mathematics

MDPI

Article

Revisited Carmichael's Reduced Totient Function

Samir Brahim Belhaouari [1,*,†], Yassine Hamdi [2,†] and Abdelouahed Hamdi [3,†]

1 College of Science and Engineering, Hamad Bin Khalifa University Education City, Doha 24404, Qatar
2 Applied Mathematics Engineering, Ecole Polytechnique of Paris, 91128 Palaiseau, France; yassine.hamdi@polytechnique.edu
3 Department of Mathematics, Statistics and Physics, College of Arts and Sciences, Qatar University, Doha 2713, Qatar; abhamdi@qu.edu.qa
* Correspondence: sbelhaouari@hbku.edu.qa
† These authors contributed equally to this work.

Abstract: The modified Totient function of Carmichael $\lambda(.)$ is revisited, where important properties have been highlighted. Particularly, an iterative scheme is given for calculating the $\lambda(.)$ function. A comparison between the Euler φ and the reduced totient $\lambda(.)$ functions aiming to quantify the reduction between is given.

Keywords: Euler theorem; Euler's totient function; prime numbers

1. Introduction

More than a century ago, Robert D. Carmichael (1879–1967) [1] introduced a function $\lambda(.)$ known as `Carmichael's function`. This $\lambda(n)$ is spread as the reduced totient function which can be seen as the `smallest divisor of Euler's totient function` verifying Euler's theorem. This Totient function is deeply related to prime numbers and integer orders [2–5], mainly used for primality testing. Furthermore, the reader may cross in the literature that the Carmichael function represents the exponent ($\lambda(n)$ represents the order of the largest cyclic subgroup of $(\mathbb{Z}/\,n\,\mathbb{Z})^*$) of the group $(\mathbb{Z}/\,n\,\mathbb{Z})^*$.

In this paper, we aim to analyse $\lambda(.)$ and we present some of its important properties. Mainly, we give in Lemma 3 a suitable iterative scheme for calculating the values of $\lambda(n)$. In addition, we prove the following estimation

$$\lambda(n) \leq \frac{1}{2^{N-1}}\,\varphi(n), \quad N \text{ is the number of odd prime divisors of } n,$$

which could be considered an indicator of reduction of the modified totient function and we can easily duduce that

$$\limsup_{n\to\infty} \frac{\varphi(n)}{\lambda(n)} = +\infty.$$

The complexity of finding the inverse function of Carmichael $\lambda(.)$ is more complex than finding the inverse of Euler function.

2. Preliminaries

In the literature, Carmichael's new totient function named λ is defined as follows: For the prime decomposition of a given natural integer

$$n = \prod_{i=1}^{k} p_i^{k_i}, \quad \lambda(n) = LCM\Big[\lambda(p_1^{k_1}), \ldots, \lambda(p_k^{k_k})\Big],$$

check for updates

Citation: Belhaouari, S.B.; Hamdi, Y.; Hamdi, A. Revisited Carmichael's Reduced Totient Function. *Mathematics* **2021**, *9*, 1800. https://doi.org/10.3390/math9151800

Academic Editors: Patrick Solé and Li Guo

Received: 13 May 2021
Accepted: 13 July 2021
Published: 29 July 2021

where (LCM denotes the least common multiple.) we have:

$$\lambda(p_i^{k_i}) = \begin{cases} 2^{k_i} - 2 & \text{If} \quad p_i = 2 \text{ and } k_i > 2, \\ p_i^{k_i - 1}(p_i - 1) & \textit{otherwise.} \end{cases}$$

We refer to [1,2,6,7] and references therein for the properties of the function λ.

Figures 1 and 2 produce the first thousand values of $\lambda(p)$ and $\varphi(p)$. The points on the top lines represent $\lambda(p) = p - 1 = \varphi(p)$, when p is a prime number.

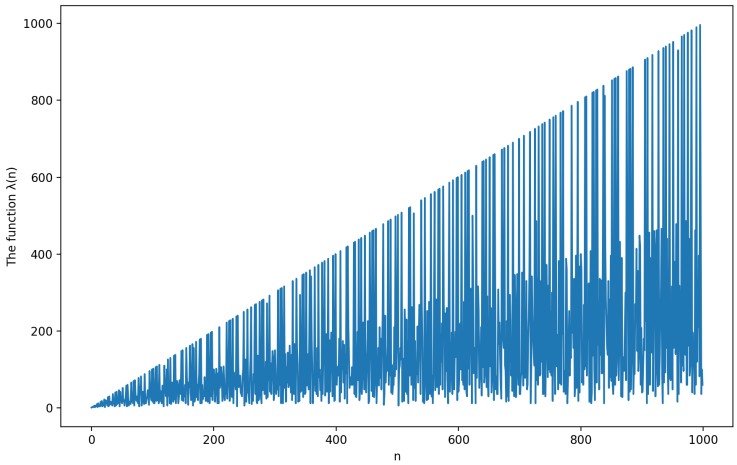

Figure 1. The first 1000 values of the Carmichael function.

