THE ARITHMETIC OF CARMICHAEL QUOTIENTS

MIN SHA

ABSTRACT. Carmichael quotients for an integer $m \geq 2$ are introduced analogous to Fermat quotients, by using Carmichael function $\lambda(m)$. Various properties of these new quotients are investigated, such as basic arithmetic properties, sequences derived from Carmichael quotients, Carmichael-Wieferich numbers, and so on. Finally, we link Carmichael quotients to perfect nonlinear functions.

1. INTRODUCTION

Let p be a prime and a an integer not divisible by p, by Fermat's little theorem, the *Fermat quotient* of p with base a is defined as follows

$$Q_p(a) = \frac{a^{p-1} - 1}{p}.$$

Moreover, if $Q_p(a) \equiv 0 \pmod{p}$, then we call p a Wieferich prime with base a.

This quotient has been extensively studied from various aspects because of its numerous applications in number theory and computer science; see, for example, [7, 8, 9, 11, 16, 17]. A first comprehensive study of Fermat quotient was published in 1905 by Lerch [12], which was based on the viewpoint of arithmetic. More arithmetic properties were investigated in [3].

In [4], the authors generalized the definition of Fermat quotient by using Euler's theorem. Let $m \ge 2$ and a be relatively prime integers, the *Euler quotient* of m with base a is defined as follows

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

where φ is Euler's totient function. Moreover, if $Q_m(a) \equiv 0 \pmod{m}$, then we call *m* a *Wieferich number* with base *a*. They also undertook a very careful study of Euler quotients.

²⁰¹⁰ Mathematics Subject Classification. 11A25, 11B50, 11A07.

Key words and phrases. Carmichael function, Carmichael quotient, Carmichael-Wieferich number, perfect nonlinear function.

In fact, there are some other generalizations of Fermat quotients, see [1, 18, 19]. Especially, in [1] the author introduced a quotient like $(a^e - 1)/m$, where gcd(a, m) = 1 and e is the multiplicative order of a modulo m.

In this paper, we introduce a different generalization of Fermat quotient by using Carmichael function and study its arithmetic properties.

For a positive integer m, the Carmichael function $\lambda(m)$ is defined to be the exponent of the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^*$. More explicitly, $\lambda(1) = 1$; for a prime power p^r we define

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

and

 $\lambda(m) = \operatorname{lcm}(\lambda(p_1^{r_1}), \lambda(p_2^{r_2}), \cdots, \lambda(p_k^{r_k})),$

where, as usual, "lcm" means the least common multiple, and $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ is the prime factorization of m.

For every positive integer m, we have $\lambda(m)|\varphi(m)$, and $\lambda(m) = \varphi(m)$ if and only if $m \in \{1, 2, 4, p^k, 2p^k\}$, where p is an odd prime and $k \ge 1$. In addition, if m|n, we have $\lambda(m)|\lambda(n)$.

Definition 1.1. Let $m \ge 2$ and a be relatively prime integers. The quotient

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

is called the *Carmichael quotient* of m with base a. Moreover, if $C_m(a) \equiv 0 \pmod{m}$, we call m a *Carmichael-Wieferich number* with base a.

We want to indicate that the term "Carmichael quotient" was introduced in [2] to denote a different quotient, and we think that there is no much danger of confusion.

We extend many known results about Fermat quotients or Euler quotients to Carmichael quotients by using the same techniques, such as basic arithmetic properties with special emphasis on congruences, the least periods of sequences derived from Carmichael quotient, Carmichael-Wieferich numbers. Finally, we link Carmichael quotients to perfect nonlinear functions.

2. Arithmetic of Carmichael Quotients

In what follows, we fix $m \geq 2$ an integer unless stated otherwise.

In this section, we study some basic arithmetic properties of Carmichael quotients and extend some results about Fermat quotients or Euler quotients in [4, 12, 13]. See [4] for historical literatures.

For any integer a with gcd(a, m) = 1, we have $C_m(a)|Q_m(a)$. In particular, $C_m(a) = Q_m(a)$ when m is an odd prime power. Furthermore, it is straightforward to prove that they have the following relation.

Proposition 2.1. For any integer a with gcd(a, m) = 1, we have

$$Q_m(a) \equiv \frac{\varphi(m)}{\lambda(m)} \cdot C_m(a) \pmod{m}.$$

Proof. Since $\lambda(m)|\varphi(m)$, we derive

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

= $\frac{(a^{\lambda(m)} - 1) (1 + a^{\lambda(m)} + \dots + (a^{\lambda(m)})^{\varphi(m)/\lambda(m)-1})}{m}$
= $\frac{\varphi(m)}{\lambda(m)} C_m(a) \pmod{m}.$

Now we state two fundamental congruences for Carmichael quotients, which are crucial for further study.

Proposition 2.2. (1) If a and b are integers with gcd(ab, m) = 1, then we have

$$C_m(ab) \equiv C_m(a) + C_m(b) \pmod{m}.$$

(2) If a, k are integers with gcd(a, m) = 1, and α is a positive integer, then we have

$$C_m(a + km^{\alpha}) \equiv C_m(a) + \frac{k\lambda(m)}{a}m^{\alpha-1} \pmod{m^{\alpha}}.$$

Proof. (1) We only need to notice that

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

= $\frac{(a^{\lambda(m)} - 1)(b^{\lambda(m)} - 1) + (a^{\lambda(m)} - 1) + (b^{\lambda(m)} - 1)}{m}$.

(2) Using the binomial expansion, it is easy to see that

$$C_m(a+km^{\alpha}) \equiv \frac{a^{\lambda(m)} + \lambda(m)a^{\lambda(m)-1}km^{\alpha} - 1}{m} \pmod{m^{\alpha}},$$

which implies the desired congruence.

