A NOTE ON LERCH'S FORMULAE FOR EULER QUOTIENTS

Alex Samuel Bamunoba[1]
Department of Mathematics, University of Stellenbosch, South Africa.
bamunoba@aims.ac.za, bamunoba@gmail.com

Received: 4/7/14, Revised: 9/4/15, Accepted: 10/8/15, Published: 11/13/15

Abstract

Lerch's formulae for Euler quotients in the rings $\mathbb{Z}$ and $\mathbb{F}_q[t]$ have already been studied. In this paper, we extend the study of these quotients to number fields and the Carlitz module. In the number fields case, we prove a version of Lerch's formula for $\mathcal{O}_{K^{\mathrm{Hil}}}$, the ring of integers of the Hilbert class field of a number field K. In the $\mathbb{F}_q[t]$ case, we replace the usual multiplication in $\mathbb{F}_q[t]$ with the Carlitz module action ρ and prove two new versions of this formula. In addition, we relate these congruences to Carlitz Wieferich primes in $\mathbb{F}_q[t]$. All our proofs use properties of Carlitz polynomials.

1. Introduction

Let p be an odd prime, a and n be integers with $a \neq 0, \pm 1$, and $n > 1$. The *Fermat-Euler Theorem* (also known as the Euler Totient Theorem) asserts that, if a and n are coprime, then $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$, where $\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^*$. If $n = p$ and a is coprime to p, then $\varphi(p) = p - 1$ and so $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$. This is the well known "little theorem" of Fermat. These two congruences motivate the following definitions.

- If a is coprime to p, then the *Fermat quotient* for a and p is defined to be

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

- If a is coprime to n, then the *Euler quotient* for a and n is defined to be

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

[1]The author was supported by the AIMS - DAAD In Country Scholarship Award (**A/13/90157**), the Post Graduate Merit Bursary Scheme at the University of Stellenbosch, South Africa and the government of Canada's International Development Research Centre (IDRC) and within the framework of the AIMS Research for Africa Project.

There is a lot of literature that discusses the history and properties of these quotients, e.g., [8] and [10]. The questions addressed in these studies can be summarized into two categories: the first category deals with questions on the divisibility of the Fermat quotients whereas in the second category, one fixes a prime p, interprets $q(\cdot, p)$ as a function and then estimates $\#\{q(a,p) : 0 \leq a \leq p-1\}$ and the multiplicity of points in the image of $q(\cdot, p)$, all considered modulo p. For an in-depth study of these two categories, see [1] and [13]. For details on the multiplicative $\mathbb{F}_q[t]$-analogues, see [6].

Amongst the many properties of the Fermat-Euler quotients, the one of interest to us is the congruence due to M. Lerch, see [8] and [7]. This congruence (or formula) relates the quotient $q(a,n)$ to the sum over all representatives of elements of $(\mathbb{Z}/n\mathbb{Z})^*$. The statement and proof of Lerch's result in Theorem 1 are from [1, Theorem 9.3].

Theorem 1 ([1, Theorem 9.3]). *If a and n are coprime, then*

$$q(a,n) = \frac{a^{\varphi(n)} - 1}{n} \equiv \sum_{\substack{r=1 \\ (r,n)=1}}^{n} \frac{1}{ar} \left[\frac{ar}{n}\right] \pmod{n},$$

where $[x]$ is the greatest integer less than or equal to x.

Proof. Let $r \geq 1$ be an integer less than and coprime to n. We write $ar \equiv c \pmod{n}$, where c is a generator of a residue class in $(\mathbb{Z}/n\mathbb{Z})^*$. Then $ar = bn + c$ for some $b = [\frac{ar}{n}] \in \mathbb{Z}$. As c goes through all residue classes in $(\mathbb{Z}/n\mathbb{Z})^*$, so does r. Let S denote the product of all such representatives of the residue classes of $(\mathbb{Z}/n\mathbb{Z})^*$. So

$$S = \prod_{\substack{r=1 \\ (r,n)=1}}^{n} c = \prod_{\substack{r=1 \\ (r,n)=1}}^{n} \left(ar - n\left[\frac{ar}{n}\right]\right) = a^{\varphi(n)} S \prod_{\substack{r=1 \\ (r,n)=1}}^{n} \left(1 - \frac{n}{ar}\left[\frac{ar}{n}\right]\right). \tag{1}$$

Divide both sides of equation (1) by S to get

$$1 = a^{\varphi(n)} \prod_{\substack{r=1 \\ (r,n)=1}}^{n} \left(1 - \frac{n}{ar}\right) \equiv a^{\varphi(n)} \left(1 - n \sum_{\substack{r=1 \\ (r,n)=1}}^{n} \frac{1}{ar}\left[\frac{ar}{n}\right]\right) \pmod{n^2}.$$

Equivalently,

$$a^{\varphi(n)} - 1 \equiv a^{\varphi(n)} n \left(\sum_{\substack{r=1 \\ (r,n)=1}}^{n} \frac{1}{ar}\left[\frac{ar}{n}\right]\right) \pmod{n^2}. \tag{2}$$

Divide both sides of congruence (2) by n and use $a^{\varphi(n)} \equiv 1 \pmod{n}$ on the right. □

Upon interpreting $q(\cdot, p)$ as an operator, we obtain Theorem 2.

Theorem 2. *Let a, b be integers coprime to p. The quotient $q(\cdot, p)$ satisfies*

$$q(ab,p) \equiv q(a,p) + q(b,p) (\mathrm{mod}\ p), \qquad q(a+bp,p) \equiv q(a,p) - \frac{b}{a} (\mathrm{mod}\ p) \text{ and}$$

$$2q(2,p) \equiv \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i}\ (\mathrm{mod}\ p).$$

Remark 3. The congruences in Theorem 2 were discovered by G. Eisenstein [10].

Remark 4. The last congruence relation in Theorem 2 was first proved by J. Sylvester.

