COLLOQUIUM MATHEMATICUM

VOL. 149 2017 NO. 2

ON TWO FUNCTIONS ARISING IN THE STUDY OF THE EULER AND CARMICHAEL QUOTIENTS

BY

FLORIAN LUCA (Johannesburg and Ostrava), MIN SHA (Sydney) and IGOR E. SHPARLINSKI (Sydney)

Abstract. We investigate two arithmetic functions naturally occurring in the study of the Euler and Carmichael quotients. The functions are related to the frequency of vanishing of the Euler and Carmichael quotients. We obtain several results concerning the relations between these functions as well as their typical and extreme values.

1. Introduction. For a positive integer m, let $\lambda(m)$ be the exponent of the multiplicative group modulo m, which is the so-called Carmichael function of m, and let $\varphi(m)$ be the Euler function of m. If the prime factorization of m is

$$m = p_1^{r_1} \dots p_k^{r_k}, \tag{1.1}$$

then

$$\lambda(m) = \mathrm{lcm}[\lambda(p_1^{r_1}), \dots, \lambda(p_k^{r_k})],$$

where for a prime power p^r we have $\lambda(p^r) = p^{r-\sigma}(p-1)$ with $\sigma = 1$ except when $p = 2$ and $r \ge 3$, in which case $\sigma = 2$.

Given an integer a relatively prime to m, the integer

$$Q_m(a) = \frac{a^{\varphi(m)} - 1}{m}$$

is called the *Euler quotient* of m with base a, which is a generalization of the classical *Fermat quotient*; moreover, the integer

$$C_m(a) = \frac{a^{\lambda(m)} - 1}{m}$$

is called the *Carmichael quotient* of m with base a. Some arithmetic properties of the numbers $Q_m(a)$ and $C_m(a)$ appear in [1] and [19], respectively. For example, if integers a, b are coprime to m, it is shown in [1, Proposition 2.1]

2010 *Mathematics Subject Classification*: 11A25, 11K65, 11N36.
Key words and phrases: Euler quotient, Carmichael quotient, Carmichael function, Euler function, greatest common divisor.
Received 5 March 2016; revised 24 January 2017.
Published online 8 May 2017.

DOI: 10.4064/cm6910-3-2017

and [19, Proposition 2.2], respectively, that

$$Q_m(ab) \equiv Q_m(a) + Q_m(b) \pmod{m},$$
$$C_m(ab) \equiv C_m(a) + C_m(b) \pmod{m};$$

if furthermore $a \equiv b \pmod{m^2}$, then $Q_m(a) \equiv Q_m(b) \pmod{m}$ and $C_m(a) \equiv C_m(b) \pmod{m}$.

In particular, we can define two group homomorphisms:

$$\psi_m \colon (\mathbb{Z}/m^2\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z}, +), \quad x \mapsto Q_m(x),$$
$$\phi_m \colon (\mathbb{Z}/m^2\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z}, +), \quad x \mapsto C_m(x).$$

For a positive integer m with prime factorization (1.1), recall that the *radical* of m is defined to be the product of all distinct prime factors of m:

$$\operatorname{rad}(m) = p_1 \dots p_k.$$

By [1, Proposition 4.4], the image of the morphism ψ_m is $d(m)\mathbb{Z}/m\mathbb{Z}$, where

$$d(m) = \gcd\big(m, \delta\varphi(\operatorname{rad}(m))\big),$$

where $\delta = 2$ if $4 \mid m$ and $\delta = 1$ otherwise. The image of the morphism ϕ_m can also be determined. The related result in [19, Proposition 4.3] concerning that image is not correct and should be replaced by the statement that the image of ϕ_m is $f(m)\mathbb{Z}/m\mathbb{Z}$, where

$$f(m) = \gcd\big(m, \delta\lambda(m)\varphi(\operatorname{rad}(m))/\varphi(m)\big)$$

(see Proposition 4.3 in the arXiv version of [19]). So, $f(m) \mid d(m)$. Moreover, by [19, Proposition 2.1], we get

$$\frac{\varphi(m)}{\lambda(m)} f(m)\mathbb{Z}/m\mathbb{Z} = d(m)\mathbb{Z}/m\mathbb{Z},$$

which implies that $\gcd\big(m, \frac{\varphi(m)}{\lambda(m)} f(m)\big) = d(m)$. Clearly,

$$\frac{d(m)}{f(m)} = \gcd(m/f(m), \varphi(m)/\lambda(m)).$$

Furthermore, by [19, Corollary 4.3], we have

$$\#\{a \in (\mathbb{Z}/m^2\mathbb{Z})^* : C_m(a) \equiv 0 \pmod{m}\} = f(m)\varphi(m). \tag{1.2}$$