The following two corollaries concern some short sums of Carmichael quotients.

Corollary 2.3. If $m \ge 3$, for any integer a with gcd(a,m) = 1, we have

$$\sum_{k=0}^{m-1} C_m(a+km) \equiv 0 \pmod{m}.$$

Proof. First applying Proposition 2.2 (2) and then noticing that $\lambda(m)$ is even when $m \geq 3$, we obtain

$$\sum_{k=0}^{m-1} C_m(a+km) \equiv \frac{\lambda(m)}{a} \cdot \frac{m(m-1)}{2} \equiv 0 \pmod{m}.$$

Corollary 2.4. If $m \ge 3$, for any integer a with gcd(a,m) = 1, we have

$$\sum_{\substack{a=1\\\gcd(a,m)=1}}^{m^2} C_m(a) \equiv 0 \pmod{m}.$$

Proof. Notice that

$$\sum_{\substack{a=1\\\gcd(a,m)=1}}^{m^2} C_m(a) = \sum_{\substack{a=1\\\gcd(a,m)=1}}^m \sum_{k=0}^{m-1} C_m(a+km).$$

Then, the desired result follows from Corollary 2.3.

We want to remark that the results in Corollaries 2.3 and 2.4 are not true when m = 2.

The next proposition concerns some relationships between various $C_m(a)$ with fixed base a and different moduli.

Proposition 2.5. (1) If gcd(a, mn) = 1, then

$$C_m(a)|nC_{mn}(a).$$

(2) If gcd(a, mn) = gcd(m, n) = 1, then

$$C_{mn}(a) \equiv \frac{\lambda(n)}{n \cdot \gcd(\lambda(m), \lambda(n))} C_m(a) \pmod{m}.$$

(3) Assume that gcd(a, mn) = gcd(m, n) = 1, and let X and Y be two integers satisfying $m^2X + n^2Y = 1$. Then

$$C_{mn}(a) \equiv \frac{n\lambda(n)}{\gcd(\lambda(m),\lambda(n))} Y C_m(a) + \frac{m\lambda(m)}{\gcd(\lambda(m),\lambda(n))} X C_n(a) \pmod{mn}.$$

Proof. (2) Under the assumption, noticing that $\lambda(mn) = \frac{\lambda(m)\lambda(n)}{\gcd(\lambda(m),\lambda(n))}$, we have

$$C_{mn}(a) = \frac{a^{\frac{\lambda(m)\lambda(n)}{\gcd(\lambda(m),\lambda(n))} - 1}}{mn} = \frac{(a^{\lambda(m)})^{\frac{\lambda(n)}{\gcd(\lambda(m),\lambda(n))} - 1}}{\frac{\lambda(n)(a^{\lambda(m)} - 1)}{mn \cdot \gcd(\lambda(m),\lambda(n))}} (\text{mod } m)$$

(3) It suffices to show that the equality is true for modulo m and modulo n respectively. But this follows directly from (2).

For any integer a with gcd(a, m) = 1, we denote $\langle a \rangle$ as the subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$ generated by a, and we let $ord_m a$ be the multiplicative order of a modulo m. The following expression is so-called Lerch's expression [13].

Proposition 2.6. If gcd(a, m) = 1 and assume $n = ord_m a$, then

$$C_m(a) \equiv \frac{\lambda(m)}{n} \sum_{\substack{r=1\\r \in \langle a \rangle}}^m \frac{1}{ar} \left\lfloor \frac{ar}{m} \right\rfloor \pmod{m},$$

where $\lfloor x \rfloor$ denotes the greatest integer $\leq x$.

Proof. For each $1 \leq r \leq m$ with $r \in \langle a \rangle$, we write $ar \equiv c_r \pmod{m}$, with $1 \leq c_r \leq m$. Notice that when r runs through all elements with $1 \leq r \leq m$ and $r \in \langle a \rangle$, so does c_r . Let P denote the product of all such integers c_r . If the products and sums below are understood to be taken over all r with $1 \leq r \leq m$ and $r \in \langle a \rangle$, we have

$$P^{\frac{\lambda(m)}{n}} = \prod c_r^{\frac{\lambda(m)}{n}} = \prod \left(ar - m \left\lfloor \frac{ar}{m} \right\rfloor\right)^{\frac{\lambda(m)}{n}} = a^{\lambda(m)} P^{\frac{\lambda(m)}{n}} \prod \left(1 - \frac{m}{ar} \left\lfloor \frac{ar}{m} \right\rfloor\right)^{\frac{\lambda(m)}{n}}.$$
So

$$1 = a^{\lambda(m)} \prod \left(1 - \frac{m}{ar} \left\lfloor \frac{ar}{m} \right\rfloor \right)^{\frac{\lambda(m)}{n}} \equiv a^{\lambda(m)} \left(1 - m \sum \frac{1}{ar} \left\lfloor \frac{ar}{m} \right\rfloor \right)^{\frac{\lambda(m)}{n}} \pmod{m^2}.$$

Then we get

$$a^{\lambda(m)} - 1 \equiv a^{\lambda(m)} \frac{m\lambda(m)}{n} \sum_{\substack{r=1\\r\in\langle a\rangle}}^{m} \frac{1}{ar} \left\lfloor \frac{ar}{m} \right\rfloor \pmod{m^2},$$

which implies the desired congruence.

In the last part of this section, we describe the decomposition of Carmichael quotients in the dependence of the prime factorization of the modulus. Further we investigate Carmichael quotients for prime power moduli.