Since the Fermat-Euler quotients are somehow hard to compute, it is natural to relate their sums over residue classes, and other quantities all defined modulo p. It was Johnson [10] who gave a practical method for determining $q(a,p)$ using this philosophy. A sketch of the proof of his result follows. Let $s \in \mathbb{Z}$ be the least positive integer with $a^s = \pm 1 + tp$, for some $t \in \mathbb{Z}_+$. Then $p = 1 + su$ for some $u \in \mathbb{Z}_+$ and

$$\begin{aligned} q(a,p) &= \frac{a^{p-1}-1}{p} = \frac{a^{su}-1}{p} = \frac{(\pm 1 + pt)^u - 1}{p} = \frac{(1 \pm pt)^u - 1}{p} \\ &\equiv \frac{(1 \pm upt) - 1}{p} \equiv \pm ut \equiv \mp \frac{t}{s} (\mathrm{mod}\ p). \end{aligned}$$

There is also a link between Fermat quotients and Wieferich primes to base a. A *Wieferich prime to base a* is a prime p (coprime to a) satisfying $a^{p-1} \equiv 1 (\mathrm{mod}\ p^2)$. This happens precisely when $q(a,p) \equiv 0 (\mathrm{mod}\ p)$. We shall briefly comment on the Carlitzian analogue of this result in Section 4, but for details, see [2] and [14].

The remainder of the paper is structured as follows. In Section 2, we shall state, and prove the $\mathcal{O}_{K^{\mathrm{Hil}}}$-analogue of Lerch's formula, state and prove properties of the $\mathcal{O}_{K^{\mathrm{Hil}}}$-analogue of Fermat quotient (interpreted as an operator) and Johnson's result. In Section 3, we shall state (without proof) Y. Meemark and S. Chinwarakorn's $\mathbb{F}_q[t]$-analogue of Lerch's formula together with the properties of the associated Fermat quotient operator. In Section 4, we shall describe the Carlitz module and Carlitz cyclotomic polynomials. Lastly, we shall prove two Carlitz module analogues of Lerch's formula and some properties of the Carlitz-Fermat quotient operator.

2. Number Fields Analogue of Lerch's Formula for Euler Quotients

Let K be a number field, $\mathcal{O}_K$ be the ring of integers in K, $\mathfrak{n}$ be a nonzero ideal, and $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Since K is a number field, the ring $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain (PID), the quotient $\mathcal{O}_K/\mathfrak{n}$ is finite. The norm of $\mathfrak{n}$ is defined as $|\mathfrak{n}| := \#(\mathcal{O}_K/\mathfrak{n})$ and $\varphi(\mathfrak{n}) := \#(\mathcal{O}_K/\mathfrak{n})^*$. This φ is the number field extension of the Euler totient function in Section 1.

The property of $\mathbb{Z}$ utilized a lot in Section 1 without explicit mention is the fact that $\mathbb{Z}$ is a PID. In general, $\mathcal{O}_K$ is not a PID, and so the proof of Lerch's formula can not be adapted for general number fields. However, the *Principal Ideal Theorem* guarantees that we can recover unique factorization by considering the ring of integers in the Hilbert class field of K. Of course, if $\mathcal{O}_K$ is a unique factorization domain then K is its own Hilbert class field. In the ring $\mathcal{O}_{K^{\text{Hil}}}$, *Fermat's Theorem* states that, if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{K^{\text{Hil}}}$ and $a \in \mathcal{O}_{K^{\text{Hil}}}$ with $a \notin \mathfrak{p}$, then $a^{\varphi(\mathfrak{p})} \equiv 1 (\text{mod } \mathfrak{p})$. The *Euler Totient Theorem* states that if $a \in \mathcal{O}_{K^{\text{Hil}}}$ is such that $a \notin \mathfrak{n}$, then $a^{\varphi(\mathfrak{n})} \equiv 1 (\text{mod } \mathfrak{n})$.

Let $\pi, \pi^* \in \mathcal{O}_{K^{\text{Hil}}}$ be the generators of $\mathfrak{p}$ and $\mathfrak{n}$, respectively, as (nonzero) ideals of $\mathcal{O}_{K^{\text{Hil}}}$. This naturally gives rise to the definition of Fermat and Euler quotients as

$$q(a, \mathfrak{p}) := \frac{a^{|\mathfrak{p}|-1} - 1}{\pi}, \qquad \textit{and} \qquad q(a, \mathfrak{n}) := \frac{a^{\varphi(\mathfrak{n})} - 1}{\pi^*},$$

respectively. Theorem 5 is the ring $\mathcal{O}_{K^{\text{Hil}}}$-analogue to Lerch's formula.

Theorem 5. *Let $a \in \mathcal{O}_{K^{\text{Hil}}}$ and $\mathfrak{n}$ be a nonzero $\mathcal{O}_{K^{\text{Hil}}}$-ideal. If $a \notin \mathfrak{n}$, then*

$$q(a, \mathfrak{n}) = \frac{a^{\varphi(\mathfrak{n})} - 1}{\pi^*} \equiv \sum_{\substack{r \in \mathcal{O}_{K^{\text{Hil}}},\ r \notin \mathfrak{n} \\ |r\mathcal{O}_{K^{\text{Hil}}}| < |\mathfrak{n}|}} \frac{1}{ar} \left[\frac{ar}{\pi^*}\right] (\text{mod } \mathfrak{n}),$$

where $\mathfrak{n} = \pi^* \mathcal{O}_{K^{\text{Hil}}}$ and $[\frac{ar}{\pi^*}]$ is the quotient when ar is divided by π^*.

Proof. Let $r \in \mathcal{O}_{K^{\text{Hil}}} - \mathfrak{n}$ and $|r\mathcal{O}_{K^{\text{Hil}}}| < |\mathfrak{n}|$. Since $r \notin \mathfrak{n}$, we write $ar \equiv c (\text{mod } \mathfrak{n})$, where c is a generator of a residue class in $(\mathcal{O}_{K^{\text{Hil}}}/\mathfrak{n})^*$. Then $ar = \beta\pi^* + c$ for some $\beta \in \mathcal{O}_{K^{\text{Hil}}}$ and so $\beta = [\frac{ar}{\pi^*}]$. As c goes through residue classes in $(\mathcal{O}_{K^{\text{Hil}}}/\mathfrak{n})^*$, so does r. Let S denote the product of representatives of elements of $(\mathcal{O}_{K^{\text{Hil}}}/\mathfrak{n})^*$. Then

$$\begin{aligned} S = \prod_{\substack{r \in \mathcal{O}_{K^{\text{Hil}}} - \mathfrak{n} \\ |r\mathcal{O}_{K^{\text{Hil}}}| < |\mathfrak{n}|}} c &= \prod_{\substack{r \in \mathcal{O}_{K^{\text{Hil}}} - \mathfrak{n} \\ |r\mathcal{O}_{K^{\text{Hil}}}| < |\mathfrak{n}|}} \left(ar - \pi^* \left[\frac{ar}{\pi^*}\right]\right) \\ &= a^{\varphi(n)} S \prod_{\substack{r \in \mathcal{O}_{K^{\text{Hil}}} - \mathfrak{n} \\ |r\mathcal{O}_{K^{\text{Hil}}}| < |\mathfrak{n}|}} \left(1 - \frac{\pi^*}{ar} \left[\frac{ar}{\pi^*}\right]\right). \end{aligned}$$

