holds for all q in the stated range and all $n > x^{1/2}$, once x is sufficiently large. By the classical result of Turán [20], we also have that the estimate

$$\omega(n, q) = S(n, q) + O(S(n, q)^{2/3})$$

holds for all n in the interval $x^{1/2} < n \leq x$, with at most

$$O(xS(n, q)^{-1/6}) = O(x\varepsilon(x)^{1/6}) = o(x)$$

possible exceptions, and the result now follows. □

Lemma 2. For real numbers $x \geq y > 1$ let

$$\Xi(x, y) = \#\{n \leq x : P(\xi(n)) > y\}.$$

Then,

$$\Xi(x, y) \ll \frac{x(\log_2 x)^2}{y \log y}.$$

Proof. If a prime q divides $\xi(n)$, then clearly $q^2 \mid \varphi(n)$. The upper bound

$$\#\{n \leq x : \varphi(n) \equiv 0 \pmod{q^2}\} \ll \frac{x(\log_2 x)^2}{q^2}$$

is a special partial case of Lemma 2 of [5] (see also the proof of Theorem 7.1 in [4]). In particular,

$$\#\{n \leq x : P(\xi(n)) = q\} \ll \frac{x(\log_2 x)^2}{q^2}. \quad (4)$$

It now follows that

$$\Xi(x, y) = \sum_{y < q \leq x} \sum_{\substack{n \leq x \\ P(\xi(n))=q}} 1 \ll \sum_{y < q \leq x} \frac{x(\log_2 x)^2}{q^2}.$$

Using Abel summation, we estimate

$$\sum_{y < q \leq x} \frac{1}{q^2} = \frac{\pi(x)}{x^2} - \frac{\pi(y)}{y^2} + 2 \int_y^x \frac{\pi(t)}{t^3} dt \ll \frac{1}{x \log x} + \int_y^x \frac{1}{t^2 \log t} dt \ll \frac{1}{y \log y},$$

and the lemma follows. \square

Theorem 1. If $\varepsilon(x)$ is any admissible function, then the inequalities

$$\varepsilon(n) \log_2 n \leq P(\xi(n)) \leq \frac{(\log_2 n)^2}{\varepsilon(n) \log_3 n}$$

hold for almost all positive integers n .

Proof. By the Prime Number Theorem, for all sufficiently large real numbers x there exists a prime q in the interval:

$$\varepsilon(x) \log_2 x < q \leq 2 \varepsilon(x) \log_2 x.$$

If n is an integer with two prime factors $p_1 \equiv p_2 \equiv 1 \pmod{q}$, then $q \mid \xi(n)$. By Lemma 1, we derive that

$$\sum_{\substack{x^{1/2} < n \leq x \\ P(\xi(n)) \geq \varepsilon(n) \log_2 n}} 1 \geq \sum_{\substack{x^{1/2} < n \leq x \\ P(\xi(n)) \geq q}} 1 \geq \sum_{\substack{x^{1/2} < n \leq x \\ \omega(n, q) \geq 2}} 1 = x + o(x).$$

This proves the lower bound. The upper bound is a direct application of Lemma 2. \square

We remark that the upper bound of Theorem 1 improves the corollary to Theorem 2 in [9].

Theorem 2. *As $x \rightarrow \infty$, we have*

$$(1 + o(1)) x \log_3 x \leq \sum_{n \leq x} \log P(\xi(n)) \leq (2 + o(1)) x \log_3 x.$$

Proof. The above lower bound follows from the lower bound from Theorem 1. For the upper bound above, we write

$$\sum_{n \leq x} \log P(\xi(n)) = \sum_{q \leq x} \log q \sum_{\substack{n \leq x \\ P(\xi(n))=q}} 1.$$

For $q \leq y$, we trivially have

$$\sum_{q \leq y} \log q \sum_{\substack{n \leq x \\ P(\xi(n))=q}} 1 \leq \log y \sum_{q \leq y} \sum_{\substack{n \leq x \\ P(\xi(n))=q}} 1 \leq \log y \sum_{n \leq x} 1 \leq x \log y,$$

while for $q > y$, we have, by (4):

$$\sum_{y < q \leq x} \log q \sum_{\substack{n \leq x \\ P(\xi(n))=q}} 1 \ll x (\log_2 x)^2 \sum_{y < q \leq x} \frac{\log q}{q^2} \ll xy^{-1} (\log_2 x)^2,$$

where we have used Abel summation to estimate

$$\begin{aligned} \sum_{y < q \leq x} \frac{\log q}{q^2} &= \pi(x) \frac{\log x}{x^2} - \pi(y) \frac{\log y}{y^2} - \int_y^x \pi(t) \left(\frac{1}{t^3} - \frac{2 \log t}{t^3} \right) dt \\ &\ll x^{-1} + \int_y^x t^{-2} dt \ll y^{-1}. \end{aligned}$$

Setting $y = (\log_2 x)^2$, we obtain the desired upper bound. \square

Theorem 3. *As $x \rightarrow \infty$, we have*

$$\sum_{n \leq x} P(\xi(n)) \asymp x (\log_2 x)^3.$$

Proof. Let $y = (\log_2 x)^3$, $z = \exp((\log x)^{1/2})$ and $w = \exp((\log x)^{2/3})$. We also put $v = z^6$. In what follows, x is taken to be arbitrarily large.

Taking $A = 5/2$, $\varepsilon = 1/2$, and $\delta = 1/15$ in the statement of Theorem 2.1 of [1], we see that there exists an absolute constant $D \geq 0$ and a set \mathcal{D} of cardinality $\#\mathcal{D} \leq D$, with $\min\{m : m \in \mathcal{D}\} \geq \log v = 6(\log x)^{1/2}$, such that the inequality

$$\pi(t; d, 1) \geq \frac{\pi(t)}{2\varphi(d)} \quad (5)$$

holds for all positive reals t provided that $1 \leq d \leq \min\{tv^{-2/3}, z^2\}$ and that d is not divisible by any element of \mathcal{D} . Note that if x is sufficiently large and $t \geq w$, then $tv^{-2/3} \geq wv^{-2/3} \geq z^2$.