Proposition 2.7. Let $m = p_1^{r_1} \cdots p_k^{r_k}$ be the prime factorization of m, and let a be an integer with gcd(a,m) = 1. For $1 \le i \le k$, let $d_i = \lambda(m)/\lambda(p_i^{r_i}), m_i = m/p_i^{r_i}$ and $m'_i \in \mathbb{Z}$ such that $m_i^2 m'_i \equiv 1 \pmod{r_i}$ $p_i^{r_i}$). Then

$$C_m(a) \equiv \sum_{i=1}^k m_i m'_i d_i C_{p_i^{r_i}}(a) \pmod{m}.$$

Proof. It suffices to prove for each $1 \le j \le k$,

$$C_m(a) \equiv \sum_{i=1}^k m_i m'_i d_i C_{p_i^{r_i}}(a) \pmod{p_j^{r_j}},$$

that is

$$C_m(a) \equiv m_j m'_j d_j C_{p_j^{r_j}}(a) \pmod{p_j^{r_j}}.$$

Since we have

$$C_m(a) = \frac{a^{\lambda(p_j^{r_j})d_j} - 1}{m} \equiv \frac{d_j(a^{\lambda(p_j^{r_j})} - 1)}{m} \equiv m_j m'_j d_j C_{p_j^{r_j}}(a) \pmod{p_j^{r_j}},$$

the result follows.

the result follows.

Proposition 2.8. Let p be an odd prime and gcd(a, p) = 1. For any two integers i and j with $1 \leq i \leq j$, we have

$$C_{p^j}(a) \equiv C_{p^i}(a) \pmod{p^i}.$$

Besides, for $3 \leq i \leq j$ and gcd(a, 2) = 1, we have

$$C_{2^{j}}(a) \equiv C_{2^{i}}(a) \pmod{2^{i-1}}.$$

Proof. Notice that $C_{p^i}(a) = Q_{p^i}(a)$ if p is an odd prime. By [4, Proposition 4.1], for any integer $k \ge 1$, we have

$$C_{p^{k+1}}(a) \equiv C_{p^k}(a) \pmod{p^k}.$$

Then the first formula follows.

Since for $r \geq 3$, we have

$$C_{2^{r+1}}(a) - C_{2^r}(a) \equiv \frac{a^{2^{r-2}} - 1}{2} C_{2^r}(a) \pmod{2^r}$$

$$\equiv 0 \pmod{2^{r-1}},$$

we get the second formula.

The following corollary, about the relation between Carmichael quotients and Fermat quotients, can be obtained directly from the above two propositions.

Corollary 2.9. Suppose that p is an odd prime factor of m, and p^{α} is the largest power of p dividing m. Let $d_1 = \frac{\lambda(m)}{\lambda(p^{\alpha})}$, $m_1 = m/p^{\alpha}$, and $m'_1 \in \mathbb{Z}$ such that $m_1^2 m'_1 \equiv 1 \pmod{p^{\alpha}}$. Then for any integer a with gcd(a,m) = 1, we have

$$C_m(a) \equiv m_1 m'_1 d_1 Q_p(a) \pmod{p}.$$

3. Sequences derived from Carmichael Quotients

In this section, we will define two periodic sequences by Carmichael quotients and determine their least (positive) periods following the method in the proof of [10, Proposition 2.1].

As usual, for a periodic sequence $\{s_n\}_{n=1}^{\infty}$, a positive integer j is called its *period* if $s_{n+j} = s_n$ for any $n \ge 1$; if further j is the smallest positive integer endowed with such property, we call j the *least period* of $\{s_n\}$.

Let $m = p_1^{r_1} \cdots p_k^{r_k}$ be the prime factorization of the integer m ($m \ge 2$). For each $1 \le i \le k$, put $m_i = m/p_i^{r_i}$, and let w_i be the integer defined by $p_i^{w_i} = \gcd(\lambda(m)/\lambda(p_i^{r_i}), p_i^{r_i})$, here note that $0 \le w_i \le r_i$.

Now, we want to define a sequence $\{a_n\}$ following the manner in [10].

First, for any integer n and any $1 \leq i \leq k$, if $p_i|n$, set $C_{p_i^{r_i}}(n) = 0$. Then, for every integer $n \geq 1$, by Proposition 2.7, a_n is defined as the unique integer with

$$a_n \equiv \sum_{i=1}^k \frac{m_i m'_i \lambda(m)}{\lambda(p_i^{r_i})} C_{p_i^{r_i}}(n) \pmod{m}, \qquad 0 \le a_n \le m - 1,$$

where $m'_i \in \mathbb{Z}$ is such that $m_i^2 m'_i \equiv 1 \pmod{p_i^{r_i}}$ for each $1 \leq i \leq k$. So, if gcd(n,m) = 1, we have $a_n \equiv C_m(n) \pmod{m}$.

By Proposition 2.2 (2), m^2 is a period of $\{a_n\}$. We denote its least period by T. For each $1 \leq i \leq k$, let T_i be the least period of the sequence $\{a_n \mod p_i^{r_i}\}$. Obviously, we have

$$T = \operatorname{lcm}(T_1, \cdots, T_k).$$

Thus, in order to determine T, it suffices to compute T_i for each $1 \leq i \leq k$.

For every $1 \le i \le k$, we have

(3.1)
$$a_n \equiv \frac{\lambda(m)}{m_i \lambda(p_i^{r_i})} C_{p_i^{r_i}}(n) \pmod{p_i^{r_i}}.$$

So, T_i equals to the least period of $\{C_{p_i^{r_i}}(n) \mod p_i^{r_i-w_i}\}$. Here, we also denote T_i as the least period of the sequence $\{C_{p_i^{r_i}}(n) \mod p_i^{r_i-w_i}\}$ without confusion. In the sequel, we will calculate T_i case by case for any fixed $1 \le i \le k$.

Lemma 3.1. If $w_i = r_i$, then $T_i = 1$.

Proof. Since in this case we have $C_{p_i^{r_i}}(n) \equiv 0 \pmod{p_i^{r_i-w_i}}$ for all $n \ge 1.$

Lemma 3.2. If $p_i > 2$ and $w_i < r_i$, then $T_i = p_i^{r_i - w_i + 1}$.