Divide through by S to get

$$1 = a^{\varphi(\mathfrak{n})} \prod_{\substack{r \in \mathcal{O}_{K^{\text{Hil}}} - \mathfrak{n} \\ |r\mathcal{O}_{K^{\text{Hil}}}| < |\mathfrak{n}|}} \left(1 - \frac{\pi^*}{ar}\right) \equiv a^{\varphi(n)} \left(1 - \pi^* \sum_{\substack{r \in \mathcal{O}_{K^{\text{Hil}}} - \mathfrak{n} \\ |r\mathcal{O}_{K^{\text{Hil}}}| < |\mathfrak{n}|}} \frac{1}{ar} \left[\frac{ar}{\pi^*}\right]\right) (\text{mod } \mathfrak{n}^2).$$

Equivalently,

$$a^{\varphi(\mathfrak{n})}-1\equiv a^{\varphi(\mathfrak{n})}\pi^*\left(\sum_{\substack{r\in\mathcal{O}_{K^{\mathrm{Hil}}}-\mathfrak{n}\\ |r\mathcal{O}_{K^{\mathrm{Hil}}}|<|\mathfrak{n}|}}\frac{1}{ar}\left[\frac{ar}{\pi^*}\right]\right)(\mathrm{mod}\ \mathfrak{n}^2). \tag{3}$$

Divide both sides of congruence (3) by π^* and use $a^{\varphi(\mathfrak{n})}\equiv 1(\mathrm{mod}\ \mathfrak{n})$ on the right. □

Theorem 6. *Let $a,b\in\mathcal{O}_{K^{\mathrm{Hil}}}$, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{K^{\mathrm{Hil}}}$, and let π be the uniformizer of $\mathfrak{p}$. The Fermat quotient operator $q(\cdot,\mathfrak{p})$ satisfies*

$$q(ab,\mathfrak{p})\equiv q(a,\mathfrak{p})+q(b,\mathfrak{p})(\mathrm{mod}\ \mathfrak{p})\quad \textit{and}\quad q(a+b\pi,\mathfrak{p})\equiv q(a,\mathfrak{p})-\frac{b}{a}(\mathrm{mod}\ \mathfrak{p}).$$

Proof. Take π to be the uniformizer of the prime ideal $\mathfrak{p}$. Then

$$\begin{aligned}q(ab,\mathfrak{p})&=\frac{(ab)^{|\mathfrak{p}|-1}-1}{\pi}=\frac{(ab)^{|\mathfrak{p}|-1}-b^{|\mathfrak{p}|-1}+b^{|\mathfrak{p}|-1}-1}{\pi}\\&=\frac{b^{|\mathfrak{p}|-1}(a^{|\mathfrak{p}|-1}-1)+b^{|\mathfrak{p}|-1}-1}{\pi}\equiv q(a,\mathfrak{p})+q(b,\mathfrak{p})(\mathrm{mod}\ \mathfrak{p}).\end{aligned}$$

To prove the second congruence, we proceed as follows. We have

$$\begin{aligned}q(a+b\pi,\mathfrak{p})&=\frac{(a+b\pi)^{|\mathfrak{p}|-1}-1}{\pi}=\frac{a^{|\mathfrak{p}|-1}+(|\mathfrak{p}|-1)a^{|\mathfrak{p}|-2}b\pi+\cdots+(b\pi)^{|\mathfrak{p}|-1}-1}{\pi}\\&\equiv\frac{(a^{|\mathfrak{p}|-1}-1)}{\pi}-a^{|\mathfrak{p}|-2}b\equiv q(a,\mathfrak{p})-\frac{b}{a}(\mathrm{mod}\ \mathfrak{p}).\end{aligned}$$

□

It is not hard to show that if $\mathfrak{p}$ is coprime to 2, then

$$q(2,\mathfrak{p})\equiv\frac{1}{2}\sum_{\substack{r\in\mathcal{O}_{K^{\mathrm{Hil}}}-\mathfrak{p}\\ |r\mathcal{O}_{K^{\mathrm{Hil}}}|<|\mathfrak{p}|}}\frac{1}{r}(\mathrm{mod}\ \mathfrak{p}).$$

Let s be the least positive integer such that $a^s\equiv\alpha(\mathrm{mod}\ \mathfrak{p})$, where $\alpha\in(\mathcal{O}_{K^{\mathrm{Hil}}})^*$. Then $a^s=\alpha+t\pi$, where $t\in\mathcal{O}_{K^{\mathrm{Hil}}}$ and $\mathfrak{p}=\pi\mathcal{O}_{K^{\mathrm{Hil}}}$. So $|\pi|=1+su$, $u\in(\mathcal{O}_{K^{\mathrm{Hil}}})^*$ and

$$\begin{aligned}q(a,\mathfrak{p})&=\frac{a^{|\mathfrak{p}|-1}-1}{\pi}=\frac{a^{su}-1}{\pi}=\frac{(\alpha+t\pi)^u-1}{\pi}=\frac{(1+\beta t\pi)^u-1}{\pi}\\&\equiv\frac{(1+\beta ut\pi)-1}{\pi}\equiv-\beta\frac{t}{s}(\mathrm{mod}\ \mathfrak{p}).\end{aligned}$$

This is the $\mathcal{O}_{K^{\mathrm{Hil}}}$-analogue of Johnson's result.