Letting \mathcal{Q} denote the set of primes $q \in [y, z] \setminus \mathcal{D}$, we therefore see that the lower bound (5) holds for all $t \in [w, x]$ and all integers $d \in [1, z^2]$ whose prime factors all lie in \mathcal{Q} . Together with the Brun–Titchmarsh theorem (see for example Theorem 3.7 in Chapter 3 of [12]), we conclude that

$$\pi(t; d, 1) \asymp \frac{\pi(t)}{\varphi(d)}$$

holds uniformly for all $t \in [w, x]$ and all integers d of the form $d = q$ or $d = q_1q_2$ composed of one or two (not necessarily distinct) primes from \mathcal{Q} . Moreover, for any sufficiently large constant $\gamma > 1$, we also have

$$\pi(t; d, 1) - \pi(t/\gamma; d, 1) \asymp \frac{\pi(t)}{\varphi(d)} \quad (6)$$

under the same conditions.

We now let

$$k = \left\lceil \frac{\log w}{\log \gamma} \right\rceil \quad \text{and} \quad K = \left\lfloor \frac{\log x}{2 \log \gamma} \right\rfloor - 1.$$

For any prime $q \in \mathcal{Q}$, we have, by (6):

$$\sum_{\substack{w < p \leq x^{1/2} \\ p \equiv 1 \pmod{q}}} \frac{1}{p} \geq \sum_{j=k}^K \frac{\pi(\gamma^{j+1}; d, 1) - \pi(\gamma^j; d, 1)}{\gamma^{j+1}} \gg \frac{1}{q} \sum_{j=k}^K \frac{1}{j} \gg \frac{\log_2 x}{q}.$$

On the other hand, the upper bound (3.1) in [7] (see also Lemma 1 of [5]) provides an upper bound of the same size as the above lower bound. Consequently,

$$\sum_{\substack{w < p \leq x^{1/2} \\ p \equiv 1 \pmod{q}}} \frac{1}{p} \asymp \frac{\log_2 x}{q}. \quad (7)$$

We now fix a prime number q in \mathcal{Q} . We denote by $N(x, q)$ the number of integers $n \leq x$ for which there exists a unique representation of the form $n = p_1 p_2 m$ for some integer m and two primes $w < p_1 < p_2 \leq x^{1/2}$ with $p_1 \equiv p_2 \equiv 1 \pmod{q}$ and such that q is the only prime in \mathcal{Q} dividing $\gcd(p_1 - 1, p_2 - 1)$. We then have

$$N(x, q) \geq T_0(x, q) - T_1(x, q) - T_2(x, q) - T_3(x, q),$$

where

- $T_0(x, q)$ is the total number of ordered triples (p_1, p_2, m) with primes $w < p_1 < p_2 \leq x^{1/2}$, $p_1 \equiv p_2 \equiv 1 \pmod{q}$, and an integer $m \leq x/p_1 p_2$. Therefore, using (7), we obtain that

$$\begin{aligned} T_0(x, q) &\gg x \sum_{\substack{w < p_1 < p_2 \leq x^{1/2} \\ p_1 \equiv p_2 \equiv 1 \pmod{q}}} \frac{1}{p_1 p_2} \\ &= \frac{x}{2} \left(\sum_{\substack{w < p \leq x^{1/2} \\ p \equiv 1 \pmod{q}}} \frac{1}{p} \right)^2 - \frac{x}{2} \sum_{\substack{w < p \leq x^{1/2} \\ p \equiv 1 \pmod{q}}} \frac{1}{p^2} \\ &\gg \frac{x}{2} \left(\frac{\log_2 x}{q} \right)^2 - \frac{x}{2q} \sum_{\substack{w < p \leq x^{1/2} \\ p \equiv 1 \pmod{q}}} \frac{1}{p} \\ &= \frac{x(\log_2 x)^2}{2q^2} + O\left(\frac{x \log_2 x}{q^2}\right) \gg \frac{x(\log_2 x)^2}{q^2}. \end{aligned}$$

- $T_1(x, q)$ is the number of triples (p_1, p_2, m) as above for which there exists another prime $\ell \in \mathcal{Q}$, $\ell \neq q$, such that $p_1 \equiv p_2 \equiv 1 \pmod{\ell}$. Then, by (7), we have that

$$\begin{aligned} T_1(x, q) &\ll x \sum_{\substack{\ell \in \mathcal{Q} \\ \ell \neq q}} \sum_{\substack{w < p_1 < p_2 \leq x^{1/2} \\ p_1 \equiv p_2 \equiv 1 \pmod{q\ell}}} \frac{1}{p_1 p_2} \leq x \sum_{\ell \in \mathcal{Q}} \left(\sum_{\substack{w < p < x^{1/2} \\ p \equiv 1 \pmod{q\ell}}} \frac{1}{p} \right)^2 \\ &\ll x \sum_{\ell \in \mathcal{Q}} \frac{(\log_2 x)^2}{q^2 \ell^2} \ll \frac{x(\log_2 x)^2}{q^2} \sum_{\ell > y} \frac{1}{\ell^2} \\ &\ll \frac{x(\log_2 x)^2}{q^2 y \log y} = o\left(\frac{x(\log_2 x)^2}{q^2}\right). \end{aligned}$$

- $T_2(x, q)$ is the number of triples (p_1, p_2, m) as above for which there exists another prime p_3 , $w < p_3 \leq x^{1/2}$, which divides m , and for some prime $\ell \in \mathcal{Q}$

(possibly $\ell = q$) one has $p_3 \equiv 1 \pmod{\ell}$, and either $p_1 \equiv 1 \pmod{\ell}$, or $p_2 \equiv 1 \pmod{\ell}$. Therefore, by (7), we see that

$$\begin{aligned} T_2(x, q) &\ll x \sum_{\ell \in \mathcal{Q}} \sum_{\substack{w < p_1, p_2 \leq x^{1/2} \\ w < p_3 \leq x^{1/2} \\ p_1 \equiv p_2 \equiv 1 \pmod{q} \\ p_3 \equiv p_2 \equiv 1 \pmod{\ell}}} \frac{1}{p_1 p_2 p_3} \\ &\ll x \sum_{\ell \in \mathcal{Q}} \sum_{\substack{w < p_1 \leq x^{1/2} \\ p_1 \equiv 1 \pmod{q}}} \frac{1}{p_1} \sum_{\substack{w < p_2 \leq x^{1/2} \\ p_2 \equiv 1 \pmod{q\ell}}} \frac{1}{p_2} \sum_{\substack{w < p_3 \leq x^{1/2} \\ p_3 \equiv 1 \pmod{\ell}}} \frac{1}{p_3} \\ &\ll x (\log_2 x)^3 \sum_{y \leq \ell \leq z} \frac{1}{q^2 \ell^2} \ll \frac{x (\log_2 x)^3}{q^2 y \log y} = o\left(\frac{x (\log_2 x)^2}{q^2}\right). \end{aligned}$$