Some questions about $d(m)$ and $f(m)$ have been studied in [19]. For example, in the proof of [19, Proposition 4.5] it has been demonstrated that $\lim_{m\to\infty} d(m)/m = 0$. Further, it is demonstrated in [19, Section 4] that under the assumption of the existence of infinitely many Sophie Germain primes, we have

$$\limsup_{m\to\infty} d(m)/m^{1/2} \geq 1/\sqrt{2}.$$

Here, using a result and some arguments from [9], we make these inequalities more precise as follows:

Theorem 1.1. *We have:*

(i) *For any integer* $m \ge 1$,

$$d(m) \le \sqrt{2}\, m \exp\bigl(-\sqrt{\log 2 \log m + (\log 2)^2/4}\bigr).$$

(ii) *For infinitely many integers* $m \ge 1$,

$$f(m) \ge m^{1-(1+o(1)) \log\log\log m/\log\log m}.$$

When m is square-free, it is easy to see that $d(m) = f(m)$. Our next result is to show that this is almost always true.

Theorem 1.2. *The set of positive integers* m *such that* $d(m) = f(m)$ *is of asymptotic density* 1.

More precisely, according to the proof of Theorem 1.2, for sufficiently large x and for all positive integers $m \le x$ outside a subset of cardinality $o(x)$, we have

$$d(m) = f(m) = \prod_{\substack{1\le j\le k\\ p_j < y/\log y}} p_j^{r_j}. \tag{1.3}$$

where $y = \log\log x$, and we have assumed that m has the prime factorization (1.1). Furthermore, we can replace $y/\log y$ by y in (1.3). Indeed, it is easy to see that the set of positive integers not exceeding x and divisible by a prime in the interval $[y/\log y, y)$ has asymptotic density 0 by considering the reciprocal sum of the primes p in the interval and using the Mertens formula

$$\sum_{\text{prime } p \le t} \frac{1}{p} = \log\log t + A + O(1/\log t), \qquad t \ge 3, \tag{1.4}$$

with some constant A (see [13, Equation (2.15)]).

Finally, since $f(m) \mid d(m)$ and $f(m) = d(m)$ for almost all m, it makes sense to ask which values are possible for $f(m)$ and $d(m)$. One may conjecture that for any fixed positive integers a and b with $a \mid b$ there exists m such that $(f(m), d(m)) = (a, b)$. We now establish this for large families of pairs (a, b) but also show that this conjecture is false in general.

Before we formulate our next result we need to recall that the notations $U \ll V$ and $U = O(V)$ are equivalent to $|U| \le cV$ for some constant $c > 0$. As usual, $U = o(V)$ means that $U/V \to 0$, and $U \sim V$ means that $U/V \to 1$.

Recall that *Linnik's Theorem* asserts that there exists a positive number L, known as *Linnik's constant*, such that, if $p(a, d)$ denotes the smallest prime in the arithmetic progression $\{a + nd : n \ge 0\}$ for integers $1 \le a < d$ with $\gcd(a, d) = 1$, then $p(a, d) \ll d^L$. It is known [4] that $L \le 2$ for almost all integers d. Currently, the best general estimate is $L \le 5$, due to Xylouris [25] (see also [24] for $L = 5.18$, which improves the previous bound $L \le 5.5$ of

Heath-Brown [11]); refer to Section 6 below for further comments on the choice of L.

THEOREM 1.3. *We have:*

(i) *Given any positive integer n, there exists $m \ll n^{2L+1}$ such that $d(m) = f(m) = n$.*
(ii) *Given any positive integer n, there exists $m \ll n^{6L+3}$ such that $d(m)/f(m) = n$.*
(iii) *Let a, b be two positive integers such that $a \mid b$. Assume moreover that $\gcd(b/a, a\varphi(\mathrm{rad}(b))) = 1$. Then there exists $m \ll b^{2L+2}/a$ such that $(f(m), d(m)) = (a, b)$.*

We remark that the co-primality assumption in Theorem 1.3(iii) might be strong, because Erdős [8] has shown that the set of positive integers n with $\gcd(n, \varphi(n)) = 1$ is of asymptotic density 0. However, when the assumption in Theorem 1.3(iii) does not hold, the situation becomes unstable. We give some examples as follows.

THEOREM 1.4. *We have:*

(i) *Let n be an odd positive integer greater than 1. Then there does not exist an integer $m \geq 1$ such that $(f(m), d(m)) = (n, 2n)$ or $(n, 4n)$.*
(ii) *Let p, q be two odd primes such that $p < q$, $p \mid q-1$ and $p^2 \nmid q-1$. Then there exists an integer $m \ll p(pq)^{L+1}$ such that $(f(m), d(m)) = (q, pq)$.*

REMARK 1.5. From the proofs in Sections 4 and 5, one can see that for each result in Theorem 1.3 and in Theorem 1.4(ii), there are infinitely many such integers m if we drop the boundedness condition.