Proof. Combining Proposition 2.2 (2) with Proposition 2.8, for integers n and ℓ with $gcd(n, p_i) = 1$, we have

$$\begin{split} C_{p_i^{r_i}}(n+\ell p_i^{r_i-w_i}) &\equiv C_{p_i^{r_i-w_i}}(n+\ell p_i^{r_i-w_i}) \\ &\equiv C_{p_i^{r_i-w_i}}(n) + \ell n^{-1}(p_i-1)p_i^{r_i-w_i-1} \\ &\equiv C_{p_i^{r_i}}(n) + \ell n^{-1}(p_i-1)p_i^{r_i-w_i-1} \pmod{p_i^{r_i-w_i}}. \end{split}$$

hus, $T_i = p_i^{r_i-w_i+1}$.

T

Now, it remains to consider the case $p_i = 2$.

Lemma 3.3. If $p_i = 2$ and $w_i = 0$, then

$$T_i = \begin{cases} 4 & r_i = 1, \\ 8 & r_i = 2, \\ 2^{r_i + 2} & r_i \ge 3 \end{cases}$$

Proof. Notice that for each n with gcd(n,2) = 1, by Proposition 2.2 (2) we have

$$C_{2^{r_i}}(n+\ell \cdot 2^{r_i}) \equiv C_{2^{r_i}}(n) + \ell n^{-1} \lambda(2^{r_i}) \pmod{2^{r_i}}.$$

Then, the result follows easily.

Lemma 3.4. For $r \geq 3$, the least period of the sequence $\{C_{2^{r+1}}(n)\}$ mod 2^r is 2^{r+2} .

Proof. For $r \ge 3$ and gcd(n,2) = 1, we have $C_{2^{r+1}}(n) = \frac{n^{2^{r-2}}+1}{2}C_{2^r}(n)$. Then using Proposition 2.2 (2), we deduce that

$$C_{2^{r+1}}(n+\ell\cdot 2^r) - C_{2^{r+1}}(n) = \frac{n^{2^{r-2}}+1}{2} \left(C_{2^r}(n+\ell\cdot 2^r) - C_{2^r}(n) \right)$$

$$\equiv \frac{n^{2^{r-2}}+1}{2} \cdot \ell n^{-1} 2^{r-2} \pmod{2^r},$$

which implies the desired result by noticing that $n^{2^{r-2}} \equiv 1 \pmod{2^r}$ and then $\frac{n^{2^{r-2}}+1}{2}$ is odd.

Lemma 3.5. If $p_i = 2$ and $3 \le r_i - w_i < r_i$, then $T_i = 2^{r_i - w_i + 2}$.

Proof. By Proposition 2.8, for gcd(n, 2) = 1, we have

$$C_{2^{r_i}}(n) \equiv C_{2^{r_i-w_i+1}}(n) \pmod{2^{r_i-w_i}}.$$

Then, the result follows directly from Lemma 3.4.

Lemma 3.6. If $p_i = 2$, $r_i \ge 3$ and $1 \le r_i - w_i \le 2$, then $T_i = 2^{r_i - w_i + 2}$.

Proof. From Proposition 2.8, for gcd(n, 2) = 1, we have

$$C_{2^{r_i}}(n) \equiv C_{2^3}(n) \pmod{2^2}.$$

So, T_i equals to the least period of the sequence $\{C_{2^3}(n) \mod 2^{r_i - w_i}\}$. By Proposition 2.2 (2), we have

$$C_{2^3}(n + \ell \cdot 2^3) \equiv C_{2^3}(n) + 2\ell n^{-1} \pmod{2^2},$$

which implies the desired result. In fact, one can also verify this lemma by direct calculations. $\hfill \Box$

Lemma 3.7. If $p_i = 2$, $r_i = 2$ and $w_i = 1$, then $T_i = 1$.

We summarize the above results in the following proposition.

Proposition 3.8. For each $1 \le i \le k$, if p_i is an odd prime, then

$$T_i = \left\{ \begin{array}{ll} 1 & w_i = r_i, \\ p_i^{r_i - w_i + 1} & w_i < r_i; \end{array} \right.$$

otherwise if $p_i = 2$, then

$$T_i = \begin{cases} 1 & w_i = r_i, \\ 4 & r_i = 1, w_i = 0, \\ 8 & r_i = 2, w_i = 0, \\ 1 & r_i = 2, w_i = 1, \\ 2^{r_i - w_i + 2} & r_i \ge 3, w_i < r_i \end{cases}$$

In particular, the least period of $\{a_n\}$ is $T = T_1T_2\cdots T_k$.

When $m = p^r$ with p an odd prime and $r \ge 1$, we have $T = p^{r+1}$, which is consistent with [10, Proposition 2.1]. If $m = 2^r$ with $r \ge 3$, then $T = 2^{r+2}$; but by [10, Proposition 2.1], the least period of the sequence defined there by Euler quotient is 2^{r+1} .

Finally, we want to define a new sequence $\{b_n\}$, which is much simpler but has the same least period as $\{a_n\}$.

For an integer $n \ge 1$ with gcd(n,m) = 1, b_n is defined to be the unique integer with

 $b_n \equiv C_m(n) \pmod{m}, \qquad 0 \le b_n \le m-1;$

and we also define

$$b_n = 0,$$
 if $gcd(n, m) \neq 1.$

Since b_n also satisfies (3.1) for any integer n with gcd(n,m) = 1, the least period of $\{b_n\}$ equals to that of $\{a_n\}$.

Proposition 3.9. The sequence $\{b_n\}$ has the same least period as $\{a_n\}$.