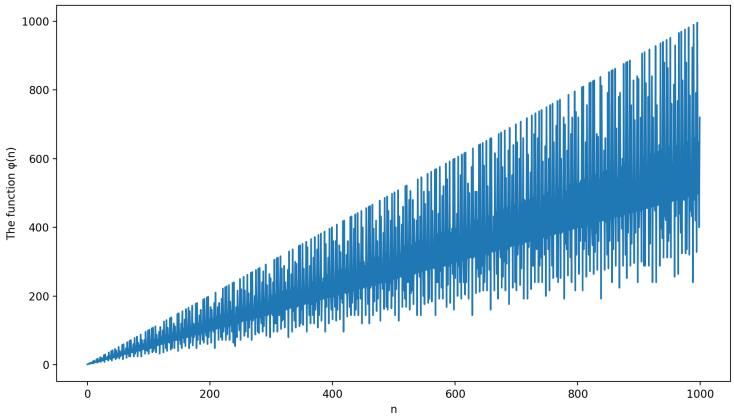

Figure 2. The first 1000 values of the Euler function.

In this section, we show how we built the modified Totient function λ.

Euler theorem [1] states that if n and m are co-prime positive integers, then

$$m^{\varphi(n)} \equiv 1 (mod\, n),$$

where $\varphi(.)$ is `Euler's Totient` function. It is known that for any `prime number` p, we have $\varphi(p) = p - 1$ since all the positive integers less than p are co-prime with p.
If p and q are two different primes, then

$$\begin{cases} m^{k_1(p-1)} \equiv 1 \, (mod\, p) & \forall k_1 \in \mathbb{N},\ gcd(m, p) = 1. \\ m^{k_2(q-1)} \equiv 1 \, (mod\, q) & \forall k_2 \in \mathbb{N},\ gcd(m, q) = 1. \end{cases}$$

The two integers k_1 and k_2 can be chosen in such a way that

$$k_1(p-1) = k_2(q-1),$$

then we obtain:

$$\begin{cases} m^{k_1(p-1)+1} \equiv m \,(mod\, p) & \forall k_1 \in \mathbb{N},\ \forall m \in \mathbb{N}. \\ m^{k_2(q-1)+1} \equiv m \,(mod\, q) & \forall k_2 \in \mathbb{N},\ \forall m \in \mathbb{N}. \end{cases}$$

We can also conclude the following

$$m^{k_1(p-1)+1} \equiv m^{k_2(q-1)+1} \equiv m \,(mod\, p\, q). \tag{1}$$

In the next definition, we introduce a new function related to the Totient function of Euler given as follows:

Definition 1. *Let $n = p\, q$*

$$\begin{array}{rcl} \lambda(n) & = & \min\{k_1(p-1) \ :\ k_1(p-1) = k_2(q-1)\} \\ & = & \min\{k_1\varphi(p) \ :\ k_1\varphi(p) = k_2\varphi(q)\}. \end{array} \tag{2}$$

According to the above definition, we will have:

$$m^{\lambda(p\,q)+1} \equiv m \,(mod\, p\, q),\ \forall m \in \mathbb{N}, \tag{3}$$

and by using previous results, we can conclude the following Lemma.

Lemma 1. *Let p and q two different primes*

- *If $gcd(m, p\, q) = 1$, then*

$$\begin{cases} m^{\varphi(n)} \equiv 1 \,(mod\, p\, q) \\ m^{\lambda(n)} \equiv 1 \,(mod\, p\, q). \end{cases}$$

- *For all integer m, then*

$$\begin{cases} m^{\varphi(n)+1} \equiv m \,(mod\, p\, q) \\ m^{\lambda(n)+1} \equiv m \,(mod\, p\, q). \end{cases}$$

Let us generalize the previous Lemma for $n = \Pi_{i=1}^{N} p_i,\ \forall N \in \mathbb{N}$, but the function $\lambda\left(n = \Pi_{i=1}^{N} p_i\right)$ needs also to be generalized.

From Euler theorem, we can write

$$\begin{cases} m^{k_i(p_i-1)+1} \equiv m \,(mod\, p_i) & \forall (m, k_i) \in \mathbb{N}^2 \\ m^{k_i(p_i-1)} \equiv 1 \,(mod\, p_i) & \forall k_i \in \mathbb{N},\ gcd(m, p_i) = 1. \end{cases}$$

Then, the function λ at $n = \Pi_{i=1}^{N} p_i$ should be defined as follows:

$$\begin{array}{rcl} \lambda\left(\Pi_{i=1}^{N} p_i\right) & = & \min\{k_1(p_1-1) \ :\ k_i(p_i-1) = k_1(p_1-1),\ i = 1, 2, \cdots, N\} \\ & = & \min\{k_1\varphi(p_1) \ :\ k_i\varphi(p_i) = k_1\varphi(p_1),\ i = 1, 2, \cdots, N\}. \end{array}$$