2. Proof of Theorem 1.1. The closely related function

$$D(m) = \gcd(m, \varphi(m))$$

for square-free integers $m \geq 1$ has been studied in [9]. For example, it is shown in [9, Theorem 5.1] that for all square-free integers $m \geq 1$ we have

$$D(m) \leq 2m \exp\bigl(-\sqrt{\log 2 \log m}\bigr), \tag{2.1}$$

and for infinitely many square-free integers $m \geq 1$,

$$D(m) \geq m^{1-(1+o(1)) \log\log\log m/\log\log m}. \tag{2.2}$$

Since $d(m) = D(m)$ for square-free m, by (2.2) there are infinitely many integers $m \geq 1$ such that

$$d(m) \geq m^{1-(1+o(1)) \log\log\log m/\log\log m}.$$

Here, we want to establish a similar result for $f(m)$, as well as a non-trivial upper bound for $d(m)$.

We start with the observation that a modification of the argument in the proof of [9, Theorem 5.1] allows us to obtain the following improvement upon (2.1).

LEMMA 2.1. *For any square-free integer $m > 1$ and $m \neq 6$, we have*

$$D(m) \leq m \exp\bigl(-\sqrt{\log 2 \log m}\bigr).$$

Proof. First, the case $k = 1$ can be checked directly, and thus we can assume that $k \geq 2$. Now, suppose that m has the prime factorization (1.1) such that

$$p_1 < \cdots < p_k.$$

In the proof of [9, Theorem 5.1] it has been shown that the desired result is true when one of the following conditions holds:

(1) $p_k > \exp(\sqrt{\log 2 \log m})$,
(2) m is odd.

So, to complete the proof, we assume that m is even, that is,

$$p_1 = 2 \quad \text{and} \quad p_k \leq \exp\bigl(\sqrt{\log 2 \log m}\bigr). \tag{2.3}$$

If $k = 2$, then we must have $p_2 > 3$ since $m \neq 6$. In this case, we find that $m = 2p_2$ and $D(m) = 2$. So, the result can also be checked directly.

Now, we assume that $k \geq 3$, and then $m \geq 30$. Then we deduce that

$$\begin{aligned} D(m) &= \gcd\Bigl(2p_2 \dots p_k, (p_2 - 1) \dots (p_k - 1)\Bigr) \\ &= 2 \gcd\left(p_2 \dots p_k, \frac{p_2 - 1}{2} \dots \frac{p_k - 1}{2}\right) \\ &= 2 \gcd\left(p_2 \dots p_k, \frac{p_3 - 1}{2} \dots \frac{p_k - 1}{2}\right) \\ &\leq 2\left(\frac{p_3 - 1}{2}\right) \dots \left(\frac{p_k - 1}{2}\right) = \frac{2\varphi(m)}{(p_2 - 1)2^{k-2}} \leq \frac{m}{2^{k-2} p_2}, \end{aligned}$$

since m is even (see (2.3)). Moreover, also by (2.3), we have

$$k - 2 \geq \frac{\log(m/(2p_2))}{\log p_k} \geq \frac{\log(m/(2p_2))}{\sqrt{\log 2 \log m}}.$$

So

$$D(m) \leq \frac{m}{p_2} \exp\bigl(-\sqrt{\log 2 \log m} + \sqrt{\log 2/\log m}\,\log(2p_2)\bigr).$$

Thus, the result follows if

$$\exp\bigl(\sqrt{\log 2/\log m}\,\log(2p_2)\bigr) \leq p_2. \tag{2.4}$$

Since $m \geq 30$, the inequality (2.4) is a consequence of

$$\sqrt{2p_2} \leq p_2,$$

which is definitely true since $p_2 \geq 3$, and we conclude the proof. ∎

Proof of Theorem 1.1. (i) We write $m = nr$, where $r = \operatorname{rad}(m)$. If $r = 6$, then $m = 2^{s_1}3^{s_2}$ with $s_1 \geq 1$ and $s_2 \geq 1$. It is easy to check this case by a direct computation. In the following, we assume that $r \neq 6$.

On the one hand,

$$d(m) = \gcd(nr, \delta\varphi(r)) \leq \delta\varphi(r) \leq r, \tag{2.5}$$

where we have used the fact that $\delta\varphi(r) \leq r$ (this is obvious for $\delta = 1$, and when $\delta = 2$, then r is even, so $\varphi(r) \leq r/2 = r/\delta$). On the other hand,

$$d(m) = \gcd(nr, \delta\varphi(r)) \mid nD(r).$$

Using Lemma 2.1 (note that $r \neq 6$), we have

$$d(m) \leq nr \exp\bigl(-\sqrt{\log 2 \log r}\bigr) = m \exp\bigl(-\sqrt{\log 2 \log r}\bigr). \tag{2.6}$$

Using (2.5) for $r \leq \sqrt{2}\, m \exp\bigl(-\sqrt{\log 2 \log m + (\log 2)^2/4}\bigr)$ and using (2.6) otherwise, we complete the proof.