- $T_3(x, q)$ is the number of triples (p_1, p_2, m) as above for which there exists another triple (r_1, r_2, k) with primes $w \leq r_1 < r_2 \leq x^{1/2}$ such that $r_1 \equiv r_2 \equiv 1 \pmod{\ell}$ for some $\ell \in \mathcal{Q}$, and $p_1 p_2 m = r_1 r_2 k$. Applying (7) once again, we obtain that

$$\begin{aligned} T_3(x, q) &\ll x \sum_{\ell \in \mathcal{Q}} \sum_{\substack{w < p_1 < p_2 \leq x^{1/2} \\ p_1 \equiv p_2 \equiv 1 \pmod{q}}} \frac{1}{p_1 p_2} \sum_{\substack{w < r_1 < r_2 \leq x^{1/2} \\ r_1 \equiv r_2 \equiv 1 \pmod{\ell}}} \frac{1}{r_1 r_2} \\ &\ll x (\log_2 x)^4 \sum_{y \leq \ell \leq z} \frac{1}{q^2 \ell^2} \ll \frac{x (\log_2 x)^4}{q^2 y \log y} = o\left(\frac{x (\log_2 x)^2}{q^2}\right). \end{aligned}$$

Consequently, we have

$$N(x, q) \geq T_0(x, q) - T_1(x, q) - T_2(x, q) - T_3(x, q) \gg \frac{x (\log_2 x)^2}{q^2}.$$

We note that $P(\xi(n)) \geq q$ for all $n \in N(x, q)$ and that the sets $N(x, q)$ are disjoint for different choices of $q \in \mathcal{Q}$. Thus,

$$\begin{aligned} \sum_{n \leq x} P(\xi(n)) &\gg \sum_{q \in \mathcal{Q}} q \#N(x, q) \gg x (\log_2 x)^2 \sum_{q \in \mathcal{Q}} \frac{1}{q} \\ &\geq x (\log_2 x)^2 \left(\sum_{y \leq q \leq z} \frac{1}{q} - \frac{D}{6(\log x)^{1/2}} \right) \\ &\gg x (\log_2 x)^2 (\log_2 z - \log_2 y + o(1)) \gg x (\log_2 x)^3. \end{aligned}$$

To prove the upper bound, we simply use (4) to derive that

$$\sum_{n \leq x} P(\xi(n)) \leq \sum_{q \leq x} q \sum_{\substack{n \leq x \\ P(\xi(n))=q}} 1 \ll x(\log_2 x)^2 \sum_{q \leq x} \frac{1}{q} \ll x(\log_2 x)^3.$$

This completes the proof. □

Concerning the minimal order of $P(\xi(n))$, little need be said; clearly $P(\xi(n)) \geq 1$ for all $n \geq 1$, and equality holds if and only if $n = 2, 4, p^v$ or $2p^v$ for some odd prime p and $v \geq 1$. As for the maximal order, we have the following:

Theorem 4. *The inequality*

$$P(\xi(n)) \leq \frac{(3n + 1)^{1/2} - 2}{6}$$

holds for all $n \geq 276$, and the inequality

$$P(\xi(n)) \gg n^{0.3335}$$

holds for infinitely many n .

Proof. For n in the range $276 \leq n \leq 579$, the upper bound can be verified case by case; hence, we assume that $n \geq 580$ in what follows. Without loss of generality, we may further assume that $q = P(\xi(n)) > 3$, since

$$3 \leq \frac{(3n + 1)^{1/2} - 2}{6} \quad \text{holds for all } n \geq 133.$$

If $P(\xi(n)) = q$, then either n has a prime divisor $p \equiv 1 \pmod{q}$ and $q^2 p \mid n$, or n has two distinct prime divisors $p_1 \equiv p_2 \equiv 1 \pmod{q}$. In the first case, we see that

$$q < (q^2 p/2)^{1/3} \leq (n/2)^{1/3} \leq \frac{(3n + 1)^{1/2} - 2}{6},$$

the last inequality being valid for all $n \geq 580$. In the second case, suppose $p_1 = aq + 1$ and $p_2 = bq + 1$, where $a < b$ are distinct even integers. Now if $2q + 1$ is prime, then $4q + 1$ is divisible by 3; thus, we must have $a \geq 2, b \geq 6$. Then

$$(2q + 1)(6q + 1) \leq (aq + 1)(bq + 1) = p_1 p_2 \leq n,$$

and we obtain the stated upper bound.

To establish the lower bound, we recall the result of Fouvry [10], which asserts that for all large x , the set \mathcal{Q} of primes p in the interval $x^{1/2} \leq p \leq x$ and satisfying $P(p - 1) \gg p^{0.667}$ is of cardinality $\#\mathcal{Q} \gg x/\log x$. We also recall that, by Brun's

method (see Theorem 2.2 in [12]), for any integer m , the number of primes of the form $p = mq + 1 \leq x$ for some other prime q is

$$O\left(\frac{x}{\varphi(m)(\log(x/m))^2}\right) = O\left(\frac{x}{\varphi(m)(\log x)^2}\right)$$

provided that $m < x^{1/2}$. Summing up the above inequalities over all positive integers $m \leq \log_2 x$, we see that

$$\#\{p \leq x : P(p-1) \geq x/\log_2 x\} \ll \frac{x}{\log^2 x} \sum_{m < \log x} \frac{1}{\varphi(m)} \ll \frac{x \log_2 x}{\log^2 x} = o(\mathcal{Q}).$$

Thus, most of the primes p in \mathcal{Q} in the interval have $q = P(p-1) < x/\log_2 x$, and therefore there exist two primes $p_1, p_2 \in \mathcal{Q}$ with the same value of $P(p_1-1) = P(p_2-1) = q$. With $n = p_1 p_2$, we see that $P(\xi(n)) \geq q \gg \max\{p_1^{0.667}, p_2^{0.667}\} \gg n^{0.3335}$. \square

As is clear from the proof, the upper bound of Theorem 4 is tight under the prime k -tuple conjecture of Hardy and Littlewood (see, for example, [3]). We also remark that the trivial upper bound $P(\xi(n)) \leq n^{1/2}$ holds for all $n \geq 1$.