Example 1. *If* $n = 105 = 3 \times 5 \times 7$, *then*

$$\lambda(n) = min\{2k_1 \ : \ 2k_1 = 4k_2 = 6k_3\} = 12,$$

so,

$$\begin{cases} m^{12k_0+1} \equiv \ m \, (mod \, 3 \times 5 \times 7) & \forall (m, k_0) \in \mathbb{N}^2 \\ m^{12k_0} \equiv \ 1 \, (mod \, 3 \times 5 \times 7) & \forall k_0 \in \mathbb{N}, \ gcd(m, 3 \times 5 \times 7) = 1. \end{cases}$$

The following proposition provides a recursive scheme to evaluate the $\lambda(n)$ for different situations.

Proposition 1. $\lambda(n)$ *can be calculated by a recursive way:*

$$\lambda(p_1 \, p_2) = \frac{(p_1 - 1)(p_2 - 1)}{gcd(p_1 - 1; \ p_2 - 1)}. \tag{4}$$

$$\lambda(p_1 \, p_2 \, p_3) = \frac{\lambda(p_1 \, p_2)(p_3 - 1)}{gcd(\lambda(p_1 \, p_2); \ p_3 - 1)}. \tag{5}$$

and

$$\lambda(\Pi_{j=1}^{i} p_j) = \frac{\lambda(\Pi_{j=1}^{i-1} p_j)(p_i - 1)}{gcd(\lambda(\Pi_{j=1}^{i-1} p_j); \ p_i - 1)}. \tag{6}$$

Again, we generalize our Lemma 1 result for $n = p_i^k$, where $k \geq 2$, as follows:

Lemma 2. *If* $n = \Pi_{i=1}^{N} p_i^{n_i}$ *and* $K = \max_i\{n_i\}$, *then*

$$\lambda(n) = \min\{k_1 \varphi(p_1^{n_1}) \ : \ k_i \varphi(_i^{n_i}) = k_1 \varphi(p_1^{n_1}), \ i = 1, 2, \cdots, N\},$$

$$\begin{cases} m^{k \, \phi(n)} \equiv \ 1 \, (mod \, n) & \forall k \in \mathbb{N}, \ gcd(m, n) = 1, \\ m^{k \, \lambda(n)+K} \equiv \ m^K \, (mod \, n) & \forall m, \ k \in \mathbb{N}, \end{cases}$$

Proof.

- If $gcd(n, m) = 1$, then
$$\begin{cases} m^{p_i^k - p_i^{k-1}} \equiv \ 1 \, (mod \, p_i^k) \\ m^{p_i^k - p_i^{k-1}+1} \equiv \ m \, (mod \, p_i^k). \end{cases}$$
- For $k \geq 2$, we have
$$p_i^k - p_i^{k-1} + 1 = p_i^{k-1}(p_i - 1) + 1 \geq 2^{k-1} + 1 \geq k.$$
- It concludes that
  - If $gcd(m, n) = 1$, then
  $$m^{p_i^k - p_i^{k-1}+1} \equiv \ m \, (mod \, p_i^k).$$
  - If $p_i | m$, then
  $$m^{p_i^k - p_i^{k-1}+1} \equiv \ m^{l \, k + r} \equiv \ m^{l \, k} \, m^r \equiv 0 \, (mod \, p_i^k) \neq m \, (mod \, p_i^k),$$
  where $p_i^k - p_i^{k-1} + 1 = l \, k + r$.

– Therefore,

$$m^{k_i(p_i^k - p_i^{k-1})+k} \equiv m^k \,(mod\, p_i^k),\ \ \forall m \in \mathbb{N},$$

we can say that if $n = \Pi_{i=1}^{N} p_i^{n_i}$ and $K = \max_i\{n_i\}$, then

$$m^{k_i(p_i^k - p_i^{k-1})+K} \equiv m^K \,(mod\, p_i^{n_i}),\ \ \forall m \in \mathbb{N},\ \ \forall k_i \in \mathbb{N}.$$

□

Proposition 2.

$$\lambda(p_1^{n_1}\, p_2^{n_2-1}) = \frac{(p_1^{n_1} - p_1^{n_1-1})(p_2^{n_2} - p_2^{n_2-1})}{gcd\left(p_1^{n_1} - p_1^{n_1-1}\,;\, p_2^{n_2} - p_2^{n_2-1}\right)}, \tag{7}$$

and

$$\lambda(\Pi_{j=1}^{i} p_j^{n_j}) = \frac{\lambda(\Pi_{j=1}^{i-1} p_j^{n_j})(p_i^{n_i} - p_i^{n_i-1})}{gcd\left(\lambda(\Pi_{j=1}^{i-1} p_j^{n_j})\,;\, p_i^{n_i} - p_i^{n_i-1}\right)}. \tag{8}$$

Proof. The proof will be given after Lemma 5. □

Lemma 3.