(ii) Let $\varphi_k(n)$ be the kth iterate of the Euler function at n. By convention, we set $\varphi_0(n) = n$ and $\varphi_1(n) = \varphi(n)$. For a positive integer n, define $F(n)$ to be the following square-free integer:

$$F(n) = \prod_{\substack{\text{prime } p \mid \varphi_k(n) \text{ for some } k \geq 1 \\ p \nmid n}} p.$$

From [15, Theorem 3], there is a set $\mathcal{T}$ of positive integers having asymptotic density 1 such that for $t \to \infty$, $t \in \mathcal{T}$, we have

$$\varphi(tF(t)) \geq t^{(1+o(1)) \log\log t/\log\log\log t}.$$

Set $m = tF(t)$, where we remark that $\gcd(t, F(t)) = 1$. Then

$$m \geq t^{(1+o(1)) \log\log t/\log\log\log t},$$

so

$$\log m \geq (1 + o(1)) \frac{\log t \log\log t}{\log\log\log t}. \tag{2.7}$$

Note that the function $g(x) = x \log\log x/\log x$ is increasing for large x. Applying g to both sides of (2.7), we derive

$$\log t \leq (1 + o(1)) \frac{\log m \log\log\log m}{\log\log m}. \tag{2.8}$$

So, by (2.8), we have

$$t \leq m^{(1+o(1)) \log\log\log m/\log\log m} \tag{2.9}$$

as $m \to \infty$ through such numbers. Moreover, noting that $\gcd(t, F(t)) = 1$ and that $F(t)$ is square-free, for each prime factor p of $F(t)$, by the definition of $F(t)$, we obtain

$$\gcd\left(p, \frac{\delta\lambda(m)\varphi(\mathrm{rad}(m))}{\varphi(m)}\right) = \gcd\left(p, \frac{\delta\lambda(m)\varphi(\mathrm{rad}(t))}{\varphi(t)}\right) = \gcd(p, \delta\lambda(m)) = p.$$

So, we have $F(t) \mid f(m)$, which together with (2.9) yields

$$f(m) \geq F(t) = \frac{m}{t} \geq m^{1-(1+o(1))\log\log\log m/\log\log m} \qquad \text{as } m \to \infty. \ \blacksquare$$

3. Proof of Theorem 1.2. Although the result in [14, Lemma 2] is enough for the proof of Theorem 1.2, we take this opportunity to generalize it, which is of independent interest and might have further applications.

It is shown in [14, Lemma 2] that there exists a positive constant c_0 such that on a set of asymptotic density 1 of positive integers m, $\varphi(m)$ is a multiple of all prime powers $p^a \leq c_0 \log\log m/\log\log\log m$. The proof of [16, Lemma 2.1] enhances this result as follows (note that the particular residue class of prime factors plays no role in this proof):

LEMMA 3.1. *For sufficiently large $x > 0$, all but $O(x/\log\log\log x)$ positive integers $m \leq x$ have the property that for any prime power $p^a \leq \log\log x/\log\log\log x$, m has at least two distinct prime factors congruent to* 1 *modulo p^a.*

Now we are ready to prove Theorem 1.2. This proof follows some of the arguments in [14].

Proof of Theorem 1.2. Let $\mathcal{E}_1(x)$ be the set of positive integers $m \leq x$ which fail the condition of Lemma 3.1. Then

$$\#\mathcal{E}_1(x) = o(x) \tag{3.1}$$

as $x \to \infty$. First we show that for almost all m, $d(m)$ does not have large prime factors. To do so, for a sufficiently large real number x we set

$$y = \log\log x,$$
$$\mathcal{E}_2(x) = \{m \leq x : p \mid d(m) \text{ for some odd prime } p > y\log y\}.$$

If $m \in \mathcal{E}_2(x)$, then $p \mid m$ and $p \mid \varphi(\mathrm{rad}(m))$. So, there is a prime factor q of m with $q \equiv 1 \pmod p$. Hence, $m = pqn$ for some positive integer n. The number of such $m \leq x$ is $\lfloor x/pq \rfloor \leq x/pq$. Summing this up over all primes $q \leq x$ congruent to 1 modulo p and then over all primes $p > y\log y$ and using the Brun–Titchmarsh Theorem (see [13, Theorem 6.6]) coupled with partial summation, we obtain

$$\#\mathcal{E}_2(x) \le \sum_{p>y\log y} \sum_{\substack{q\le x\\ q\equiv 1 \pmod p}} \frac{x}{pq} = x \sum_{p>y\log y} \frac{1}{p} \sum_{\substack{q\le x\\ q\equiv 1 \pmod p}} \frac{1}{q} \tag{3.2}$$
$$\ll x \sum_{p\ge y\log y} \frac{\log\log x}{p^2} \ll xy \sum_{n\ge y\log y} \frac{1}{n^2} \ll \frac{x}{\log y} = o(x)$$

as $x \to \infty$.