Unfortunately, our method of proof for the lower bound of Theorem 4 can not be combined with the more recent results of [2], since the set of primes considered there is too thin.

Theorem 5. *The inequalities*

$$\Omega(\xi(n)) = (1 + o(1)) \log_2 n \log_4 n \quad \text{and} \quad \frac{\log_2 n}{(\log_3 n)^2} \ll \omega(\xi(n)) \ll \log_2 n$$

hold for almost all positive integers n .

Proof. We start with $\Omega(\xi(n))$ and first turn our attention to the upper bound. Let x be a large positive real number, and let \mathcal{A}_1 be the set of all positive integers n in the interval $[x/\log x, x]$. Clearly, \mathcal{A}_1 contains all but $o(x)$ positive integers $n \leq x$. Let \mathcal{A}_2 be the set of those integers $n \in \mathcal{A}_1$ for which $P(\xi(n)) \leq (\log_2 x)^2$; by Theorem 1, \mathcal{A}_2 contains all but $o(x)$ positive integers $n \leq x$. Let $y = (\log_2 x)^2$. For any positive integer m , we write

$$\omega_y(m) = \sum_{\substack{p < y \\ p | m}} 1 \quad \text{and} \quad \Omega_y(m) = \sum_{\substack{p < y \\ p^v || m}} v.$$

Thus, the inequality $\Omega(\xi(n)) \leq \Omega_y(\varphi(n))$ holds for all $n \in \mathcal{A}_2$. The argument on page 349 in [8] shows that

$$\sum_{n \leq x} |\Omega_y(\varphi(n)) - \log_2 x \log_2 y|^2 \ll x \log_2 x (\log_2 y)^2. \quad (8)$$

Now let $\varepsilon_1(x) = (\log_2 x)^{-1/3}$, and let \mathcal{B} be the set of those $n \leq x$ such that

$$\Omega_y(\varphi(n)) > (1 + \varepsilon_1(x)) \log_2 x \log_2 y.$$

Using (8), it follows that

$$\#\mathcal{B} \ll \frac{x}{\varepsilon_1(x)^2 \log_2 x} = o(x).$$

The set $\mathcal{A}_3 = \mathcal{A}_2 \setminus \mathcal{B}$ contains all but $o(x)$ positive integers $n \leq x$, and for each $n \in \mathcal{A}_3$ we have

$$\Omega(\xi(n)) \leq \Omega_y(\varphi(n)) \leq (1 + \varepsilon_1(x)) \log_2 x \log_2 y = (1 + o(1)) \log_2 x \log_4 x. \quad (9)$$

Since $n \geq x/\log x$ for all $n \in \mathcal{A}_3$, this shows that

$$\Omega(\xi(n)) \leq (1 + o(1)) \log_2 n \log_4 n$$

for almost all positive integers n .

Next we turn to the lower bound for $\Omega(\xi(n))$. As before, let x be a large real number, and put $\varepsilon_2(x) = (\log_3 x)^{-1/3}$ and $Q = (\log_2 x)^{1/2}$. For natural numbers n and q , we again write $\omega(n, q)$ for the number of prime factors p of n that are congruent to 1 modulo q . For a prime $q \leq Q$ we define the sets

$$\mathcal{C}_q = \left\{ n \leq x : \omega(n, q) \leq (1 - \varepsilon_2(x)) \frac{\log_2 x}{\varphi(q)} \right\},$$

and

$$\mathcal{C} = \bigcup_{q \leq Q} \mathcal{C}_q.$$

We claim that $\#\mathcal{C} = o(x)$ as $x \rightarrow \infty$. Indeed, for a fixed prime $q \leq Q$, by a result of Turán [20] (see also (1.2) of [17]), we have

$$\#\mathcal{C}_q \ll \frac{xq}{\varepsilon_2^2(x) \log_2 x} \ll \frac{x(\log_3 x)^{2/3}}{\log_2 x} q.$$

Therefore,

$$\#\mathcal{C} \leq \sum_{q \leq Q} \#\mathcal{C}_q \ll \frac{x(\log_3 x)^{2/3}}{\log_2 x} \sum_{q \leq (\log_2 x)^{1/2}} q \ll \frac{x}{(\log_3 x)^{1/3}} = o(x).$$

Now let \mathcal{D} be the set of those positive integers $n \leq x$ not lying in \mathcal{C} . Then for each

$n \in \mathcal{D}$, one has

$$\begin{aligned}
\Omega(\xi(n)) &\geq \sum_{q \leq Q} (\omega(n, q) - 1) = \sum_{q \leq Q} \omega(n, q) - \pi(Q) \\
&\geq (1 - \varepsilon_2(x)) \log_2 x \sum_{q \leq Q} \frac{1}{\varphi(q)} - \pi(Q) \\
&\geq (1 - \varepsilon_2(x)) \log_2 x \sum_{q \leq Q} \frac{1}{q} - \pi(Q) \\
&\geq (1 + o(1)) \log_2 x \log_4 x \geq (1 + o(1)) \log_2 n \log_4 n.
\end{aligned}$$

This completes the proof of the normal order of $\Omega(\xi(n))$.

We now turn our attention to $\omega(\xi(n))$ and start with the lower bound. Again, let x be a large positive real number, and let $\varepsilon_3(x)$ be any admissible function. Let q be a prime number and let $v_q(m)$ denote the largest power of q dividing a natural number m . It suffices to show that there exists a constant c_1 such that for all but $o(x)$ positive integers $n \leq x$, the estimate

$$v_q(\xi(n)) \geq \varepsilon_3(x) \log_2 x, \quad (10)$$

holds simultaneously for all primes $q \leq c_1 \log_2 x / \log_3 x$.