$$\lambda(\Pi_{j=1}^{i} p_j^{n_j}) = \left(p_1^{n_1} - p_1^{n_1-1}\right) LCM\left(\left\{\frac{p_k^{n_k} - p_k^{n_k-1}}{gcd(p_k^{n_k} - p_k^{n_k-1}\,;\, p_1^{n_1} - p_1^{n_1-1})} \,:\, 2 \le k \le i.\right\}\right) \tag{9}$$

Proof. According to the definition of λ:

$$\begin{aligned}\lambda(\Pi_{j=1}^{i} p_j^{n_j}) &:= \min\left\{k_1(p_1^{n_1} - p_1^{n_1-1}) \,:\, \exists\, k_j,\ k_1(p_1^{n_1} - p_1^{n_1-1}) = k_j(p_j^{n_j} - p_j^{n_j-1}),\ 2 \le j \le i.\right\}\\ &:= \min\left\{k_1(p_1^{n_1} - p_1^{n_1-1}) \,:\, \forall 2 \le j \le i \,:\, k_j,\ (p_j^{n_j} - p_j^{n_j-1}) \middle| k_1(p_1^{n_1} - p_1^{n_1-1})\right\}\end{aligned}$$

and using the fact that

$$If\ a \middle| bc \iff \frac{a}{gcd(a,b)} \middle| c,$$

we obtain

$$\lambda(\Pi_{j=1}^{i} p_j^{n_j}) = \min\left\{k_1(p_1^{n_1} - p_1^{n_1-1}) \,:\, \forall\, 2 \le j \le i,\ \frac{p_j^{n_j} - p_j^{n_j-1}}{gcd(p_j^{n_j} - p_j^{n_j-1}\,;\, p_1^{n_1} - p_1^{n_1-1})} \middle|\, k_1\right\},$$

and the smallest k_1 satisfying the above relation is the least common multiple (LCM) of $\dfrac{p_j^{n_j} - p_j^{n_j-1}}{gcd(p_j^{n_j} - p_j^{n_j-1}\,;\, p_1^{n_1} - p_1^{n_1-1})}$, which completes the proof. □

Lemma 4.

$$\lambda(\Pi_{j=1}^{i+1} p_j^{n_j}) = \lambda(\Pi_{j=1}^{i} p_j^{n_j}) \times \frac{p_{i+1}^{n_{i+1}} - p_{i+1}^{n_{i+1}-1}}{gcd(p_{i+1}^{n_{i+1}} - p_{i+1}^{n_{i+1}-1}\,;\, p_1^{n_1} - p_1^{n_1-1}) \times gcd(A_{i+1}\,;\, B_1)} \tag{10}$$

where

$$A_{i+1} = \frac{p_{i+1}^{n_{i+1}} - p_{i+1}^{n_{i+1}-1}}{gcd(p_{i+1}^{n_{i+1}} - p_{i+1}^{n_{i+1}-1}\,;\, p_1^{n_1} - p_1^{n_1-1})}, \quad B_1 = \frac{\lambda(\Pi_{j=1}^{i} p_j^{n_j})}{p_1^{n_1} - p_1^{n_1-1}}.$$

Proof. We will use the following two results:

$$LCM(a_1, \cdots, a_{i+1}) = LCM(LCM(a_1, \cdots, a_i),\ a_{i+1}), \tag{11}$$

and

$$LCM(a, b) = \frac{a\,b}{gcd(x, y)}. \tag{12}$$

According to Lemma 3 and (11), we have by setting
$d_j = gcd(p_j^{n_j} - p_j^{n_j-1}\ ;\ p_1^{n_1} - p_1^{n_1-1})$:

$$\lambda(\Pi_{j=1}^{i+1} p_j^{n_j}) = \left(p_1^{n_1} - p_1^{n_1-1}\right) LCM\left(LCM\left[\left\{\frac{p_j^{n_j} - p_j^{n_j-1}}{d_j}\ :\ 2 \le j \le i.\right\}\right]\ ;\ A_{i+1}\right)$$

which is equivalent to

$$\lambda(\Pi_{j=1}^{i+1} p_j^{n_j}) = \left(p_1^{n_1} - p_1^{n_1-1}\right) LCM\left(\frac{\lambda(\Pi_{j=1}^{i} p_j^{n_j})}{p_1^{n_1} - p_1^{n_1-1}}\ ;\ A_{i+1}\right).$$

Furthermore, according to (12), we obtain:

$$\lambda(\Pi_{j=1}^{i+1} p_j^{n_j}) = \frac{\lambda(\Pi_{j=1}^{i} p_j^{n_j}) \times A_{i+1}}{gcd\left(\frac{\lambda(\Pi_{j=1}^{i} p_j^{n_j})}{p_1^{n_1} - p_1^{n_1-1}}\ ;\ A_{i+1}\right)},$$

which proves Lemma 4. □

Lemma 5.