Remark 7. The units ±1 in Johnson's result [10] are now replaced by $\alpha,\beta\in\mathcal{O}^*_{K^{\mathrm{Hil}}}$.

Recently, J. Sauerberg, L. Shu [12] and other several authors have studied the multiplicative $\mathbb{F}_q[t]$-analogues of these results. In Section 3, we state their findings.

3. Multiplicative $\mathbb{F}_q[t]$-analogue of Lerch's Formula for Euler Quotients

Let $A := \mathbb{F}_q[t]$ be the ring of polynomials in the variable t defined over the finite field $\mathbb{F}_q$ and let P be a monic irreducible in A. For each $a, m \in A - \{0\}$, the absolute value of a is defined as $|a| := \#(A/aA) = q^{\deg(a)}$. For this ring, the *Euler Totient Theorem* states that, if $m \in A$ is coprime to a, then $a^{\varphi(m)} \equiv 1 (\text{mod } m)$, where $\varphi(m) := \#(A/mA)^*$. If $m = P$, then we get an $\mathbb{F}_q[t]$-analogue of *Fermat's Little Theorem* [11, Chapters 1, 3]. The *Fermat* and *Euler quotients* are then defined as

$$q(a, P) := \frac{a^{|P|-1} - 1}{P} \text{ and } q(a, m) := \frac{a^{\varphi(m)} - 1}{m},$$

respectively. In Theorems 8 and 9, we give the two $\mathbb{F}_q[t]$-analogues of Lerch's formula as proved by Y. Meemark and S. Chinwarakorn. For their proofs, refer to [9].

Theorem 8 ([9], Theorem 2). *If $a, m \in A$ are coprime, then*

$$q(a, m) = \frac{a^{\varphi(m)} - 1}{m} \equiv \sum_{\substack{\deg(R) < \deg(m) \\ (R,m)=1}} \frac{1}{aR} \left[\frac{aR}{m}\right] (\text{mod } m),$$

where $\left[\frac{aR}{m}\right]$ is the quotient when aR is divided by m.

Fix $d \mid q - 1$. For the prime P, the dth power residue symbol $(\frac{\cdot}{P})_d$ is defined as

$$\left(\frac{a}{P}\right)_d \equiv \begin{cases} a^{\frac{|P|-1}{d}} (\text{mod } P), & (a, P) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Meemark and Chinwarakorn [9] defined the *Fermat quotient of degree d* to base a as

$$q_d(a, P) := \frac{a^{\frac{|P|-1}{d}} - (\frac{a}{P})_d}{P}.$$

Furthermore, Meemark and Chinwarakorn proved the following result.

Theorem 9 ([9], Theorem 3). *If $a \in A$ is coprime to P, then*

$$q_d(a, P) \equiv \left(\frac{\frac{C_a}{R_0} - (\frac{a}{P})_d}{P}\right) + \left(\frac{a}{P}\right)_d \sum_{\substack{\deg(R) < \deg(P) \\ (R,P)=1 \\ (\frac{a}{P})_d = 1}} \frac{1}{aR} \left[\frac{aR}{P}\right] (\text{mod } P),$$

where

$$R_0 = \prod_{\substack{\deg(R) < \deg(P) \\ (R,P)=1 \\ (\frac{a}{P})_d = 1}} R \quad \textit{and} \quad C_a = \prod_{\substack{\deg(R) < \deg(P) \\ (R,P)=1 \\ (\frac{a}{P})_d = 1}} \left(aR - P\left[\frac{aR}{P}\right]\right).$$

Moreover, if there exists an $\alpha \in \mathbb{F}_q^*$ *such that* $(\frac{a}{P})_d = (\frac{\alpha}{P})_d$, *then*

$$q_d(a,P) \equiv \alpha^{\frac{q-1}{d}\deg(P)} \sum_{\substack{\deg(R)<\deg(P)\\(R,P)=1\\(\frac{a}{P})_d=1}} \frac{1}{aR}\left[\frac{aR}{P}\right] (\text{mod } P).$$

The properties of the quotient operator $q(\cdot, P)$ are summarized in Theorem 10.

Theorem 10. *Let* $a, b \in A$. *For any prime* P, *we have that* $q(\cdot, P)$ *satisfies*

$$q(ab,P) \equiv q(a,P) + q(b,P)(\text{mod } P), \quad q(a+bP,P) \equiv q(a,P) - \frac{b}{a}(\text{mod } P) \text{ and}$$
$$q(\alpha,P) \equiv 0(\text{mod } P) \text{ for any } \alpha \in \mathbb{F}_q^*.$$

The proofs of the congruences in Theorem 10 are straightforward calculations from the definition of $q(\cdot, P)$ and are therefore left for the reader.

Let s be the least positive integer for which $a^s = \alpha + bP$ for some $b \in A$ and $\alpha \in \mathbb{F}_q^*$. So $|P| = 1 + su$ for some positive integer u, (take $\alpha\beta \equiv 1(\text{mod } P)$) and

$$q(a,P) = \frac{a^{|P|-1}-1}{P} = \frac{(\alpha+bP)^u - 1}{P} = \frac{(1+\beta bP)^u - 1}{P} \equiv -\beta\frac{b}{s}(\text{mod } P).$$

This is the version of Johnson's result associated with the Fermat quotient $q(a, P)$.

Remark 11. Here, the units ± 1 in Johnson's result are replaced by $\alpha, \beta \in \mathbb{F}_q^*$.

The above analogues are built out of the multiplicative parallels of $\mathbb{Z}$ in A. We obtain the additive versions by using the analogy coming from the Carlitz module.

4. Carlitz $\mathbb{F}_q[t]$-module Analogues of Lerch's Formula

We shall maintain $A := \mathbb{F}_q[t]$, let A_+ be the set of monic polynomials in A, let k be the fraction field of A and let $\mathcal{F}$ be an algebraically closed field containing k. Furthermore, let τ be the qth power Frobenius map on $\mathcal{F}$ and let $\mathcal{F}\{\tau\}$ be the ring of twisted polynomials over $\mathcal{F}$ with commutation relation $\tau w = w^q\tau$ for all $w \in \mathcal{F}$. The ring $\mathcal{F}\{\tau\}$ is isomorphic to the non-commutative ring of $\mathbb{F}_q$ - linear polynomials in x with coefficients in $\mathcal{F}$ and multiplication defined by composition of polynomials. The map $\rho : A \to \mathcal{F}\{\tau\}$ satisfying $t \mapsto \rho_t = \tau + t\tau^0$ is called the *Carlitz homomorphism*.