Let $\mathcal{E}_3(x)$ be the set of $m \le x$ having a prime divisor in the interval $I = [y/\log y, y\log y]$. Writing $m = pn$ for $p \in I$ and fixing p, we deduce that there are $\lfloor x/p \rfloor \le x/p$ possible choices for n. Hence, using the Mertens formula (1.4), we obtain

$$\#\mathcal{E}_3(x) \le x \sum_{y/\log y\le p\le y\log y} \frac{1}{p} \tag{3.3}$$
$$= x(\log\log(y\log y) - \log\log(y/\log y)) + O(x/\log y)$$
$$= x\log(1 + O(\log\log y/\log y)) + O(x/\log y)$$
$$\ll \frac{x\log\log y}{\log y} = o(x)$$

as $x \to \infty$.

Now, let $\mathcal{E}_4(x)$ be the set of $m \le x$ which are not in $\mathcal{E}_1(x) \cup \mathcal{E}_2(x) \cup \mathcal{E}_3(x)$ such that $\gcd(m, \varphi(m))$ is divisible by some prime power $p^a > y/\log y$. If $p \mid \varphi(\mathrm{rad}(m))$, then as m is not in $\mathcal{E}_2(x)$, it follows that $p \le y\log y$, and as m is not in $\mathcal{E}_3(x)$, it follows that $p < y/\log y$; hence, $a \ge 2$. If $p \nmid \varphi(\mathrm{rad}(m))$, then we must have $p^2 \mid m$, and since $m \notin \mathcal{E}_3(x)$, we have $p < y/\log y$ or $p > y\log y$; so $p^2 \mid m$, and either $a \ge 2$ or $p > y\log y$. Thus, m has a square-full divisor $d > y/\log y$ or $d > (y\log y)^2$. For fixed d, the number of such $m \le x$ is $\lfloor x/d \rfloor \le x/d$. So, we deduce that

$$\#\mathcal{E}_4(x) \le x \sum_{\substack{d>y/\log y\\ d\,\text{square-full}}} \frac{1}{d} + x \sum_{\substack{d>(y\log y)^2\\ d\,\text{square-full}}} \frac{1}{d} \tag{3.4}$$
$$\ll \frac{x(\log y)^{1/2}}{y^{1/2}} + \frac{x}{y\log y} = o(x)$$

as $x \to \infty$.

We see from (3.1)–(3.4) that for the exceptional set

$$\mathcal{E}(x) = \mathcal{E}_1(x) \cup \mathcal{E}_2(x) \cup \mathcal{E}_3(x) \cup \mathcal{E}_4(x),$$

we have

$$\#\mathcal{E}(x) = o(x) \quad \text{as } x \to \infty.$$

From now on, we assume that m is in $[1,x]\setminus\mathcal{E}(x)$ and has the prime factorization as in (1.1). Looking at

$$d(m)=\gcd\bigl(m,\delta\varphi(\mathrm{rad}(m))\bigr),$$

we claim that

$$d(m)=\prod_{\substack{1\le j\le k\\ p_j<y/\log y}} p_j^{r_j}.$$

Indeed, since $m\notin\mathcal{E}_2(x)\cup\mathcal{E}_3(x)$, it follows that if $p_j\ge y/\log y$, then $p_j\nmid d(m)$. Further, if $p_j<y/\log y$, then since $m\notin\mathcal{E}_1(x)$, by Lemma 3.1 we have $p_j\mid\varphi(\mathrm{rad}(m))$, and so from $p_j^{r_j}\mid\gcd(m,\varphi(m))$ we deduce that $p_j^{r_j}\le y/\log y$ because $m\notin\mathcal{E}_4(x)$, and thus $p_j^{r_j}$ divides $\varphi(\mathrm{rad}(m))$ because $m\notin\mathcal{E}_1(x)$. This yields the claim.

Finally, we look at

$$f(m)=\gcd\bigl(m,\delta\lambda(m)\varphi(\mathrm{rad}(m))/\varphi(m)\bigr).$$

Let $\mathcal{E}_5(x)$ be the set of positive integers $m\le x$ for which there exist a prime p and an integer $r\ge 2$ such that $p^r\mid m$ and $p^r>(y/\log y)^{1/2}$. Thus, each $m\in\mathcal{E}_5(x)$ has a square-full divisor $d>(y/\log y)^{1/2}$, so as in (3.4) we deduce that

$$\#\mathcal{E}_5(x)=o(x)\qquad\text{as } x\to\infty.$$

Let $m\in[1,x]\setminus(\mathcal{E}(x)\cup\mathcal{E}_5(x))$. We still assume that m has the prime factorization (1.1). For a prime factor $p_j<y/\log y$, from the above discussion we have $p_j^{r_j}\le y/\log y$, and then $p_j^{r_j}\mid\lambda(m)$ because $m\notin\mathcal{E}_1(x)$, and so $p_j\mid f(m)$. If $r_j\ge 2$, then $p_j^{r_j}\le(y/\log y)^{1/2}$ because $m\notin\mathcal{E}_5(x)$, and thus $p_j^{2r_j}\le y/\log y$, which together with $m\notin\mathcal{E}_1(x)$ and Lemma 3.1 implies that there exists a prime factor q of m such that $p_j^{2r_j}\mid q-1$. Thus, $p_j^{r_j}\mid f(m)$. Hence,

$$f(m)=\prod_{\substack{1\le j\le k\\ p_j<y/\log y}} p_j^{r_j}=d(m).\ \blacksquare$$

4. Proof of Theorem 1.3. (i) Choose an odd prime $p\equiv 1 \pmod{n^2}$. By Linnik's Theorem, the smallest such prime satisfies $p\ll n^{2L}$. By construction, we have $p>n^2$.