Let us define

$$\mathcal{W}_q = \left\{ n \leq x : \omega(n, q) < \frac{\log_2 x}{2\varphi(q)} \right\}.$$

By the result of Turán mentioned above, we have $\#\mathcal{W}_q \ll xq / \log_2 x$; summing up these estimates for all $q \leq (\log_3 x)^{1/2}$, we see that

$$\sum_{q \leq (\log_3 x)^{1/2}} \#\mathcal{W}_q \ll \frac{x}{\log_2 x} \sum_{q \leq (\log_3 x)^{1/2}} q \ll \frac{x \log_3 x}{\log_2 x \log_4 x} = o(x).$$

We also note that for $q \leq (\log_3 x)^{1/2}$, we have

$$\frac{\log_2 x}{2\varphi(q)} \gg \frac{\log_2 x}{(\log_3 x)^{1/2}}$$

which establishes (10) for q in this small range if $\varepsilon_3(x) \leq (\log_3 x)^{-1/2}$, which we now assume.

Next we consider the case in which $q > (\log_3 x)^{1/2}$.

Let us denote by $\omega_y(n)$ the number of prime factors p of n with $p \leq y$. Let \mathcal{N} be the set of integers $x^{1/2} \leq n \leq x$ for which

$$\omega_y(n) = \log_2 y + O((\log_2 y)^{2/3})$$

holds simultaneously for $y = \exp((\log x)^{1/2})$ and for $y = x$. By [20], we have that $\#\mathcal{N} = x + o(x)$.

Let \mathcal{E}_q be the set of $n \in \mathcal{N}$ such that $p^2 \mid n$ for some $p \equiv 1 \pmod{q}$ and let \mathcal{E} be the union of all \mathcal{E}_q for $q > (\log_3 x)^{1/2}$. Clearly,

$$\#\mathcal{E}_q \ll \sum_{p \equiv 1 \pmod{q}} \frac{x}{p^2} \leq \frac{x}{q^2} \sum_{t \geq 1} \frac{1}{t^2} \ll \frac{x}{q^2},$$

and therefore

$$\#\mathcal{E} \leq \sum_{q > (\log_3 x)^{1/2}} \#\mathcal{E}_q \ll x \sum_{q > (\log_3 x)^{1/2}} \frac{1}{q^2} = o\left(\frac{x}{(\log_3 x)^{1/2}}\right) = o(x).$$

For a fixed positive integer k and primes $p_1 \equiv \dots \equiv p_k \equiv 1 \pmod{q}$, let $\mathcal{N}_{k,q}(p_1, \dots, p_k)$ be the set of integers $n \in \mathcal{N} \setminus \mathcal{E}$ such that $n = p_1 \dots p_k m$ holds with some integer m with $\omega(m, q) = 0$.

We first show that if $k \leq 0.5 \log_2 x$, then $\mathcal{N}_{k,q}(p_1, \dots, p_k)$ is empty unless

$$\frac{x}{p_1 \dots p_k} \geq z, \tag{11}$$

where $z = \exp((\log x)^{1/2})$. Indeed, in the opposite case, we see that for $n \in \mathcal{N}_{k,q}(p_1, \dots, p_k)$,

$$\omega(n) \leq k + \omega(m) \leq k + \omega_z(n) \leq 0.5 \log_2 x + O((\log_2 x)^{1/2}),$$

which is impossible because $\omega(n) \sim \log_2 n \sim \log_2 x$ for $n \in \mathcal{N}$.

We now have

$$\#\mathcal{N}_{k,q}(p_1, \dots, p_k) \leq \sum_{\substack{m \leq x/(p_1 \dots p_k) \\ q \nmid \varphi(m)}} 1. \tag{12}$$

It has been shown in the proof of Theorem 4.1 of [7] that there exists an absolute constant $c_2 > 0$ such that the upper bound

$$\sum_{\substack{m \leq t \\ q \nmid \varphi(m)}} 1 \ll t \exp(-c_2 S(t, q))$$

holds uniformly when $\log t > q$, where $S(t, q)$ is given by (2). By Theorem 3.4 of [7], we know that the lower bound

$$S(t, q) \gg \frac{\log_2 t}{q}$$

holds provided that $q < \log t$. Thus, assuming (11), and remarking that $\log z = (\log x)^{1/2} > q$, we derive from (12) that the estimate

$$\#\mathcal{N}_{k,q}(p_1, \dots, p_k) \ll \frac{x}{p_1 \dots p_k} \exp\left(-c_3 \frac{\log_2 x}{q}\right)$$

holds with some absolute constant $c_3 > 0$.

Therefore, the set $\mathcal{N}_{k,q}$ consisting of all integers n in $\mathcal{N} \setminus \mathcal{E}$ that belong to at least one of the sets $\mathcal{N}_{k,q}(p_1, \dots, p_k)$, for fixed k and q , has cardinality at most

$$\begin{aligned} \#\mathcal{N}_{k,q} &= \frac{1}{k!} \sum_{\substack{p_1 < x \\ p_1 \equiv 1 \pmod{q}}} \cdots \sum_{\substack{p_k < x \\ p_k \equiv 1 \pmod{q}}} \#\mathcal{N}_{k,q}(p_1, \dots, p_k) \\ &\leq \frac{1}{k!} \sum_{\substack{p_1 < x \\ p_1 \equiv 1 \pmod{q}}} \cdots \sum_{\substack{p_k < x \\ p_k \equiv 1 \pmod{q}}} \frac{x}{p_1 \dots p_k} \exp\left(-c_3 \frac{\log_2 x}{q}\right) \\ &\leq \frac{x}{k!} \exp\left(-c_3 \frac{\log_2 x}{q}\right) S(x, q)^k. \end{aligned}$$

Put $K_q = \varepsilon_3(x)(\log_2 x)/q$. Recalling the bound (3) and using the Stirling formula, we obtain

$$\begin{aligned} \sum_{k \leq K_q} \#\mathcal{N}_{k,q} &\ll x \exp\left(-c_3 \frac{\log_2 x}{q}\right) \sum_{k \leq K_q} \frac{(2 \log_2 x)^k}{q^k k!} \\ &\ll x \exp\left(-c_3 \frac{\log_2 x}{q}\right) \sum_{k \leq K_q} \left(\frac{6 \log_2 x}{qk}\right)^k. \end{aligned}$$