With each $m \in A - \{0\}$, ρ associates the separable polynomial $\rho_m(x) := \rho_m(\tau)(x)$ called the *Carlitz m-polynomial*. Proposition 12 shows one way to compute $\rho_m(x)$.

Proposition 12 ([5], Proposition 3.3.10). *Let* $m \in A - \{0\}$. *Then*

$$\rho_m(x) = a_{m,\deg(m)}x^{|m|} + \cdots + a_{m,0}x,$$

where $a_{m,0} = m$, *and* $[i]a_{m,i} = (a_{m,i-1})^q - a_{m,i-1}$, $i = 1, \ldots, \deg(m)$.

As an example, we compute $\rho_{t^2+1}(x)$ using Proposition 12. Given $m = t^2+1 \in A$, we have $a_{m,0} = t^2+1$ and $a_{m,2} = 1$, since m is a degree 2 monic polynomial. Lastly,

$$a_{m,1} = \frac{a_{m,0}^q - a_{m,0}}{t^q - t} = \frac{(t^2+1)^q - (t^2+1)}{t^q - t} = \frac{t^{2q} - t^2}{t^q - t} = \frac{(t^q - t)(t^q + t)}{t^q - t} = t^q + t.$$

So $\rho_{t^2}(x) = a_{m,2}x^{q^2} + a_{m,1}x^q + a_{m,0}x = x^{q^2} + (t^q + t)x^q + (t^2+1)x$.

Remark 13. We have a few consequences of Proposition 12,

1. If m is a monic polynomial in A, then $a_{m,\deg(m)} = 1$.
2. If $m = P^s$ where P is a prime, then $a_{m,i} \equiv 0 (\text{mod } P)$ for all $i \neq \deg(m)$.

Remark 13 (2) implies that for any $a, P \in A$, we have that $\rho_P(a) \equiv a^{|P|} (\text{mod } P)$. As a consequence, we get an analogue for Fermat's Little Theorem for the Carlitz module, i.e., for any $a \in A$, $\rho_{P-1}(a) \equiv 0 (\text{mod } P)$. This version of the theorem does not require a and P to be coprime. The requirement $(a, P) = 1$ gives rise to a definition of a Fermat quotient (we divide by a to exclude the case $a \equiv 0 (\text{mod } P)$):

$$q_C(a, P) := \frac{\rho_{P-1}(a)}{aP} = \frac{a^{|P|} - a}{aP} + \frac{1}{P} \sum_{i=0}^{-1+\deg(P)} a_{P,i} a^{q^i - 1}.$$

We shall later refer to this as the Carlitz-Fermat quotient of type I.

For simplicity, we shall often refer to "Carlitz-something" as "c-something". For example, Carlitz-Fermat quotient will become c-Fermat quotient.

Theorem 14. *Let $a, P \in A$. If a and P are coprime, then*

$$q_C(a, P) = \frac{\rho_{P-1}(a)}{aP} \equiv \sum_{\substack{\deg(R) < \deg(P) \\ (R,P)=1}} \frac{1}{aR} \left(\left[\frac{aR}{P} \right] + \chi(R) a^{q^{\deg(R)}} \right) (\text{mod } P),$$

where $\chi(R) = 1$ if R is monic and $\chi(R) = 0$ otherwise.

Before we prove Theorem 14, let us first recall the fundamental numbers used in the arithmetic of the ring A. We shall use the following notation: for each positive integer i, $[i] := t^{q^i} - t$, $L_i := [i][i-1] \cdots [1]$ and $D_i := [i][i-1]^q \cdots [1]^{q^{i-1}}$. The symbol $[i]$ is the product of monic irreducible polynomials of degree dividing i, L_i is the least common multiple of monic polynomials of degree i and D_i is the product of all monic polynomials of degree i [5, Proposition 3.1.6] and [15, page 44]. To define [0], we use the philosophy that the empty product is equal to 1. So, $L_0 = D_0 = [0] = 1$.

For each $i \in \mathbb{Z}_{\geq 0}$, set

$$S_i := \frac{(-1)^i}{L_i} = \sum_{R \in A_{i+}} \frac{1}{R}, \tag{4}$$

where the sum runs over monic polynomials of degree i, [15].

Proof of Theorem 14. Suppose that $\deg(P) = n$. By Proposition 12, we get $a_{P,0} = P$ and $[i]a_{P,i} = a_{P,i-1}^q - a_{P,i-1}$ for $i = 1, \ldots, n-1$. Taking coefficients modulo P^2 gives $a_{P,0} = P$ and $[i]a_{P,i} = a_{P,i-1}^q - a_{P,i-1} \equiv -a_{P,i-1} (\text{mod } P^2)$ for $i = 1, \ldots, n$. By recursion, we obtain the following chain of congruence relations:

$$\begin{aligned} L_i a_{P,i} = [i]L_{i-1}a_{P,i-1} &\equiv -L_{i-1}a_{P,i-1} = -[i-1]L_{i-2}a_{P,i-1} \\ &\equiv (-1)^2 L_{i-2}a_{P,i-2} \equiv \cdots \equiv (-1)^i L_0 a_{P,0} (\text{mod } P^2). \end{aligned}$$

For all $i = 1, \ldots, n-1$, we have $L_i \not\equiv 0 (\text{mod } P)$ and so

$$\begin{aligned} aPq_C(a,P) = \rho_{P-1}(a) = a^{|P|} - a + \sum_{i=0}^{n-1} a_{P,i} a^{q^i} &\equiv a^{|P|} - a + P \sum_{i=0}^{n-1} \frac{(-1)^i}{L_i} a^{q^i} \\ &\equiv aP \left(q(a,P) + \sum_{i=0}^{n-1} S_i a^{q^i - 1} \right) (\text{mod } P^2). \end{aligned}$$