Now, take $m=np$. Clearly,

$$d(m)=\gcd\bigl(m,\delta\varphi(\mathrm{rad}(m))\bigr)=\gcd\bigl(np,\delta\varphi(\mathrm{rad}(n))(p-1)\bigr)=n,$$

and then noticing $n^2\mid\lambda(m)$, we have

$$\begin{aligned}f(m)&=\gcd\bigl(m,\delta\lambda(m)\varphi(\mathrm{rad}(m))/\varphi(m)\bigr)\\&=\gcd\bigl(np,\delta\lambda(m)\varphi(\mathrm{rad}(n))/\varphi(n)\bigr)=n.\end{aligned}$$

So, we can construct an integer $m \ll n^{2L+1}$ such that

$$d(m) = f(m) = n.$$

(ii) We first write $\lambda(n) = \lambda_1\lambda_2$ so that

$$\gcd(\lambda_1, n) = 1 \quad \text{and} \quad \operatorname{rad}(\lambda_2) \mid n.$$

We then choose an odd prime q satisfying

$$q \equiv 1 + 8n^3\lambda_2^2/\operatorname{rad}(n) \pmod{8n^4\lambda_2^2/\operatorname{rad}(n)}.$$

By Linnik's Theorem, the smallest such prime satisfies $q \ll n^{6L}$. By construction, we can write

$$q - 1 = 8kn^3\lambda_2^2/\operatorname{rad}(n)$$

with

$$\gcd(q, 8n^3\lambda_2^2/\operatorname{rad}(n)) = 1 \quad \text{and} \quad \gcd(k, n) = 1.$$

Take $m = 4n^2\lambda_2 q$. Clearly,

$$d(m) = \gcd\big(m, \delta\varphi(\operatorname{rad}(m))\big) = \gcd\big(4n^2\lambda_2 q, 2\varphi(\operatorname{rad}(n))(q-1)\big) = 4n^2\lambda_2.$$

In addition,

$$\lambda(m) = \operatorname{lcm}[\lambda(4n^2\lambda_2), q-1] = c(q-1)$$

for some integer c dividing λ_1, and so $\gcd(c, n) = 1$. Then

$$\frac{\lambda(m)\varphi(\operatorname{rad}(m))}{\varphi(m)} = \frac{c(q-1)\varphi(\operatorname{rad}(n))}{\varphi(4n^2\lambda_2)} = \begin{cases} 2ckn\lambda_2 & \text{if } n \text{ is even,} \\ 4ckn\lambda_2 & \text{if } n \text{ is odd,} \end{cases}$$

where we use the identity

$$\varphi(4n^2\lambda_2) = \begin{cases} 4n\lambda_2\varphi(n) & \text{if } n \text{ is even,} \\ 2n\lambda_2\varphi(n) & \text{if } n \text{ is odd.} \end{cases}$$

Thus, if n is even, we obtain

$$\begin{aligned} f(m) &= \gcd\big(m, \delta\lambda(m)\varphi(\operatorname{rad}(m))/\varphi(m)\big) \\ &= \gcd(4n^2\lambda_2 q, 4ckn\lambda_2) = 4n\lambda_2, \end{aligned}$$

while if n is odd,

$$f(m) = \gcd(4n^2\lambda_2 q, 8ckn\lambda_2) = 4n\lambda_2.$$

Hence, we always have $f(m) = 4n\lambda_2$, and so

$$d(m)/f(m) = n.$$

We conclude the proof by noticing that we can make $m \ll n^{6L+3}$.

(iii) Denote $c = b/a$. If c is even, then since $\gcd(c, \varphi(\operatorname{rad}(b))) = 1$, we must have $b = 2^r$ for some integer $r \geq 1$. Then, from the assumption $\gcd(c, a) = 1$, we see that $a = 1$. For $(a, b) = (1, 2)$, by choosing $m = 2^s$, $s \geq 3$, we get $(f(m), d(m)) = (1, 2)$. If $r \geq 2$, then by choosing a prime p such that $2^{r-1} \mid p - 1$ and $2^r \nmid p - 1$ (for example, $p \equiv 1 + 2^{r-1} \pmod{2^r}$) and letting $m = 2^{r+1}p$, we obtain $(f(m), d(m)) = (1, 2^r) = (a, b)$.

