CHAPTER I
INTRODUCTION

Fermat's little theorem says that for a prime number p and an integer a with $p \nmid a$, we have $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$. Then we get the integer

$$F(a,p) := \frac{a^{p-1}-1}{p}$$

which is called the **Fermat quotient of p base a**. Another integer in which we are interested is called the **Wilson quotient of a prime number p**, denoted by $W(p)$. This quotient is induced from the Wilson's theorem stating that for a prime number p, $(p-1)! \equiv -1 (\mathrm{mod}\ p)$. Then we obtain

$$W(p) := \frac{(p-1)!+1}{p}.$$

In 1905, Lerch [7] studied the Fermat quotients and the Wilson quotients and gave some congruence relations of them.

In general, Euler improved Fermat's little theorem for an integer $n \geq 2$. Let a be an integer with $(a,n) = 1$. We have $a^{\phi(n)} \equiv 1 (\mathrm{mod}\ n)$ where $\phi(n)$ is the Euler function given by the number of positive integers which are less than n and relatively prime to n. Then we also get the integer

$$E(a,n) := \frac{a^{\phi(n)}-1}{n}$$

which is called the **Euler quotient of n base a**. In addition, Gauss generalized the Wilson's theorem to any positive integer. He proved that for an integer $n \geq 2$,

$$\prod_{\substack{i=1 \\ (i,n)=1}}^{n} i \equiv \epsilon_n \pmod{n}$$

where $\epsilon_n = -1$ if $n = 2, 4, p^k$ or $2p^k$ where p is an odd prime and k is a positive integer and $\epsilon_n = 1$ otherwise. Let $P(n) = \prod_{\substack{i=1 \\ (i,n)=1}}^{n} i$. Then for an integer $n \geq 2$, we obtain the **Wilson quotient of** n as the integer

$$W(n) := \frac{P(n) - \epsilon_n}{n}.$$

Surely, there are many researchers who developed the results of Lerch [7] by using the Euler quotients and the Wilson quotients defined by Gauss such as Agoh, Dilcher and Skula [1], [2].

The next quotient is the main idea in our work. Let $n \geq 2$ be an integer. From the Euler's theorem, for an integer a with $(a, n) = 1$, $a^{\phi(n)} \equiv 1 \pmod{n}$. By the well-ordering principle, there is the smallest positive integer l such that $a^l \equiv 1 \pmod{n}$ for all integers a with $(a, n) = 1$ and the number l is called the **Carmichael function of** n, denoted by $\lambda(n)$. In other words, $\lambda(n)$ is the least common multiple of the orders of all elements in $(\mathbb{Z}/n\mathbb{Z})^\times$. We can write the Carmichael function in form of the Euler function as follows

$$\lambda(n) := \begin{cases} \phi(n) & \text{for } n = 2, 4, \text{ or } p^\alpha \\ & \quad \text{where } p \text{ is an odd prime and } \alpha \geq 1. \\ \frac{1}{2}\phi(n) & \text{for } n = 2^\alpha \text{ where } \alpha \geq 3. \\ \operatorname{lcm}\{\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_r^{\alpha_r})\} & \text{for } n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \\ & \quad \text{where } p_i \text{ is a prime and } \alpha_i \in \mathbb{N}. \end{cases}$$

Now, we have $a^{\lambda(n)} \equiv 1 \pmod{n}$, so this congruence gives an integer which is called the **Carmichael quotient of n base a**,

$$C(a,n) := \frac{a^{\lambda(n)}-1}{n}.$$

This quotient was introduced by Sha [11] and he also studied the Euler quotients and the Carmichael quotients and gave some congruence relations of these quotients.

Theorem 1.1. *[11] For an integer $n \geq 2$ and an integer a with $(a,n) = 1$, we write $\langle a \rangle$ for the subgroup of $(\mathbb{Z}/n\mathbb{Z})^{\times}$ generated by a and $o(a) = |\langle a \rangle|$. Then*

$$C(a,n) \equiv \frac{\lambda(n)}{o(a)} \sum_{\substack{s=1 \\ s \in \langle a \rangle}}^{n} \frac{1}{as} \left\lfloor \frac{as}{n} \right\rfloor \pmod{n},$$

where $\lfloor \cdot \rfloor$ denotes the greatest integer function.

For a finite group G, the least common multiple of the orders of all elements in G is called the **exponent of** G, denoted by $\exp(G)$. Note that $\exp(G)$ divides $|G|$. In addition, if $G \cong G_1 \times G_2$ then $\exp(G) = \operatorname{lcm}\{\exp(G_1), \exp(G_2)\}$. For a commutative ring $\mathcal{R}$ with identity 1, the **exponent of** $\mathcal{R}$ is the exponent of its unit group $\mathcal{R}^{\times}$. Let $b\mathcal{R}$ be an ideal of $\mathcal{R}$ generated by $b \in \mathcal{R}$. If $\mathcal{R}/b\mathcal{R}$ is finite, then we can define $\lambda(b) = \exp((\mathcal{R}/b\mathcal{R})^{\times})$ similar to $\lambda(n) = \exp((\mathbb{Z}/n\mathbb{Z})^{\times})$. Hence, we may develop the Carmichael quotients over other rings which have close properties to $\mathbb{Z}$.

The first ring is the ring of integer $\mathcal{O}_K$ of a number field K (Section 2.1). We are interested in this ring because Bamunoba [3] studied the Euler quotients over $\mathcal{O}_K$ where $\mathcal{O}_K$ is a PID. He used the fact that for all $m \in \mathcal{O}_K \smallsetminus \{0\}$, the cardinality of the quotient ring $\mathcal{O}_K/m\mathcal{O}_K$ is finite to define his Euler quotient of m and also developed congruence relations similar to [1]. In general, the ring $\mathcal{O}_K$ may not be a PID or even a UFD, but this ring has no zero divisor. Then it satisfies the cancellative law, so the definition of quotient in any $\mathcal{O}_K$ is well defined. Hence, we can construct the Wilson quotients and the Carmichael quotients over a ring of integers $\mathcal{O}_K$ and study congruence relations of them in Chapter II.

The second ring is the polynomial ring $\mathbb{F}_q[x]$ over a finite field $\mathbb{F}_q$. This ring is a Euclidean domain and has infinitely many prime elements as $\mathbb{Z}$. In 2010. Meemark and Chinwarakorn [10] studied the Euler quotients over $\mathbb{F}_q[x]$ and obtained some congruence relations of them as the Lerch's theorem for $\mathbb{F}_q[x]$. Recently, Iamthong and Meemark [6] generalized the results in [10] by weakening the assumption. They replaced the polynomial ring $\mathbb{F}_q[x]$ over a finite field $\mathbb{F}_q$ with the polynomial ring $R[x]$ over a finite local ring R. Note that $\mathbb{F}_q[x]$ is a UFD. but $R[x]$ may contain zero divisors and has no unique factorization property. However, Iamthong and Meemark could define the Euler quotients and the Wilson quotients over $R[x]$ by using the division algorithm. For our work, we construct the Carmichael quotients over the polynomial ring over a finite local ring and study the congruence relations in Section 3.1.

Moreover, Iamthong and Meemark [6] defined the dth power residue symbol over $R[x]$ which induces the Euler quotient of degree d over $R[x]$ and studied congruence relations of them. We also get the inspirations to define the new symbol which we call λ, dth power residue symbol over $R[x]$ in Section 3.2. Finally, in Section 3.3, we construct the Carmichael quotients of degree d induced from the our new symbol and study relations of these quotients and the Euler quotients of degree d and the Wilson quotients defined by Iamthong and Meemark [6].