Dividing both sides of the congruence by aP gives

$$\begin{aligned} q_C(a,P) &\equiv q(a,P) + \sum_{i=0}^{n-1} S_i a^{q^i - 1} (\text{mod } P) \\ &\overset{\text{Eq. (4)}}{\equiv} \sum_{\substack{\deg(R) < n \\ (R,P)=1}} \frac{1}{aR} \left[\frac{aR}{P} \right] + \frac{\chi(R)}{R} a^{q^{\deg(R)} - 1} (\text{mod } P) \\ &\equiv \sum_{\substack{\deg(R) < n \\ (R,P)=1}} \frac{1}{aR} \left(\left[\frac{aR}{P} \right] + \chi(R) a^{q^{\deg(R)}} \right) (\text{mod } P), \end{aligned}$$

where χ is defined as $\chi(R) = 1$ if R is monic and $\chi(R) = 0$ otherwise. □

In [2] and [14], a c-Wieferich prime is defined to be any prime P satisfying $\rho_{P-1}(1) \equiv 0 (\text{mod } P^2)$. This is equivalent to saying that $q_C(1,P) \equiv 0 (\text{mod } P)$. So Lerch's formula gives a criterion to check for c-Wieferich primes in A. Calculations for c-Wieferich primes are simplified by the fact that $q(\alpha, P) = 0$ for any $\alpha \in \mathbb{F}_q^*$.

For each $m \in A - \{0\}$, the set $\Lambda_m := \{\lambda \in \mathcal{F} : \rho_m(\lambda) = 0\}$ denotes the Carlitz m-torsion points. An element $\lambda \in \Lambda_m$ is *primitive* if it generates Λ_m as an A-module.

Definition 15. Let $m \in A_+$. The Carlitz m-cyclotomic polynomial is defined as

$$\Phi_m(x) := \prod_{\lambda \in \Lambda_m : \text{primitive}} (x - \lambda).$$

$\Phi_m(x)$ has integer coefficients, degree $\varphi(m)$ and is irreducible over k. It satisfies nice relations, for example, factorization and composition identities, see [4] and [3].

Fix $d \mid q-1$. The c-Fermat quotient of degree d to base a is defined as

$$q_{C,d}(a,P) := \frac{\rho_P(a^{\frac{1}{d}}) - (\frac{a}{P})_d a^{\frac{1}{d}}}{a^{\frac{1}{d}} P} = \frac{\Phi_P(a^{\frac{1}{d}}) - (\frac{a}{P})_d}{P}.$$

This is related to the multiplicative Fermat quotient of degree d to base a as follows:

$$q_{C,d}(a,P) = \frac{a^{\frac{|P|-1}{d}} - (\frac{a}{P})_d}{P} + \frac{1}{P}\sum_{i=0}^{n-1} a_{P,i} a^{\frac{q^i-1}{d}} = q_d(a,P) + \frac{1}{P}\sum_{i=0}^{n-1} a_{P,i} a^{\frac{q^i-1}{d}},$$

where $n = \deg(P)$. Moreover, if $d = 1$, then $q_{C,1}(a,P) = q_C(a,P)$.

Theorem 16. *Let $a \in A$ and P be a prime in A. If a and P are coprime, then*

$$q_{C,d}(a,P) \equiv \sum_{\substack{\deg(R)<\deg(P) \\ (R,P)=1}} \left(\frac{1}{a^{\frac{1}{d}} R} \left[\frac{a^{\frac{1}{d}} R}{P} \right] + \frac{\chi(R)}{R} a^{\frac{q^{\deg(R)}-1}{d}} \right) \pmod P,$$

where $\chi(R) = 1$ if R is a monic polynomial in A and $\chi(R) = 0$ otherwise.

Proof. Let $b \in A$ be such that $b^d = a$. Then

$$\begin{aligned} q_{C,d}(a,P) = q_{C,d}(b^d,P) &= q_d(b^d,P) + \frac{1}{P}\sum_{i=0}^{-1+\deg(P)} a_{P,i} b^{q^i-1} \\ &= q(b,P) + \frac{1}{P}\sum_{i=0}^{-1+\deg(P)} a_{P,i} b^{q^i-1} = q_C(b,P). \end{aligned}$$

By Theorem 14, we have

$$\begin{aligned} q_C(b,P) &\equiv \sum_{\substack{\deg(R)<\deg(P) \\ (R,P)=1}} \frac{1}{bR} \left(\left[\frac{bR}{P} \right] + \chi(R) b^{q^{\deg(R)}} \right) \pmod P \\ &\equiv \sum_{\substack{\deg(R)<\deg(P) \\ (R,P)=1}} \left(\frac{1}{a^{\frac{1}{d}} R} \left[\frac{a^{\frac{1}{d}} R}{P} \right] + \frac{\chi(R)}{R} a^{\frac{q^{\deg(R)}-1}{d}} \right) \pmod P, \end{aligned}$$

which completes the proof. □

Theorem 17. *Let $a, b \in A$ and P be a prime in A. We have that $q_C(\cdot, P)$ satisfies*

$$q_C(ab,P) \equiv q(a,P) + q(b,P) + \sum_{\substack{\deg(f)<\deg(P) \\ (f,P)=1}} \frac{\chi(f)}{f} (ab)^{q^{\deg(f)}-1} \pmod P,$$

$$q_C(a+bP,P) \equiv q_C(a,P) - \frac{b}{a} \pmod P, \text{ and } q_C(\alpha,P) \equiv \sum_{\substack{\deg(f)<\deg(P) \\ (f,P)=1}} \frac{\chi(f)}{f} \pmod P,$$

where $\chi(f) = 1$ if f a monic polynomial in A and $\chi(f) = 0$ otherwise.