Furthermore, we derive

$$\begin{aligned} \sum_{k \leq K_q} \left(\frac{6 \log_2 x}{qk}\right)^k &\ll \sum_{0 \leq i \leq \log K_q} \sum_{K_q e^{-i-1} \leq k \leq K_q e^{-i}} \left(\frac{6e^{i+1} \log_2 x}{qK_q}\right)^k \\ &= \sum_{0 \leq i \leq \log K_q} \sum_{K_q e^{-i-1} \leq k \leq K_q e^{-i}} \left(6\varepsilon_3^{-1}(x)e^{i+1}\right)^k \\ &\ll \sum_{0 \leq i \leq \log K_q} \left(6\varepsilon_3^{-1}(x)e^{i+1}\right)^{K_q e^{-i}} \\ &\ll \exp\left(c_4 K_q \log(\varepsilon_3^{-1}(x))\right) \end{aligned}$$

for some constant c_4 . Therefore, for an appropriate constant c_1 ,

$$\begin{aligned} & \sum_{q \leq c_1 \log_2 x / \log_3 x} \sum_{k \leq K_q} \#\mathcal{N}_{k,q} \\ & \ll x \sum_{q \leq c_1 \log_2 x / \log_3 x} \exp\left(-c_3 \frac{\log_2 x}{q} + c_4 K_q \log(\varepsilon_3^{-1}(x))\right) \\ & \ll x \sum_{q \leq c_1 \log_2 x / \log_3 x} \exp\left(-0.5c_3 \frac{\log_2 x}{q}\right) = o(x) \end{aligned}$$

provided that x is large enough. Clearly, the inequality (10) implies the desired lower bound on $\omega(\xi(n))$.

We now prove the upper bound on $\omega(\xi(n))$. By (1), we know that the inequality

$$\log(\xi(n)) \ll \log_2 n \log_3 n \tag{13}$$

holds on a set of positive integers 1 of asymptotic density 1. The upper bound on $\omega(\xi(n))$ claimed by our Theorem 5 follows now from inequality (13) above combined with the classical estimate

$$\omega(\xi(n)) \ll \frac{\log \xi(n)}{\log_2 \xi(n)},$$

which concludes the proof. □

It is easy to see that Theorem 5 implies that for some constant $c_5 > 0$, the bound

$$\tau(\xi(n)) \geq 2^{\omega(\xi(n))} \gg \exp\left(c_5 \frac{\log_2 n}{(\log_3 n)^2}\right)$$

holds for almost all positive integers n , where, as usual, $\tau(k)$ denotes the number of divisors of an integer $k \geq 1$.

It is also clear that for any positive integer n

$$\omega(\xi(n)) \leq \omega(\varphi(n)) \ll \frac{\log \varphi(n)}{\log_2 \varphi(n)} \ll \frac{\log n}{\log_2 n}$$

and

$$\Omega(\xi(n)) \ll \Omega(\varphi(n)) \ll \log \varphi(n) \ll \log n.$$

Theorem 6. *The inequalities*

$$\Omega(\xi(n)) \gg \log n \quad \text{and} \quad \omega(\xi(n)) \gg \frac{\log n}{\log_2 n}$$

hold for infinitely many positive integers n .

Proof. Let k be a sufficiently large integer, and then let p_1 and p_2 be the first two primes in the arithmetic progression $1 \pmod{2^k}$. By Linnik's Theorem, in the form given by Heath-Brown [13], we know that $\max\{p_1, p_2\} \ll 2^{11k/2}$. With $n = p_1 p_2$, we have that $2^k \mid \xi(n)$; therefore $\Omega(\xi(n)) \geq k \gg \log n$. Finally, let y be large and let $M = \prod_{p < y} p$. By the Prime Number Theorem, we have $\log M = (1 + o(1))y$. Let p_1 and p_2 be the first two primes in the arithmetic progression $1 \pmod{M}$. We again have that $\max\{p_1, p_2\} \ll M^{11/2}$, and with $n = p_1 p_2$ we have that $M \mid \xi(n)$. Thus,

$$\omega(\xi(n)) \gg \omega(M) = \pi(y) \gg \frac{\log M}{\log_2 M} \gg \frac{\log n}{\log_2 n},$$

which finishes the proof. \square

3. Average q -adic norm and order of $\varphi(n)$

Let q be a prime, and let $|m|_q$ be the q -adic norm of m , that is, $|m|_q = q^{-v_q(m)}$ where, as before, $v_q(m)$ is the largest power of q dividing m . In this section, we address the average value of $|\varphi(n)|_q$ and $v_q(\varphi(n))$.

Recall that an arithmetic function $f(n)$ is said to be *multiplicative* if $f(nm) = f(n)f(m)$ for any integers n and m with $\gcd(n, m) = 1$. Accordingly, if $f(nm) = f(n) + f(m)$ for any integers n and m with $\gcd(n, m) = 1$ then $f(n)$ is called *additive*.

In particular, $v_q(\varphi(n))$ is an additive function. Thus, $|\varphi(n)|_q$ is a bounded multiplicative function, and therefore it is natural that our principal tool is the following theorem of Wirsing [21].

Lemma 3. *Assume that a real-valued multiplicative function $f(n)$ satisfies the following conditions:*

- $f(n) \geq 0$, $n = 1, 2, \dots$;
- $f(p^v) \leq ab^v$, $v = 2, 3, \dots$, for some constants $a, b > 0$ with $b < 2$;
- there exists a constant $\tau > 0$ such that

$$\sum_{p \leq x} f(p) = (\tau + o(1)) \frac{x}{\log x}.$$

Then, for any $x \geq 0$,

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

where γ is the Euler constant, and

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

is the Γ -function.

Lemma 4. For any fixed prime q ,

$$\prod_{p \leq x} \left(1 + \frac{|p-1|_q}{p-1}\right) = (\eta_q + o(1)) (\log_2 x)^{\alpha_q},$$

where $\alpha_q = (q^2 - q - 1)/(q^2 - 1)$, and η_q is a constant depending only on q .

Proof. We have

$$\log \left(1 + \frac{|p-1|_q}{p-1}\right) = \frac{|p-1|_q}{p} + O\left(\frac{|p-1|_q}{p^2}\right),$$

therefore the series

$$\zeta_q = \sum_p \left| \log \left(1 + \frac{|p-1|_q}{p-1}\right) - \frac{|p-1|_q}{p} \right|$$

converges absolutely. Hence, it is enough to show that

$$\sum_{p \leq x} \frac{|p-1|_q}{p} = \alpha_q \log_2 x + \beta_q + o(1) \tag{14}$$

holds with some constant β_q .