$$gcd(z\ ;\ x\,y) = gcd(z\ ;\ x)\ gcd\left(\frac{z}{gcd(z\ ;\ x)}\ ;\ y\right). \tag{13}$$

Proof. Let $d = gcd(z; x)$, then $z = d\,c$ and $x = d\,a$ where $gcd(a, c) = 1$. Thus

$$gcd(z; x\,y) = gcd(d\,c\,; d\,a\,y) = d\,gcd(c\,;\,a\,y) = d \times gcd(c\,;\,y) = gcd(z\,;\,x)\,gcd\left(\frac{z}{gcd(z\,;\,x)}\ ;\ y\right).$$

□

Proof of Proposition 2. By applying Lemma 5 to the denominator of the expression in Lemma 4, with $x = p_1^{n_1} - p_1^{n_1-1}$, $y = B_i$ and $z = p_{i+1}^{n_{i+1}} - p_{i+1}^{n_{i+1}-1}$ we will obtain:

$$\lambda(\Pi_{j=1}^{i+1} p_j^{n_j}) = \frac{\lambda(\Pi_{j=1}^{i} p_j^{n_j})\left(p_{i+1}^{n_{i+1}} - p_{i+1}^{n_{i+1}-1}\right)}{gcd\left(p_{i+1}^{n_{i+1}} - p_{i+1}^{n_{i+1}-1}\ ;\ \lambda(\Pi_{j=1}^{i} p_j^{n_j})\right)}.$$

The Carmichael and Euler functions are a very important theoretic functions having a deep relationship with prime numbers. Figures 1 and 2 shows the first thousand values of $\lambda(n)$ and $\varphi(n)$, respectively, where the Euler function has been defined as $\varphi(n) = (p_1^{n_1} - p_1^{n_1-1}).\cdots.(p_k^{n_k} - p_k^{n_k-1})$, where $p_1^{n_1}.\cdots.p_k^{n_k}$ is the prime factorization of the integer n. □

3. Properties of $\lambda(.)$

In this section, we present some properties of the new Totient function $\lambda(.)$.

1.

$$\forall k \in \mathbb{N},\ \forall\ \text{prime}\ p\ :\ \lambda(p^k) = \varphi(p^k) = p^k - p^{k-1}.$$

2. If $n = 2\,\Pi_{i=1}^{k}\, p_i^{k_i},\ p_i$ are odd primes and k is any positive integer, then

$$\lambda(n) = \lambda(n/2).$$

3. If $n = 2\,p$, where p is an odd prime, then $\lambda(2\,p) = \varphi(p)$;
4. If $n = 2^k,\ k > 2$, then $\lambda(2^k) = \varphi(2^k)/2$.
5. If $n > 5$ then $\lambda(n)$ is an even number.
6. If p and q are two odd primes, and k and l are any natural numbers, then

$$\lambda(p^k\,q^l) \leq \frac{1}{2}\,\varphi(p^k\,q^l).$$

7. If $m,\ p$, and q are three odd primes, and $k,\ l$ and s are any natural numbers, then

$$\lambda(m^k\,p^l\,q^r) \leq \frac{1}{4}\,\varphi(m^k\,p^l\,q^r).$$

8. Let $(p_i)_i$ be an increasing sequence of primes, then:

$$\lambda\left(\prod_{i=1}^{k}\, p_i^{n_i}\right) = \frac{\lambda\left(\prod_{i=1}^{k-1}\, p_i^{n_i}\right)\left(p_k^{n_k} - p_k^{n_k-1}\right)}{gcd\left[\lambda\left(\prod_{i=1}^{k-1}\, p_i^{n_i}\right),\ p_k - 1\right]}.$$

9.

$$\lambda\left(\prod_{i=1}^{k}\, p_i^{n_i}\right) = \frac{\lambda\left(\prod_{j=1,\,j\neq i}^{k}\, p_j^{n_j}\right)\left(p_i^{n_i} - p_i^{n_i-1}\right)}{gcd\left[\lambda\left(\prod_{j=1,\,j\neq i}^{k}\, p_j^{n_j}\right),\ p_i^{n_i} - p_i^{n_i-1}\right]}.$$

Proof.

1. From the definition of the function $\lambda(n)$, we can conclude the following:

$$\forall\, k \in \mathbb{N},\ \forall\, \text{prime}\, p\ :\ \lambda(p^k) = \varphi(p^k) = p^k - p^{k-1}.$$

2. If $n = 2\Pi_{i=1}^{k}\, p_i^{k_i},\ p_i$ are primes and k is any integer, then $\lambda(n) = \lambda(n/2)$. Indeed,

$$\lambda(n) = \frac{\lambda\left(\Pi_{i=1}^{k}\, p_i^{k_i}\right)(2-1)}{GCD\left(\Pi_{i=1}^{k}\, p_i^{k_i},\ 2-1\right)} = \lambda\left(\Pi_{i=1}^{k}\, p_i^{k_i}\right).$$