Now, assume that c is odd. We choose an odd prime q such that

$$q \equiv 1 + a^2 c \pmod{a^2 c^2}.$$

Write $q - 1 = a^2 cj$. By construction, $\gcd(c, j) = 1$.

We let $m = ac^2 q$. Since $\gcd(c, j) = 1$ and $\gcd(c, a\varphi(\mathrm{rad}(b))) = 1$, it is easy to see that

$$d(m) = \gcd\big(ac^2 q, \delta\varphi(\mathrm{rad}(b))a^2 cj\big) = ac = b,$$
$$f(m) = \gcd\left(ac^2 q, \frac{\delta \,\mathrm{lcm}[\lambda(a), \lambda(c^2), a^2 cj]\varphi(\mathrm{rad}(b))}{\varphi(ac^2)}\right) = a.$$

As above, by Linnik's Theorem, we can choose $m \ll b^{2L+2}/a$.

5. Proof of Theorem 1.4. (i) By contradiction, assume that there exists an integer $m \geq 1$ such that $f(m) = n$ and $d(m) = 2n$, that is,

$$\gcd\big(m, \delta\varphi(\mathrm{rad}(m))\big) = 2n, \tag{5.1}$$

$$\gcd\big(m, \delta\lambda(m)\varphi(\mathrm{rad}(m))/\varphi(m)\big) = n. \tag{5.2}$$

Note that $n > 1$ and n is odd.

Write $m = 2nm_1$. Note that we must have $m_1 > 1$. If m_1 is even, then $\delta = 2$, and so $4 \mid \gcd(m, \delta\varphi(\mathrm{rad}(m)))$. Thus, $4 \mid 2n$ by (5.1), which contradicts the fact that n is odd. So, m_1 must be odd.

Then it is easy to see that the integer $\lambda(m)\varphi(\mathrm{rad}(m))/\varphi(m)$ is even. So, $2 \mid n$ by (5.2). This contradicts the fact that n is odd. Hence, such an integer m does not exist.

Similarly, we can also show that there is no positive integer m such that $(f(m), d(m)) = (n, 4n)$.

(ii) We choose an odd prime ℓ such that

$$\ell \equiv 1 + q \pmod{pq}.$$

Write $\ell - 1 = qa$. By construction, $\gcd(p, a) = 1$.

Now, let $m = p^2 q\ell$. Since $\gcd(p, a) = 1$, $p \mid q - 1$ and $p^2 \nmid q - 1$, it is easy to see that

$$d(m) = \gcd(p^2 q\ell, (p-1)(q-1)qa) = pq,$$
$$f(m) = \gcd\left(p^2 q\ell, \frac{\mathrm{lcm}[p(p-1), q-1, qa]}{p}\right) = q.$$

As before, by Linnik's Theorem, we can choose $m \ll p(pq)^{L+1}$.

6. Comments. We see from the proof of Theorem 1.3 that its bounds depend on the smallest prime in some specific arithmetic progressions, and thus in many cases, the value of L can be chosen to be smaller than that implied by the general results of Xylouris [24, 25].

For example, in Theorem 1.3(i) the result depends on the smallest prime $p \equiv 1 \pmod{n}$. We have already mentioned that [4] allows the value of $L = 2$ for almost all n. One can however do better with the use of a result of Mikawa [17] that allows one to take $L = 32/17$ for almost all n in the statement of Theorem 1.3(i).

Furthermore, in Theorem 1.3(ii) the result depends on the smallest prime $q \equiv 1 \pmod{n^2}$. The result of Baker [3] (see also [2]), which gives a version of the Bombieri–Vinogradov Theorem for square moduli, implies that for almost all n the statement of Theorem 1.3(ii) holds with any fixed $L > 2$.

We also recall that there are concrete families of moduli which admit a better value of L. For example, by the result of Chang [6, Corollary 11] one can take any $L > 12/5$ for moduli without large prime divisors. In particular, this is true for all powers of a fixed prime number.

It is also likely that one can use the above results to improve Theorems 1.3(ii) and 1.4(ii) for almost all values of the parameters involved.

We remark that the additivity of the Carmichael quotients implies that for any integer k the exponential function $\exp(2\pi i k C_m(a)/m)$ is a multiplicative character of the group $(\mathbb{Z}/m^2\mathbb{Z})^*$. For a prime $m = p$, this has been observed and used by Heath-Brown [12, Theorem 2] (see also [21]) in the classical case of Fermat quotients $(a^{p-1} - 1)/p$ modulo a prime p. The same approach also works for the Carmichael quotients, and combined with the Burgess bound (see [13, Theorem 12.6]) allows one to study the distribution of values $C_m(a)$, $1 \le a \le A$, modulo m. One can also study their algebraic and additive properties (see [7] and [10], respectively, for the case of Fermat quotients). Furthermore, using the fact that the set (1.2) is a subgroup of $(\mathbb{Z}/m^2\mathbb{Z})^*$ one can obtain analogues of several other results about the distribution of its elements, in particular about the smallest element which does not belong to this set (see [5, 18, 20, 22, 23] and references therein).