We have:

$$\begin{aligned} \sum_{p \leq x} \frac{|p-1|_q}{p} &= \sum_{k=0}^\infty \left(\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{q^k}}} \frac{q^{-k}}{p} - \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{q^{k+1}}} } \frac{q^{-k}}{p} \right) \\ &= S(x, 1) - (q-1) \sum_{k=1}^\infty q^{-k} S(x, q^k), \end{aligned} \tag{15}$$

where, as before, $S(x, q^k)$ is given by (2).

We write K for the largest positive integer such that $q^K \leq \log_2 x$; thus, $K \asymp \log_3 x$. Using the classical *Page bound* (see Chapter 20 of [6]) and partial summation (see a remark in Chapter 22 of [6]), we have

$$\pi(t; q^k, 1) = \frac{t}{(q-1)q^{k-1} \log t} + O\left(\frac{t}{q^k (\log t)^2}\right) \tag{16}$$

for all positive integers $k \leq K$ and real $t \geq e^K$.

Therefore, using the same partial summation arguments as in the proof of Theorem 1 of [18] (see also Lemma 6.3 of [17]), and using (16) in the appropriate place (starting with the value of $t \geq e^K$), we derive that for every $k \leq K$,

$$S(x, q^k) = \frac{\log_2 x}{(q-1)q^{k-1}} + A_{k,q} + O\left(\frac{1}{(\log x)^{1/2}}\right), \quad (17)$$

for some constants $A_{k,q}$ depending only on k and q . Moreover, by Theorem 1 of [18] or Lemma 6.3 of [17], $A_{k,q} = O(1)$ uniformly for q and $k = 0, 1, \dots$ (see (3)).

For $k \geq K$, we use the fact that

$$S(x, q^k) \ll \frac{\log_2 x}{(q-1)q^{k-1}} \quad (18)$$

(see the bound (3.1) in [7] and also Lemma 1 of [5]). Define

$$\beta_q = A_{k,0} - (q-1) \sum_{k \geq 1} \frac{A_{k,q}}{q^k}.$$

Using (17) and (18) in (15), and taking into account that

$$1 - (q-1) \sum_{k \geq 1} \frac{1}{(q-1)q^{2k-1}} = \frac{q^2 - q - 1}{q^2 - 1} = \alpha_q,$$

we get (14) and thus finish the proof. \square

Theorem 7. For any prime q ,

$$\sum_{n \leq x} |\varphi(n)|_q = (\gamma_q + o(1)) x (\log x)^{-q/(q^2-1)},$$

where γ_q is a constant depending only on q .

Proof. For $p \neq q$, we have

$$\sum_{v=0}^{\infty} \frac{|\varphi(p^v)|_q}{p^v} = 1 + \sum_{v=1}^{\infty} \frac{|p-1|_q}{p^v} = \frac{|p-1|_q}{p-1},$$

and certainly

$$\sum_{v=0}^{\infty} \frac{|\varphi(q^v)|_q}{q^v} = 1 + \sum_{v=1}^{\infty} \frac{1}{q^{2v-1}} = 1 + \frac{q}{q^2-1} = \frac{q^2+q-1}{q^2-1}.$$

Combining Lemma 3 and Lemma 4, we obtain the desired result. \square

We now show that the classical *Turán–Kubilius* inequality can be used to study the normal order of $v_q(\varphi(n))$.

Theorem 8. *For any prime q , the estimate*

$$v_q(\varphi(n)) = \left(\frac{q}{(q-1)^2} + o(1) \right) \log_2 n$$

holds for almost all positive integers n .

Proof. Because $v_q(\varphi(n))$ is an additive function, by the *Turán–Kubilius* inequality (see [14], [19]), we have

$$\frac{1}{x} \sum_{n \leq x} |v_q(\varphi(n)) - A_q(x)|^2 \ll D_q(x)$$

where

$$A_q(x) = \sum_{p^r \leq x} \frac{v_q(\varphi(p^r))}{p^r} \quad \text{and} \quad D_q(x) = \sum_{p^r \leq x} \frac{v_q^2(\varphi(p^r))}{p^r},$$

and in both sums the summation is extended over all prime powers $p^r \leq x$. Thus, it is enough to show that

$$A_q(x) = \left(\frac{q}{(q-1)^2} + o(1) \right) \log_2 x \quad \text{and} \quad D(x) = o((\log_2 x)^2). \quad (19)$$

Because $v_q(\varphi(p)) \ll \log p$, using the Prime Number Theorem, we derive that

$$\sum_{\substack{p^r \leq x \\ r \geq 2}} \frac{v_q(\varphi(p))}{p^r} \ll \sum_{r=2}^x \sum_{k=2}^{\infty} \frac{\log k}{(0.5k \log k)^r} \ll \sum_{r=2}^x \sum_{k=2}^{\infty} \frac{1}{k^r} \ll \sum_{r=2}^x 2^{-r} \ll 1.$$

Thus

$$A_q(x) = \sum_{\substack{p \leq x \\ p \neq q}} \frac{v_q(\varphi(p))}{p} + O(1) = \sum_{\substack{p \leq x \\ p \neq q}} \frac{v_q(\varphi(p))}{p} + O(1).$$

Furthermore, as in the proof of Lemma 4, we derive that

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \neq q}} \frac{v_q(\varphi(p))}{p} &= \sum_{k=1}^{\infty} \left(\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{q^k}}} \frac{k}{p} - \sum_{\substack{p \leq x \\ p \equiv 1 \pmod{q^{k+1}}} } \frac{k}{p} \right) \\ &= \sum_{k=1}^{\infty} S(x, q^k) = \left(\frac{q}{(q-1)^2} + o(1) \right) \log_2 x. \end{aligned}$$

Similar arguments show that $D_q(x) = O(\log_2 x)$ (in fact, our arguments give an asymptotic formula for $D_q(x)$). Therefore, we obtain (19), which finishes the proof. \square

4. Distribution of $\Omega(\varphi(n)) - \omega(\varphi(n))$

It has been shown in [8] that for almost all positive integers n , both $\Omega(\varphi(n))$ and $\omega(\varphi(n))$ are close to $0.5(\log_2 n)^2$. Here, we study the behavior of the difference $\Omega(\varphi(n)) - \omega(\varphi(n))$.