3. For all odd primes p, we have: $\lambda(2p) = \lambda(p) = p - 1$. Indeed,

$$\begin{array}{rcl} \lambda(2p) & = & \lambda(p)\ \text{(from P2)} \\ & = & \varphi(p)\ \text{(from P1)} \\ & = & p-1\ \text{(from def. of}\ \varphi(p)). \end{array}$$

4. If $n = 2^k,\ k > 2$, then $\lambda(2^k) = \varphi(2^k)/2$.
We note the following

$$m^{2^k-2^{k-1}} - 1 = (m^{2^{k-2}-2^{k-3}} - 1)(m^{2^{k-2}-2^{k-3}} + 1)(m^{2^{k-1}-2^{k-2}} + 1).$$

Therefore, for any odd number m, we have

$$\left(m^{2^{k-2}-2^{k-3}} - 1\right)\left(m^{2^{k-2}-2^{k-3}} + 1\right) \equiv 0\ (\ mod(2^3)\ ).$$

If $k > 3$, we can factor more the term

$$m^{2^k-2^{k-1}} - 1 = (x^4+1)(x^2+1)(x+1)(x-1), \;\; x = m^{2^{k-3}-2^{k-4}}.$$

By the Euler theorem, we have $m^{2^k-2^{k-1}} - 1 \equiv 0 \; (\, mod(2^5)\,)$.
By induction, we can easily prove that for any odd integer m and for all integer $k > 2$ the following statement is true:

$$m^{2^{k-1}-2^{k-2}} - 1 = 0 \; (\, mod(2^k)\,).$$

Thus,

$$\lambda(2^k) = 2^{k-1} - 2^{k-2} = \varphi(2^k)/2.$$

5. For $n > 5$, we have the following:
   - $\lambda(3) = 2, \;\; \lambda(2) = 1.$
   - $\lambda(4) = 2^{2-1}(2-1) = 2.$
   - $\lambda(5) = 4.$
   - $\lambda(p) = p - 1$, which is even for any odd prime p.
   - $\lambda(p^k) = p^{k-1}(p-1)$, which is even for any odd prime p.
   -
   $$\begin{aligned} \lambda\left(p_1^{k_1}\, p_2^{k_2}\right) &= \frac{\lambda(p_1^{k_1})\,(p_2^{k_2} - p_2^{k_2-1}}{GCD\left(\lambda(p_1^{k_1}),\; p_2^{k_2} - p_2^{k_2-1}\right)} \\ &= \frac{p_1^{k_1-1}(p_1-1)\; p_2^{k_2-1}(p_2-1)}{GCD\left(p_1^{k_1-1}(p_1-1),\; p_2^{k_2-1}(p_2-1)\right)} \end{aligned}$$

     (a) For some integer l, if 2^l divides $GCD\left(p_1^{k_1-1}(p_1-1),\; p_2^{k_2-1}(p_2-1)\right)$, then $2^l \left| p_2^{k_2-1}(p_2-1)\right.$.
     (b) $p_1 - 1$ is an even number.

     (a) and (b) imply that $\lambda\left(p_1^{k_1}\, p_2^{k_2}\right)$ is even.

6. According to Lemma 3, we have:

$$\begin{aligned} \lambda\left(p^k\, q^l\right) &= \frac{\lambda(p^k)\,(q^l - q^{l-1})}{GCD\left(\lambda(p^k),\; q^l - q^{l-1}\right)} \\ &\leq \frac{\lambda(p^k)\,(q^l - q^{l-1})}{2}, \quad \text{Property 5.} \\ &\leq \frac{\varphi\left(p^k\, q^l\right)}{2}, \quad \text{Property 1.} \end{aligned}$$

7. According to Lemma 3, we have:

$$\begin{aligned} \lambda\left(m^k\, p^r\, q^s\right) &= \frac{\lambda(m^k\, p^r)\,(q^s - q^{s-1})}{GCD\left(\lambda(m^k\, p^r),\; q^s - q^{s-1}\right)} \\ &\leq \frac{\lambda(m^k\, p^r)\,(q^s - q^{s-1})}{2}, \quad \text{Property 5.} \\ &\leq \frac{\varphi(m^k\, p^r)\,(q^s - q^{s-1})}{4}, \quad \text{Property 6.} \\ &\leq \frac{\varphi(m^k\, p^r\, q^s)}{4}. \end{aligned}$$

8. Obvious, it is enough to prove that $gcd\left[\lambda\left(\prod_{i=1}^{k-1} p_i^{n_i}\right),\ p_k\right] = 1$.
9. Obvious.