Proof. We have that

$$\begin{aligned} q_C(ab,P) = \frac{\rho_{P-1}(ab)}{abP} &= \frac{1}{abP}\left((ab)^{q^{\deg(P)}} - ab + \sum_{i=0}^{-1+\deg(P)} a_{P,i}(ab)^{q^i}\right) \\ &= \frac{(ab)^{q^{\deg(P)}} - ab}{abP} + \frac{1}{abP}\left(\sum_{i=0}^{-1+\deg(P)} a_{P,i}(ab)^{q^i}\right) \\ &\equiv q(ab,P) + \left(\sum_{i=0}^{-1+\deg(P)} \frac{(-1)^i}{L_i}(ab)^{q^i-1}\right) \pmod P \\ &\equiv q(a,P) + q(b,P) + \sum_{\substack{\deg(f)<\deg(P)\\(f,P)=1}} \frac{\chi(f)}{f}(ab)^{q^{\deg(f)}-1} \pmod P. \end{aligned}$$

For the second congruence, we have that

$$\begin{aligned} q_C(a+bP,P) = \frac{\rho_{P-1}(a+bP)}{(a+bP)P} &= \frac{\rho_{P-1}(a)}{(a+bP)P} + \frac{\rho_{P-1}(bP)}{(a+bP)P} \\ &\equiv \frac{\rho_{P-1}(a)}{aP} + \frac{\rho_{P-1}(bP)}{aP} \equiv q_C(a,P) - \frac{b}{a} \pmod P. \end{aligned}$$

The last congruence follows from the first one utilising the fact that, for each $\alpha \in \mathbb{F}_q^*$,

$$q_C(\alpha,P) \equiv q(\alpha,P) + \sum_{\substack{\deg(f)<\deg(P)\\(f,P)=1}} \frac{\chi(f)}{f}\alpha^{q^{\deg(f)}-1} \equiv \sum_{\substack{\deg(f)<\deg(P)\\(f,P)=1}} \frac{\chi(f)}{f} \pmod P.$$

□

To extend $q_C(\cdot,P)$ to a c-Euler quotient, we use Theorem 18 below.

Theorem 18 (Carlitz-Euler Totient Theorem of type I). *If $(a,m)=1$, then*

$$\Phi_m(a) \equiv 1 \pmod m.$$

For the proper flow of the paper, we postpone the proof of Theorem 18 to after Theorem 23. Now since Theorem 18 is analogous to the Euler Totient Theorem, we define

$$q_C(a,P) := \frac{\Phi_P(a)-1}{P} \quad \text{and} \quad q_C(a,m) := \frac{\Phi_m(a)-1}{m},$$

as the *c-Fermat* and *c-Euler quotients* of type I respectively.

Theorem 19. *Let $a,m \in A$. If a and m are coprime, then*

$$q_C(a,m) = \frac{\Phi_m(a)-1}{m} \equiv \sum_{\substack{\deg(R)<\deg(m)\\(R,m)=1}} \frac{1}{aR}\left(\left[\frac{aR}{m}\right]\right) + \frac{1}{m}\sum_{i=0}^{\varphi(m)-1} c_{m,i}a^i \pmod m,$$

where $c_{m,i}$ is the coefficient of x^i in $\Phi_m(x)$.

Proof. Let $a, m \in A$. If a and m are coprime, then

$$q_C(a,m) = \frac{\Phi_m(a)-1}{m} = \frac{a^{\varphi(m)}-1}{m} + \frac{1}{m}\sum_{i=0}^{\varphi(m)-1} c_{m,i}a^i$$
$$\equiv \sum_{\substack{\deg(R)<\deg(m)\\(R,m)=1}} \frac{1}{aR}\left(\left[\frac{aR}{m}\right]\right) + \frac{1}{m}\sum_{i=0}^{\varphi(m)-1} c_{m,i}a^i (\mathrm{mod}\ m).$$

□

Proposition 20. *The sum of coefficients of $\Phi_m(x)$ is congruent to 1 modulo m.*

Proof. Since $(a,m)=1$, we have $\Phi_m(a) \equiv 1(\mathrm{\ mod\ } m)$, by Theorem 18. Set $a=1$. □

To define another analogue of the Fermat and Euler quotients in the Carlitzian context, we introduce the function ϕ_*. This is the map $\phi_* : A_+ \to A$ defined by $\phi_*(m) = \sum_{\deg(D)<\deg(m)}(D,m)$. This is an $\mathbb{F}_q[t]$-analogue of the Pillai function.

Proposition 21. *ϕ_* is a multiplicative function.*

Proof. By grouping the terms according to gcd, $\phi_*(m) = \sum_{\deg(a)<\deg(m)}(a,m) = \sum_{D|m}\varphi(\frac{m}{D})(D,m)$. The result follows from the multiplicativity of the gcd map. □

By definition, we have $\phi_*(1)=1$, $\phi_*(P^s) = P^{s-1}(P-1)$. For any $a, b \in A$, if a is coprime to b, then $\phi_*(ab) = \phi_*(a)\phi_*(b)$, this is the multiplicativity property of ϕ_*.

Proposition 22. *Equivalently,*

$$m = \sum_{D|m}\phi_*(D), \text{ and } \phi_*(m) = \sum_{D|m} D\mu\left(\frac{m}{D}\right).$$

Proof. For the second formula, $\phi_*(m) = \sum_{\deg(a)<\deg(m)}(a,m) = \sum_{D|m}\varphi(\frac{m}{D})(D,m) = \sum_{D|m} D\mu\left(\frac{m}{D}\right)$. Let $\mathbb{I}$ be a map defined as $\mathbb{I}(m)=1$ for each $m \in A$. $\mathbb{I}$ is completely multiplicative, so by the Mobius inversion formula, we get $m = \sum_{D|m}\phi_*(D)$. □

With $\phi_*(\cdot)$, we get the second (or additive) version of the c-Euler Totient Theorem.

Theorem 23 (Carlitz-Euler Totient Theorem of type II). *Let $a, m \in A - \{0\}$. Then $\rho_{\phi_*(m)}(a) \equiv 0(\mathrm{mod}\ m)$.*

Proof. Let $n := \deg(P)$. Since ϕ_* is a multiplicative function, it suffices to check that $\rho_{\phi_*(P^s)}(a) \equiv 0(\mathrm{mod}\ P^s)$. So $\rho_{P^{s-1}}(a) = \sum_{i=0}^{n(s-1)} a_{P^{s-1},i}a^{q^i}$. It is not hard to show that $v_P(a_{P^{s-1},i}) = s-1-\lfloor\frac{i}{n}\rfloor$ for $i = 0,1,\ldots,n(s-1)$. If $a = Pg$, $g \in A$, then $v_P(a_{P^{s-1},i}a^{q^i}) = s-1-\lfloor\frac{i}{n}\rfloor + q^i \geq s$, since $q^i > i$ for $i \geq 0$. So $v_P(\rho_{P^{s-1}}(Pg)) \geq s$,

$$\frac{\rho_{\phi_*(P^s)}(a)}{P^{s-1}} = \frac{\rho_{P^{s-1}(P-1)}(a)}{P^{s-1}} = \frac{\rho_{P^{s-1}}(\rho_{P-1}(a))}{P^{s-1}} = \frac{\rho_{P^{s-1}}(Pg)}{P^{s-1}} \equiv 0(\mathrm{mod}\ P).$$

It follows by the Chinese Remainder Theorem that $\rho_{\phi_*(m)}(a) \equiv 0(\mathrm{mod}\ m)$. □

Proof of Theorem 18. To prove this result, there are three cases we need to consider.