Theorem 9. *The estimate*

$$\Omega(\varphi(n)) - \omega(\varphi(n)) = (1 + o(1)) \log_2 n \log_4 n$$

holds for almost all positive integers n .

Proof. By Theorem 5, we know that

$$\Omega(\xi(n)) = (1 + o(1)) \log_2 n \log_4 n$$

holds for almost all positive integers n . Since

$$\Omega(\varphi(n)) - \omega(\varphi(n)) = \Omega(\varphi(n)) - \omega(\lambda(n)) \geq \Omega(\varphi(n)) - \Omega(\lambda(n)) \geq \Omega(\xi(n)),$$

we see that

$$\Omega(\varphi(n)) - \omega(\varphi(n)) \geq (1 + o(1)) \log_2 n \log_4 n$$

holds for almost all positive integers n .

To obtain the upper bound, let x be a large positive real number, and let $y = (\log_2 x)^2$. The argument on page 404 of [16] shows that the set of all positive integers $n \leq x$ such that $\varphi(n)$ is not divisible by the square of any prime $q > y$ has cardinality $x + o(x)$ (see the bound on $\#\mathcal{E}_2$ in Theorem 9 of [16]). Thus, for all but $o(x)$ positive integers $n \leq x$, we have that

$$\Omega(\varphi(n)) - \omega(\varphi(n)) = \Omega_y(\varphi(n)) - \omega_y(\varphi(n)) \leq \Omega_y(\varphi(n)).$$

Now using (9) (which is established with the same value of y), we finish the proof. \square

References

- [1] W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers. *Ann. of Math.* **140** (1994), 703–722. Zbl 0816.11005 MR 1283874
- [2] R. C. Baker and G. Harman, Shifted primes without large prime factors. *Acta Arith.* **83** (1998), 331–361. Zbl 0994.11033 MR 1610553
- [3] A. Balog, The prime k -tuplets conjecture on average. In *Analytic Number Theory*, Progr. Math. 85, Birkhäuser, Boston 1990, 47–75. Zbl 0719.11066 MR 1084173

- [4] W. Banks, J. B. Friedlander, C. Pomerance and I. E. Shparlinski, Multiplicative structure of values of the Euler function. In *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Institute Communications, Amer. Math. Soc., Providence, RI, 2004, 29–47. Zbl 02154269 MR 2075645
- [5] N. L. Bassily, I. Kátai and M. Wijsmuller, On the prime power divisors of the iterates of the Euler- φ function. *Publ. Math. Debrecen* **55** (1999), 17–32. Zbl 0933.11047 MR 1708438
- [6] H. Davenport, *Multiplicative number theory*. 2nd ed., Grad. Texts in Math. 74, Springer-Verlag, New York 1980. Zbl 0453.10002 MR 0606931
- [7] P. Erdős, A. Granville, C. Pomerance and C. Spiro, On the normal behavior of the iterates of some arithmetic functions. In *Analytic Number Theory*, Prog. Math. 85, Birkhäuser, Boston 1990, 165–204. Zbl 0721.11034 MR 1084181
- [8] P. Erdős and C. Pomerance, On the normal number of prime factors of $\varphi(n)$. *Rocky Mountain J. Math.* **15** (1985), 343–352. Zbl 0617.10037 MR 0823246
- [9] P. Erdős, C. Pomerance and E. Schmutz, Carmichael’s lambda function. *Acta Arith.* **58** (1991), 363–385. Zbl 0734.11047 MR 1121092
- [10] É. Fouvry, ‘Théorème de Brun-Titchmarsh, Application au théorème de Fermat. *Invent. Math.* **79** (1985), 383–407. Zbl 0557.10035 MR 0778134
- [11] J. B. Friedlander, C. Pomerance and I. E. Shparlinski, Period of the power generator and small values of Carmichael’s function. *Math. Comp.* **70** (2001), 1591–1605. Zbl 1029.11043 MR 1836921
- [12] H. Halberstam and H.-E. Richert, *Sieve Methods*. London Math. Soc. Monographs 4, Academic Press, London 1974. Zbl 0298.10026 MR 0424730
- [13] R. Heath-Brown, Zero-free regions for Dirichlet L -functions and the least prime in an arithmetic progression. *Proc. Lond. Math. Soc.* **64** (1991), 265–338. Zbl 0739.11033 MR 1143227
- [14] J. Kubilius, *Probabilistic methods in the theory of numbers*. Transl. Math. Monographs 11, Amer. Math. Soc., Providence, RI, 1964. Zbl 0133.30203 MR 0160745
- [15] F. Luca and C. Pomerance, On some problems of Mąkowski–Schinzel and Erdős concerning the arithmetical functions φ and σ . *Colloq. Math.* **92** (2002), 111–130. Zbl 1027.11007 MR 1899242
- [16] F. Luca and I. Shparlinski, Average multiplicative orders of elements modulo n . *Acta Arith.* **109** (2003), 387–411. Zbl 1043.11067 MR 2009051
- [17] K. K. Norton, On the number of restricted prime factors of an integer I. *Illinois J. Math.* **20** (1976), 681–705. Zbl 0329.10035 MR 0419382
- [18] C. Pomerance, On the distribution of amicable numbers. *J. Reine Angew. Math.* **293/294** (1977), 217–222. Zbl 0349.10004 MR 0447087
- [19] P. Turán, On a theorem of Hardy and Ramanujan. *J. London Math. Soc.* **9** (1934), 274–276. JFM 60.0145.02
- [20] P. Turán, Über einige Verallgemeinerungen eines Satzes von Hardy und Ramanujan. *J. London Math. Soc.* **11** (1936), 125–133. Zbl 0014.00901
- [21] E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen. *Math. Ann.* **143** (1961), 75–102. Zbl 0104.04201 MR 0131389

Received November 11, 2003

William D. Banks, Department of Mathematics, University of Missouri, Columbia,
MO 65211, U.S.A.

E-mail: bbanks@math.missouri.edu

Florian Luca, Instituto de Matemáticas, Universidad Nacional Autónoma de México,
C.P. 58089, Morelia, Michoacán, México

E-mail: fluca@matmor.unam.mx

Igor E. Shparlinski, Department of Computing, Macquarie University, Sydney, NSW 2109,
Australia

E-mail: igor@ics.mq.edu.au