□

Corollary 1.

$$\lambda\left(\prod_{i=1}^{k} p_i^{n_i}\right) \leq \frac{1}{2^{k-1}}\,\varphi\left(\prod_{i=1}^{k} p_i^{n_i}\right).$$

Proof. From properties P6 and P7, the proof can be completed by induction.
As a conclusion, we can easily prove the following limit

$$\limsup_{n\to\infty} \frac{\varphi(n)}{\lambda(n)} = +\infty,$$

by considering the subsequence $n_k = p_1.p_2.\cdots.p_k$, where $(p_1, p_2, \ldots, p_k)$ are the first k-consecutive odd primes.

Again, since the primes are not bounded, we can conclude that

$$\liminf_{n\to\infty} \frac{\varphi(n)}{\lambda(n)} = 1.$$

□

4. Computations of $\lambda(n)$ versus $\varphi(n)$

In this section, we compare the magnitude of the Euler function $\varphi(n)$ versus the Carmichael function $\lambda(n)$ see Tables 1 and 2.

Figures 3 and 4 present, respectively, the ratio $\frac{\varphi(n)}{\lambda(n)}$ when n is a product of two primes, respectively, three primes.

Table 1. Comparison between Carmichael and Euler functions for the product of two primes.

n	3×5	5×7	5×29	5×61	11×31	17×97	37×73	73×109
$\lambda(n)$	4	12	28	60	30	96	72	216
$\frac{\varphi(n)}{\lambda(n)}$	2	2	4	4	10	16	36	36

Table 2. Comparison between Carmichael and Euler functions for the product of three primes.

n	$3\times5\times7$	$5\times13\times97$	$7\times31\times61$	$11\times31\times71$	$13\times19\times113$	$37\times73\times109$
$\lambda(n)$	12	96	60	210	108	216
$\frac{\varphi(n)}{\lambda(n)}$	4	48	180	100	216	1296

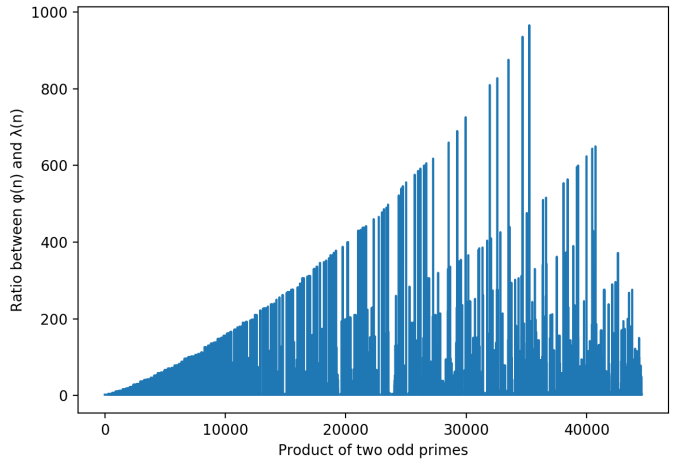

Figure 3. The Ratio between Carmichael and Euler functions for n less than 45,000.

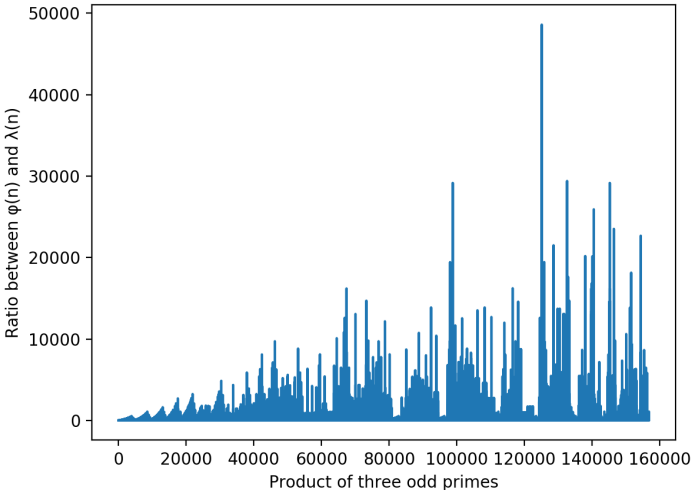

Figure 4. The Ratio between Carmichael and Euler functions for n less than 155,000.

5. Conclusions

In this paper, we presented how we built the modified Totient function of Carmichael $\lambda(.)$. Important properties have been highlighted, particularly the given iterative scheme for calculating the $\lambda(.)$ function. Some preliminary numerical results comparing the Euler φ and the reduced totient $\lambda(.)$ functions aiming to quantify the reduction between them are given (see Tables 1 and 2 and Figures 3–5). Figures 6 and 7 express the frequency of n for getting the value of $\lambda(n)$; in other words, determining the cardinal of the following set:

$$\{n \ : \ \lambda(n) = k\}, \ k \text{ is a given positive integer.}$$

Furthermore, it may be worthwhile investigating more results in Corollary 1 by finding a better upper-bound.