Acknowledgments. The authors are grateful to the referee for valuable comments, suggestions and especially for pointing out the error in [19, Proposition 4.3] and for suggesting establishing the results in Theorem 1.3(i) and (ii).

This paper started during a visit of F. L. to the School of Mathematics and Statistics of the University of New South Wales in January 2016. This author thanks that institution for hospitality and support. Part of this work was also done when F. L. was visiting the Max Planck Institute for Mathematics in Bonn in 2017. He thanks this institution for hospitality. In addition, he was also supported by grants CPRR160325161141 and an A-rated researcher award both from the NRF of South Africa, and by grant no. 17-02804S of the Czech Granting Agency. The research of the second and third authors was supported by the Australian Research Council Grant DP130100237.

REFERENCES

[1] T. Agoh, K. Dilcher and L. Skula, *Fermat quotients for composite moduli*, J. Number Theory 66 (1997), 29–50.

[2] R. Baker, *Primes in arithmetic progressions to spaced moduli*, Acta Arith. 153 (2012), 133–159.

[3] R. Baker, *Primes in arithmetic progressions to spaced moduli. III*, arXiv:1602.03500.

[4] E. Bombieri, J. B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli. III*, J. Amer. Math. Soc. 2 (1989), 215–224.

[5] J. Bourgain, K. Ford, S. V. Konyagin and I. E. Shparlinski, *On the divisibility of Fermat quotients*, Michigan Math. J. 59 (2010), 313–328.

[6] M.-C. Chang, *Short character sums for composite moduli*, J. Anal. Math. 123 (2014), 1–33.

[7] Z. X. Chen and A. Winterhof, *Interpolation of Fermat quotients*, SIAM J. Discrete Math. 28 (2014), 1–7.

[8] P. Erdős, *Some asymptotic formulas in number theory*, J. Indian Math. Soc. 12 (1948), 75–78.

[9] P. Erdős, F. Luca and C. Pomerance, *On the proportion of numbers coprime to a given integer*, in: Anatomy of Integers, J.-M. De Koninck et al. (eds.), CRM Proc. Lecture Notes 46, Amer. Math. Soc., Providence, RI, 2008, 47–64.

[10] G. Harman and I. E. Shparlinski, *Products of small integers in residue classes and additive properties of Fermat quotients*, Int. Math. Res. Notices 2016, no. 5, 1424–1446.

[11] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. 64 (1992), 265–338.

[12] D. R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, in: Analytic Number Theory (in Honor of Heini Halberstam), Birkhäuser, Boston, 1996, Vol. 2, 451–463.

[13] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.

[14] 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.

[15] F. Luca and C. Pomerance, *Irreducible radical extensions and Euler-function chains*, Integers 7 (2007), no. 2, paper A25.

[16] F. Luca and C. Pomerance, *The range of the sum-of-proper-divisors function*, Acta Arith. 168 (2015), 187–199.

[17] H. Mikawa, *On primes in arithmetic progressions*, Tsukuba J. Math. 25 (2001), 121–153.

[18] A. Ostafe and I. E. Shparlinski, *Pseudorandomness and dynamics of Fermat quotients*, SIAM J. Discrete Math. 25 (2011), 50–71.

[19] M. Sha, *The arithmetic of Carmichael quotients*, Period. Math. Hungar. 71 (2015), 11–23.

[20] I. D. Shkredov, E. V. Solodkova and I. V. Vyugin, *Intersections of multiplicative subgroups and Heilbronn's exponential sum*, arXiv:1302.3839 (2013).

[21] I. E. Shparlinski, *Fermat quotients: exponential sums, value set and primitive roots*, Bull. London Math. Soc. 43 (2011), 1228–1238.

[22] I. E. Shparlinski, *On the value set of Fermat quotients*, Proc. Amer. Math. Soc. 140 (2012), 1199–1206.
[23] I. E. Shparlinski, *On vanishing Fermat quotients and a bound of the Ihara sum*, Kodai Math. J. 36 (2013), 99–108.
[24] T. Xylouris, *On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions*, Acta Arith. 150 (2011), 65–91.
[25] T. Xylouris, *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, PhD thesis, Rheinische Friedrich-Wilhelms-Universität Bonn, 2011.

Florian Luca
School of Mathematics
University of the Witwatersrand
Private Bag X3
Wits 2050, South Africa
and
Department of Mathematics
Faculty of Sciences
University of Ostrava
30. dubna 22
701 03 Ostrava 1, Czech Republic
E-mail: florian.luca@wits.ac.za

Min Sha, Igor E. Shparlinski
School of Mathematics and Statistics
University of New South Wales
Sydney, NSW 2052, Australia
E-mail: shamin2010@gmail.com
igor.shparlinski@unsw.edu.au