4. CARMICHAEL-WIEFERICH NUMBERS

In this section, except for extending some results in [4], we study Carmichael-Wieferich numbers from more aspects, especially Proposition 4.5.

First, we want to deduce some basic facts for Carmichael-Wieferich numbers.

Proposition 4.1. If $m \ge 3$ and $1 \le a \le m$ with gcd(a, m) = 1, then m cannot be a Carmichael-Wieferich number with bases both a and m-a.

Proof. Notice that $\lambda(m)$ is even when $m \ge 3$. By Proposition 2.2 (2), we have

$$C_m(m-a) \equiv C_m(a) - \frac{\lambda(m)}{a} \pmod{m}.$$

Then, the desired result comes from $\lambda(m) < m$.

Corollary 4.2. If $m \ge 3$, define the set $S_m = \{a : 1 \le a \le m, \gcd(a, m) = 1, m \text{ is a Carmichael-Wieferich number with base } a\}$. Then $|S_m| \le \varphi(m)/2$.

By Proposition 2.2 (2), for any gcd(b, m) = 1, there exists $1 \le a \le m^2$ with $b \equiv a \pmod{m^2}$, such that

$$C_m(b) \equiv C_m(a) \pmod{m}.$$

Hence, if we want to determine with which base m can be a Carmichael-Wieferich number, we only need to consider $1 \le a \le m^2$.

Assume that m has the prime factorization $m = p_1^{r_1} \cdots p_k^{r_k}$. In [4, Proposition 4.4] the authors have used the Euler quotient Q_m to define a homomorphism from $(\mathbb{Z}/m^2\mathbb{Z})^*$ to $(\mathbb{Z}/m\mathbb{Z}, +)$, whose image is $d\mathbb{Z}/m\mathbb{Z}$, where

$$d = \prod_{i=1}^{k} d_i \quad \text{and} \quad d_i = \begin{cases} \gcd(p_i^{r_i}, 2\varphi(m)/\varphi(p_i^{r_i})) & \text{if } p_i = 2 \text{ and } r_i \ge 2, \\ \gcd(p_i^{r_i}, \varphi(m)/\varphi(p_i^{r_i})) & \text{otherwise.} \end{cases}$$

Here, we can do similar things using the Carmichael quotient and applying the same strategy as in [4].

By Proposition 2.2, the Carmichael quotient $C_m(x)$ induces a homomorphism

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

Proposition 4.3. Let $m = p_1^{r_1} \cdots p_k^{r_k}$ be the prime factorization of $m \ge 2$. For $1 \le i \le k$, put

$$d'_{i} = \begin{cases} \gcd(p_{i}^{r_{i}}, 2\lambda(m)/\lambda(p_{i}^{r_{i}})) & \text{if } p_{i} = 2 \text{ and } r_{i} = 2, \\ \gcd(p_{i}^{r_{i}}, \lambda(m)/\lambda(p_{i}^{r_{i}})) & \text{otherwise.} \end{cases}$$

Let $d' = \prod_{i=1}^{k} d'_{i}$. Then the image of the homomorphism ϕ_m is $d'\mathbb{Z}/m\mathbb{Z}$.

Proof. We show the desired result case by case.

(I) First we prove the result for the case k = 1, that is $m = p^r$, where p is a prime and r is a positive integer.

Suppose that p = 2. If r = 2, then $C_m(3) = 2$, and for any positive integer n we have $C_m(2n + 1) = n(n + 1)$, which is even, so the image of ϕ_m is $2\mathbb{Z}/m\mathbb{Z}$. On the other hand, if r = 1 or $r \geq 3$, since $C_2(3) = 1$ and $C_8(3) = 1$, by using Proposition 2.8 we see that $C_m(3)$ is an odd integer, so the image of ϕ_m is $\mathbb{Z}/m\mathbb{Z}$.

Now, assume that p > 2. Note that $C_p(p+1) \equiv -1 \pmod{p}$, by Proposition 2.8 we have $C_m(p+1) \equiv -1 \pmod{p}$, which implies that $p \nmid C_m(p+1)$. Thus, there exists a positive integer n such that $nC_m(p+1) \equiv 1 \pmod{m}$. Then, by Proposition 2.2 (1) we deduce that $C_m((p+1)^n) \equiv 1 \pmod{m}$. So, the image of ϕ_m is $\mathbb{Z}/m\mathbb{Z}$.

(II) To complete the proof, we prove the result when $k \ge 2$.

For simplicity, denote $m_i = m/p_i^{r_i}$ and $n_i = \lambda(m)/\lambda(p_i^{r_i})$ for each $1 \leq i \leq k$, and then let m'_i be an integer such that $m_i^2 m'_i \equiv 1 \pmod{p_i^{r_i}}$. By Proposition 2.7, we have

(4.2)
$$C_m(a) \equiv \sum_{i=1}^k m_i m'_i n_i C_{p_i^{r_i}}(a) \pmod{m}.$$

So, for each $1 \leq i \leq k$, $C_m(a) \equiv m_i m'_i n_i C_{p_i^{r_i}}(a) \pmod{p_i^{r_i}}$. If $p_i = 2$ and $r_i = 2$, note that for any odd integer a > 1, $C_4(a)$ is even, then we see that $d'_i \mid n_i C_{p_i^{r_i}}(a)$, and thus $d'_i \mid C_m(a)$. Otherwise if $p_i > 2$ or $r_i \neq 2$, then $d'_i \mid n_i$, and so $d'_i \mid C_m(a)$. Hence, we have $d' \mid C_m(a)$ for any integer a coprime to m.