1. $m = P$, a prime polynomial in A. Since a and P are coprime, dividing both sides of the congruence $\rho_P(a) \equiv a (\text{mod } P)$ by a gives $\Phi_P(a) \equiv 1 (\text{mod } P)$.

2. $m = P^s$, where $s \in \mathbb{Z}_{>1}$. Then $\rho_{\phi_*(P^s)}(a) \equiv 0 (\text{mod } P^s)$. It follows that $\rho_P(a) \equiv a \not\equiv 0 (\text{mod } P)$ and $\rho_{P^i}(a) \not\equiv 0 (\text{mod } P^i)$. By [2, Corollary 2.2.5] together with the congruence $\rho_{P^s}(a) \equiv \rho_{P^{s-1}}(a) \not\equiv 0 (\text{mod } P^s)$, we have that

$$\Phi_{P^s}(a) = \frac{\rho_{P^s}(a)}{\rho_{P^{s-1}}(a)} \equiv 1 (\text{mod } P^s).$$

3. m has at least two prime factors. Here, it suffices to show that $\Phi_m(a) \equiv 1 (\text{mod } P^s)$ for every prime factor of m, with $P^s \| m$, where $s \geq 1$. If $m = NP^s$, then

$$\Phi_m(a) = \frac{\Phi_N(\rho_{P^s}(a))}{\Phi_N(\rho_{P^{s-1}}(a))} = \frac{\Phi_N(\rho_{\phi_*(P^s)}(a) + \rho_{P^{s-1}}(a))}{\Phi_N(\rho_{P^{s-1}}(a))} \equiv 1 (\text{mod } P^s).$$

□

We define the c-Fermat and Euler quotients of type II as follows:

$$q_{C_*}(a, P) := \frac{\rho_{\phi_*(P)}(a)}{aP} \quad \text{and} \quad q_{C_*}(a, m) := \frac{\rho_{\phi_*(m)}(a)}{am}.$$

Theorem 24. *Let $a, m \in A$. If $a, m \in A$ are coprime, then*

$$q_{C_*}(a, m) \equiv \sum_{\substack{\deg(R) \leq \deg(m) \\ 0 \neq R \in A_+}} \left(\mu\left(\frac{m}{R}\right) \sum_{i=0}^{\deg(R)} \frac{a_{R,i}}{m} a^{q^i - 1} \right) (\text{mod } m),$$

where $\mu(\cdot)$ is the extended Möbius μ function. The extended Möbius function is defined as $\mu\left(\frac{m}{R}\right) = \mu(C)$, where $m = CR$ for some $C \in A$ and 0 if $R \nmid m$.

Proof. We have

$$\begin{aligned} q_{C_*}(a, m) = \frac{\rho_{\phi_*(m)}(a)}{am} &\overset{\text{Prop } 22}{\equiv} \sum_{D|m} \mu\left(\frac{m}{D}\right) \frac{\rho_D(a)}{am} \\ &\equiv \sum_{\substack{\deg(R) \leq \deg(m) \\ 0 \neq R \in A_+}} \mu\left(\frac{m}{R}\right) \sum_{i=0}^{\deg(R)} \frac{a_{R,i}}{m} a^{q^i - 1} (\text{mod } m), \end{aligned}$$

where $a_{R,i}$ is the coefficient of x^i in $\rho_R(x)$ and $\mu(\cdot)$ is the extended Möbius map. □

Remark 25. The c-Fermat quotients of type I and II are the same.

Acknowledgement I thank my advisor, A. Keet, for having read and improved the drafts of this document. I also thank the editor for pointing out the many errors in the earlier manuscript.

References

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

[2] Bamunoba,A., Arithmetic of Carlitz polynomials (Ph.D. thesis), Stellenbosch University, 2014.

[3] Bamunoba, A., On some properties of Carlitz cyclotomic polynomials, J. of Number Theory **143** (2014), 102 – 108.

[4] Bae, S., The arithmetic of Carlitz polynomials, J. Korean Math. Soc. **35** (1998), 341–360.

[5] Goss D., Basic Structures of Function Field Arithmetic, 1996, Springer-Verlag.

[6] Jeong, S. and Li, C., Remarks on Fermat quotient operators over function fields, Finite Fields and Appl. **23** (2013), 60–68.

[7] Lerch, M., Sur les théorèmes de Sylvester concernant le quotient de Fermat, C. R. Acad. Sci. Paris **142** (1906), 35–38.

[8] Lerch, M., Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$, Math. Ann. **60** (1905), 471–490.

[9] Meemark, Y. and Chinwarakorn, S., Lerch's Theorems over Function Fields, Integers **10** (2010), 25–30.

[10] Ribenboim, P. My Numbers, My Friends: Popular Lectures on Number Theory, 2000, Springer-Verlag.

[11] Rosen, M., Number Theory in Function Fields, 2002, Springer-Verlag.

[12] Sauerberg, J. and Shu, L., Fermat quotients over function fields, Finite Fields and Appl. **3** (1997), 275–286.

[13] Shparlinski, I. and Winterhof, A., Distribution of values of polynomial Fermat quotients, Finite Fields and Appl. **19** (2013), 94–104.

[14] Thakur, D., Fermat versus Wilson congruences, arithmetic derivatives and zeta values, Finite Fields and Appl. **32** (2015), 192–206.

[15] Thakur D., Function Field Arithmetic, 2004 World Scientific.