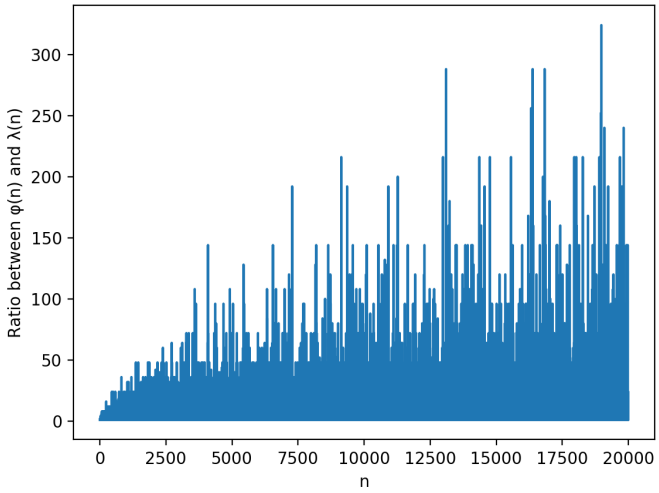

Figure 5. $\frac{\varphi(n)}{\lambda(n)}$ for all $n \leq 20{,}000$.

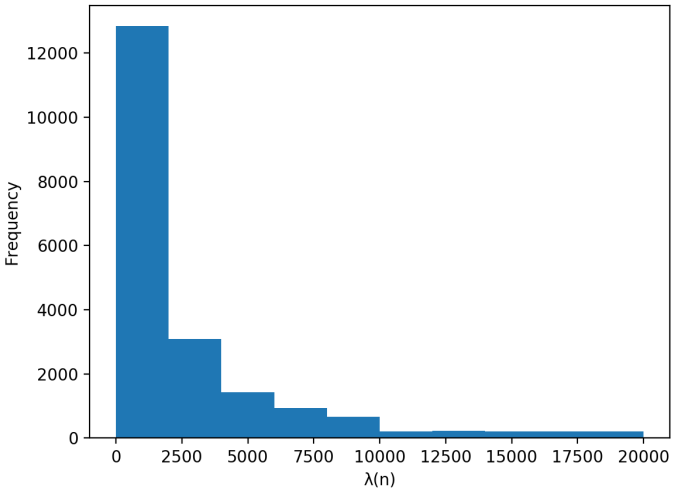

Figure 6. The Cardinal of the Inverse of Carmichael function.

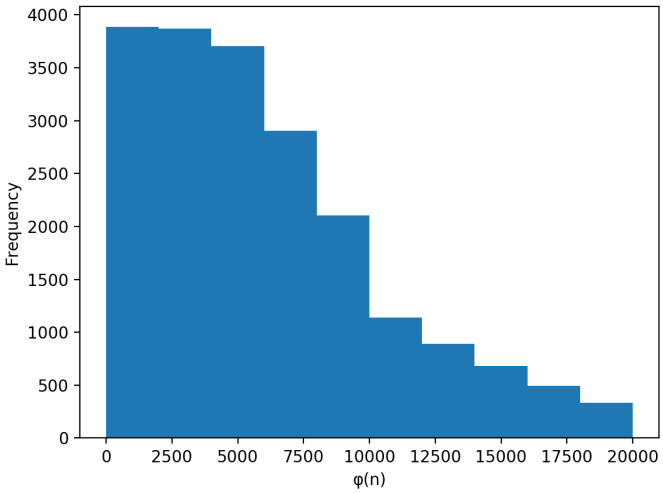

Figure 7. The Cardinal of the Inverse of Euler function.

Author Contributions: Conceptualization, S.B.B. and A.H.; methodology, Y.H.; validation, S.B.B. and Y.H.; formal analysis, A.H.; investigation, S.B.B.; writing—original draft preparation, A.H.; writing—review and editing, S.B.B. and A.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: The publication of this article was funded by the Qatar National Library.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Carmichael, R.D. On composite numbers p which satisfy the Fermat congruence $a^{p-1} \equiv 1 \, mod(p)$. *Am. Math. Mon.* **1912**, *19*, 22–27.
2. Erdős, P.; Pomerance, C.; Schmutz, E. Carmichael's lambda function. *Acta Arith.* **1991**, *58*, 363–385. [CrossRef]
3. Padberg, F. *Elementare Zahlentheorie*; Spektrum Akademischer Verlag: Heidelberg/Berlin, Germany, 1996.
4. Riesel, H. *Prime Numbers and Computer Methods for Factorization*; Birkhäuser Boston: Basel, Switzerland; Berlin, Germany, 1994.
5. Contini, S.; Croot, E.; Shparlinski, I.E. Complexity of Inversing the Euler Function. *Math. Comput.* **2006**, *75*, 983–996. [CrossRef]
6. Ford, K.; Hu, Y.Y. Divisors of the Euler and Carmichael functions. *Acta Arith.* **2007**, *133*. [CrossRef]
7. Ge, Y. A Note on the Carmichael Function. Available online: https://www.math.sinica.edu.tw/www/file_upload/summer/crypt2017/data/2015/[20150707][carmichael].pdf (accessed on 1 May 2021).