Let $b = \gcd(m, m_1m'_1n_1, \ldots, m_km'_kn_k)$. Then, there exist integers X_1, \ldots, X_k such that

(4.3)
$$b \equiv \sum_{i=1}^{k} m_i m'_i n_i X_i \pmod{m}.$$

If we denote $b_i = \gcd(p_i^{r_i}, m_i m'_i n_i)$ for each $1 \leq i \leq k$, then $b = \prod_{i=1}^k b_i$, here we remark that $b_i = \gcd(p_i^{r_i}, n_i)$. It is easy to see that for each $1 \leq i \leq k$, if $p_i > 2$ or $r_i \neq 2$, we have $d'_i = b_i$. Further, when $p_i = 2$ and $r_i = 2$, $d'_i = 2b_i$ if $8 \nmid \lambda(2p_1 \dots p_k)$, and $d'_i = b_i$ otherwise.

We now have three cases for m:

(i) There exists $1 \le j \le k$ such that $p_j = 2, r_j = 2$ and

$$8 \nmid \lambda(2p_1 \dots p_k).$$

(ii) There exists $1 \le j \le k$ such that $p_j = 2, r_j = 2$ and

 $8 \mid \lambda(2p_1 \dots p_k).$

(iii) All the other cases.

Clearly, in Cases (ii) and (iii) we have d' = b, and in Case (i) d' = 2b.

According to (I), there exist integers a_i with $p_i \nmid a_i$ for $1 \leq i \leq k$ defined by

$$C_{p_i^{r_i}}(a_i) \equiv \begin{cases} 2X_i & \text{in Case (i)}, \\ X_i & \text{in Case (iii)}, \\ \\ X_i & \text{in Case (ii) and } i \neq j, \\ 0 & \text{in Case (ii) and } i = j. \end{cases} \pmod{p_i^{r_i}}$$

By the Chinese Remainder Theorem, we can choose a positive integer a such that $a \equiv a_i \pmod{p_i^{2r_i}}$. So, by Proposition 2.2 (2) we have $C_{p_i^{r_i}}(a) \equiv C_{p_i^{r_i}}(a_i) \pmod{p_i^{r_i}}$. Then, combining with (4.3) and the relation between b and d', we obtain $m_i m'_i n_i C_{p_i^{r_i}}(a) \equiv d' \pmod{p_i^{r_i}}$ for each $1 \leq i \leq k$ in all the three cases. Finally, using (4.2) we have $C_m(a) \equiv d' \pmod{m}$, which completes the proof.

Comparing (4.1) with Proposition 4.3, we have $d' \mid d$. Moreover, by Proposition 2.1 we get

$$\frac{\varphi(m)}{\lambda(m)}d'\mathbb{Z}/m\mathbb{Z} = d\mathbb{Z}/m\mathbb{Z}.$$

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

In Proposition 4.3, if choosing $m = 2^r$ with $r \ge 3$, we have d = 2and d' = 1; while choosing $m = 2^{r_1}p^{r_2}$ with $r_1 \ge 3$ and odd prime $p \equiv 3 \pmod{4}$, we have d = 4 and d' = 1. Hence, compared with [4, Proposition 4.4], the homomorphism ϕ_m can be surjective in more cases.

For any integer $m \ge 2$, we define the set

$$T_m = \{a : 1 \le a \le m^2, \gcd(a, m) = 1, \}$$

m is a Carmichael-Wieferich number with base a.

Actually, T_m is the kernel of the homomorphism ϕ_m , then the following result follows directly from Proposition 4.3.

Corollary 4.4. We have $|T_m| = d'\varphi(m)$, where d' is defined in Proposition 4.3.

Corollary 4.4 shows that any integer $m \ge 2$ can be a Carmichael-Wieferich number with some base. However, the next proposition suggests that such Carmichael-Wieferich numbers are rare.

Proposition 4.5. We have $\lim_{m \to \infty} \frac{|T_m|}{\varphi(m^2)} = 0.$

Proof. Denote by d(m) the parameter d in (4.1). By Corollary 4.4, we know that

$$\frac{|T_m|}{\varphi(m^2)} \le \frac{d(m)}{m}.$$

So, it suffices to prove that $\lim_{m \to \infty} \frac{d(m)}{m} = 0.$ For primes p, we have

$$\lim_{p \to \infty} \frac{d(p)}{p} = \lim_{p \to \infty} \frac{1}{p} = 0.$$

1()

So $\liminf_{m \to \infty} \frac{d(m)}{m} = 0.$

Suppose that $\limsup \frac{d(m)}{m} \neq 0$. Then there exists a subsequence

Suppose that $\limsup_{m\to\infty} \frac{\alpha(m)}{m} \neq 0$. Then there exists a base q for $m \to \infty$ $\{\frac{d(n_i)}{n_i}\}$ such that $\lim_{i\to\infty} \frac{d(n_i)}{n_i} = \limsup_{m\to\infty} \frac{d(m)}{m} \neq 0$. For an integer $m \geq 2$, let $m = p_1^{r_1} \cdots p_k^{r_k}$ be its prime factorization. Put $\alpha_m = \max\{r_1, \cdots, r_k\}$. Here we use the notation in (4.1). For each $1 \leq j \leq k$, we have $\frac{d(m)}{m} \leq d_j/p_j^{r_j}$. In particular, if p_j is the largest prime factor of m, then $\frac{d(m)}{m} \leq 2/p_j^{r_j}$. For each i, let p_i be the largest prime factor of n_i , we abbreviate α_{n_i} to α_i . Since $\frac{d(n_i)}{n_i} \leq \frac{2}{p_i}$ for each i and $\lim_{i\to\infty} \frac{d(n_i)}{n_i} \neq 0$, there must exist an integer q such that $p_i < q$ for all i. Put $\beta = 2 \prod_{\substack{2 \leq p < q \\ p \text{ prime}}} (p-1)$.

Since $d(n_i) \leq \beta$, we have $\frac{d(n_i)}{n_i} \leq \frac{\beta}{2^{\alpha_i}}$ for each *i*. Notice that $n_i \to \infty$ when $i \to \infty$, we must have $\alpha_i \to \infty$ as $i \to \infty$. Hence, we have $\lim_{i\to\infty}\frac{d(n_i)}{n_i}=0.$ This leads to a contradiction. $i \rightarrow \infty$

So, we have
$$\limsup_{m \to \infty} \frac{d(m)}{m} = 0$$
. This completes the proof.

Assume that there are infinitely many Sophie Germain primes. We construct a sequence $\{n_i\}$ with $n_i = p_i(2p_i + 1)$, where p_i is a Sophie Germain prime, and then $2p_i + 1$ is also a prime. It is easy to see that $d(n_i) = p_i$ and $\lim_{i \to \infty} \frac{d(n_i)}{\sqrt{n_i}} = \frac{1}{\sqrt{2}}$. This implies that the limit $\lim_{m \to \infty} \frac{d(m)}{\sqrt{m}} = 0$ may be not true in general.

In the sequel, we want to characterize all the Carmichael-Wieferich numbers.

Let p be a prime and a an integer with $p \nmid a$. Put

$$\sigma(a, p) = \operatorname{ord}_p(a^{p-1} - 1) - 1 \quad \text{if } p \text{ is odd};$$

$$\sigma(a,2) = \begin{cases} \operatorname{ord}_2(a-1) - 1 & \text{if } a \equiv 1 \pmod{4}, \\ \operatorname{ord}_2(a+1) - 1 & \text{if } a \equiv 3 \pmod{4}. \end{cases}$$

Then, we can state an analogue of [4, Proposition 5.4]. For the convenience of the reader, we reproduce the proof.

Proposition 4.6. Let gcd(a, m) = 1, and $m = p_1^{r_1} \cdots p_k^{r_k}$ be the prime factorization of $m \ge 3$. Fix an integer j with $1 \le j \le k$, let $p = p_j$ and $r = r_j$. If $p \ne 2$ or $r \le 2$, put

$$n = \begin{cases} 0 & \text{if } \operatorname{ord}_p \operatorname{lcm}(p_1 - 1, \cdots, p_k - 1) \le r - 1, \\ \operatorname{ord}_p \operatorname{lcm}(p_1 - 1, \cdots, p_k - 1) - r + 1 & \text{otherwise}; \end{cases}$$

otherwise if p = 2 and r > 2, put

$$n = \begin{cases} 0 & \text{if } \operatorname{ord}_p \operatorname{lcm}(p_1 - 1, \cdots, p_k - 1) \le r - 2, \\ \operatorname{ord}_p \operatorname{lcm}(p_1 - 1, \cdots, p_k - 1) - r + 2 & \text{otherwise.} \end{cases}$$

Moreover, put

$$e(m,p) = \begin{cases} n & \text{if } p \neq 2 \text{ or } r \leq 2, \\ n-1 & \text{otherwise.} \end{cases}$$

Then we have

$$\operatorname{ord}_p C_m(a) = e(m, p) + \sigma(a, p).$$

Proof. Notice that $\lambda(m) = p^n \lambda(p^r) X$, where X is an integer with $p \nmid X$. Put $b = a^{p^n \lambda(p^r)}$. Then, since

$$a^{\lambda(m)} - 1 = b^X - 1 = (b-1) \sum_{i=0}^{X-1} b^i$$

 $b \equiv 1 \pmod{p}$ and $\sum_{i=0}^{X-1} b^i \equiv X \not\equiv 0 \pmod{p}$, we obtain

$$\operatorname{ord}_p(a^{\lambda(m)} - 1) = \operatorname{ord}_p(b - 1) = \operatorname{ord}_p(a^{p^n \lambda(p^r)} - 1).$$

Thus, if p is an odd prime, by using [4, Lemma 5.1] we have $\operatorname{ord}_p(a^{\lambda(m)}-1) = \operatorname{ord}_p((a^{p-1})^{p^{n+r-1}}-1) = \operatorname{ord}_p(a^{p-1}-1) + n + r - 1$, which implies that

$$\operatorname{ord}_p C_m(a) = e(m, p) + \sigma(a, p).$$

Similarly, applying [4, Lemmas 5.1 and 5.3], one can verify the remaining case p = 2 by noticing that $m \ge 3$.

The next proposition, a criterion for a number m being a Carmichael-Wieferich number, follows directly from Proposition 4.6.

Proposition 4.7. Let gcd(a, m) = 1, and $m = p_1^{r_1} \cdots p_k^{r_k}$ be the prime factorization of $m \ge 3$. Then the following statements are equivalent:

(1) m is a Carmichael-Wieferich number with base a,

(2) $e(m, p_j) + \sigma(a, p_j) \ge r_j$, for any $1 \le j \le k$.

Although it is known that Wieferich primes exist for many different bases (see [15]), the following problem is still open.

Whether Wieferich primes exist for all bases?

Proposition 4.8. For a non-zero integer a, if there exists a Carmichael-Wieferich number m with base a and m has an odd prime factor, then there exists a Wieferich prime with base a.

Proof. Let $m = p_1^{r_1} \cdots p_k^{r_k}$ be the prime factorization of m with $p_1 < p_2 < \cdots < p_k$, where p_k is an odd prime. Since $e(m, p_k) = 0$ and m is a Carmichael-Wieferich number with base a, by Proposition 4.7 we have $\sigma(a, p_k) \ge r_k \ge 1$. Notice that p_k is an odd prime, so p_k is a Wieferich prime with base a.

Finally, we want to remark that a Carmichael-Wieferich number m with base a is also a Wieferich number with base a, but the converse is not true.

Example 4.9. From Table 1 of [15], 3 and 7 are two Wieferich primes with base 19. It is straightforward to see that 2 is not a Wieferich prime with base 19. By [4, Theorem 5.5], $m = 2^2 \cdot 3 \cdot 7$ is a Wieferich number with base 19. But by Proposition 4.7, m is not a Carmichael-Wieferich number with base 19.

5. Involving perfect nonlinear function

Let (A, +) and (B, +) be two additive abelian groups, and denote by \overline{A} the set of non-identity elements of A. When |A| is a multiple of |B|, we can consider the following definition; see [5] for more details.

Definition 5.1. Let $f : A \to B$ be a function from A to B. Then f is called *perfect nonlinear* if for every $(a,b) \in \overline{A} \times B$, $|\{x \in A : f(x+a) - f(x) = b\}| = \frac{|A|}{|B|}$.

Perfect nonlinear functions have important applications in cryptography, sequences and coding theory. For example, as in [6], such functions can be used to construct authentication codes.

For the homomorphism $\phi_m : (\mathbb{Z}/m^2\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z}, +)$, defined in Section 4, we extend its definition to those integers a with $gcd(a, m) \neq 1$ by defining $\phi_m(a) = 0$. Then we get a function

$$f_m : (\mathbb{Z}/m^2\mathbb{Z}, +) \to (\mathbb{Z}/m\mathbb{Z}, +), x \mapsto \phi_m(x).$$

For this function f_m , we have the following proposition.

Proposition 5.2. The function f_m is perfect nonlinear if and only if m is a prime number.

Proof. First, suppose that m is a prime number. By [6, Lemma 8] (or [5, Theorem 48]) and Proposition 4.3, it is easy to show that f_m is perfect nonlinear.

Now assume that m is a composite integer. Let p be a prime factor of m. Notice that $f_m(kp) = 0$ for any $k \ge 1$, and $(m+2)p \le m(m+2)/2 < m^2$. Then choosing $(p, 0) \in \mathbb{Z}/m^2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, we obtain

$$|\{x \in \mathbb{Z}/m^2\mathbb{Z} : f_m(x+p) - f_m(x) = 0\}| \ge |\{x = kp : 1 \le k \le m+2\}|$$

= m+2 > m.

By definition, the function f_m is not perfect nonlinear.

Thus, the function f_m gives a new kind of perfect nonlinear functions when m is a prime number. Furthermore, this kind of perfect nonlinear functions is much more convenient for computations than that given in [5, Example 49].

ACKNOWLEDGEMENTS

The author would like to thank Professor Arne Winterhof for sending him the recent work [10]. He wants to thank the referee for careful reading and valuable comments. He is also grateful to the referee of his recent joint paper [14] for pointing our the error in the previous Proposition 4.3.

References

- T. Agoh, Fermat and Euler type quotients, C. R. Math. Rep. Acad. Sci. Canada, 17 (1995), 159–164.
- [2] T. Agoh, On Giuga's conjecture Manuscripta Math., 87 (1995), 501–510.
- [3] T. Agoh, On Fermat and Wilson quotients, Expo. Math., 14 (1996), 145–170.
- [4] T. Agoh, K. Dilcher and L. Skula, Fermat quotients for composite moduli, J. Number Theory, 66 (1997), 29–50.
- [5] C. Carlet and C. Ding, *Highly nonlinear mappings*, J. Complexity 20 (2004), 205–244.
- [6] S. Chansona, C. Ding and A. Salomaab, Cartesian authentication codes from functions with optimal nonlinearity, Theoretical Computer Science, 290 (2003), 1737–1752.
- [7] Z. Chen, Trace representation and linear complexity of binary sequences derived from Fermat quotients, Sci. China Inf. Sci., 57(11) (2014), 1–10.
- [8] Z. Chen and X. Du, On the linear complexity of binary threshold sequences derived from Fermat quotients, Des. Codes Cryptogr., 67 (2013), 317–323.

- [9] Z. Chen, A. Ostafe and A. Winterhof, Structure of pseudorandom numbers derived from Fermat quotients, in Arithmetic of Finite Fields, Lecture Notes in Computer Science, ed. by M.A. Hasan, T. Helleseth. vol. 6087, pp. 73–85, Springer, Berlin, 2010.
- [10] Z. Chen and A. Winterhof, On the distribution of pseudorandom numbers and vectors derived from Euler-Fermat quotients, Int. J. Number Theory, 08 (2012), 631–641.
- [11] A. Granville, Some conjectures related to Fermat's Last Theorem, in Number Theory, ed. by R.A. Mollin, pp. 177–192, Walter de Gruyter, New York, 1990.
- [12] M. Lerch, Zur Theorie des Fermatschen Quotienten $(a^{p-1}-1)/p = q(a)$, Math. Ann., **60** (1905), 471–490.
- M. Lerch, Sur les théorèmes de Sylvester concernant le quotient de Fermat, C. R. Acad. Sci. Paris, 142 (1906), 35–38.
- [14] F. Luca, M. Sha and I.E. Shparlinski, On two functions arising in the study of the Euler and Carmichael quotients, preprint, 2016.
- [15] P.L. Montgomery, New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp., 61 (1993), 361–363.
- [16] A. Ostafe and I. Shparlinski, Pseudorandomness and dynamics of Fermat quotients, SIAM J. Discr. Math., 25 (2011), 50–71.
- [17] P. Ribenboim, Thirteen lectures on Fermat's Last Theorem, Springer, New York, 1979.
- [18] J. Sauerberg and L. Shu, Fermat quotients over function fields, Finite Fields Th. App., 3 (1997), 275–286.
- [19] L. Skula, Fermat and Wilson quotients for p-adic integers, Acta Mathematica Universitatis Ostraviensis, (1998) 6, 167–181.

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY, NSW 2052, AUSTRALIA *E-mail address*: shamin2010@gmail.com