ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 46, Number 1, 2016

NON-VANISHING OF CARLITZ-FERMAT QUOTIENTS MODULO PRIMES

NGUYEN NGOC DONG QUAN

1. Introduction. Let $q = p^s$, where p is a prime and s is a positive integer. Let $\mathbb{F}_q$ be the finite field of q elements, and set $A = \mathbb{F}_q[T]$ and $k = \mathbb{F}_q(T)$. Let τ be the mapping defined by $\tau(x) = x^q$, and let $k\langle\tau\rangle$ denote the twisted polynomial ring. Let $C : A \to k\langle\tau\rangle$ $(a \mapsto C_a)$ be the Carlitz module, namely, let C be an $\mathbb{F}_q$-algebra homomorphism such that $C_T = T + \tau$. Let R be any commutative k-algebra. The definition of the Carlitz module C implies that $C_T(a) = Ta + a^q$ for every $a \in R$.

Let $\wp$ be a monic prime in A. The *Carlitz-Fermat quotient* $\mathcal{Q}_\wp : A \to A$ is the mapping defined by

$$\mathcal{Q}_\wp(a) := \frac{C_{\wp-1}(a)}{\wp} \quad \text{for each } a \in A.$$

The notion of Carlitz-Fermat quotients first appeared in the work of Mauduit [**6**]. In this note, we prove several non-vanishing results of Carlitz-Fermat quotients modulo primes in A, which are Carlitz module analogues of the results in [**5**]. As a by-product, we give an alternative proof of the result in [**2**] that a Mersenne prime in A is a non-Wieferich prime in the Carlitz module context. We briefly recall the notions of Mersenne primes and Wieferich primes in the Carlitz module setting.

Definition 1.1. A *Mersenne prime* M in A is a prime of the form $\alpha C_\wp(1)$, where $\wp$ is a monic prime in A and α is an element in $\mathbb{F}_q^\times$.

Definition 1.2. Let W be a prime element in A. Write $W = \alpha\wp$, where $\alpha \in \mathbb{F}_q^\times$ is the leading coefficient of W and $\wp$ is a monic prime in A. We say that W is a *Wieferich prime* if $\mathcal{Q}_\wp(1) \equiv 0 \pmod{\wp}$; otherwise, W is called a *non-Wieferich prime*.

2010 AMS *Mathematics subject classification.* Primary 11G09, 11R58, 11T55.

Keywords and phrases. Carlitz module, Carlitz-Fermat quotients, Mersenne prime, Wieferich prime.

Received by the editors on May 9, 2014.

DOI:10.1216/RMJ-2016-46-1-125

The notion of Mersenne primes in A was introduced by the author in **[2]**, and the notion of Wieferich primes in A was first introduced by Dinesh Thakur in **[9]**. See also Thakur's recent preprint **[11]** for more beautiful results on several types of primes in A and their connections with zeta values.

2. Carlitz-Fermat quotients. In this section, we prove several properties of Carlitz-Fermat quotients. The main result of this section is the following.

Proposition 2.1. *Let $\wp$ be a monic prime in A of degree $d > 0$. Then*

(i) $\mathcal{Q}_\wp$ *is an $\mathbb{F}_q$-module homomorphism;*
(ii) $\mathcal{Q}_\wp(a + m\wp) \equiv \mathcal{Q}_\wp(a) - m \pmod{\wp}$ *for all $a, m \in A$; and*
(iii) $\mathcal{Q}_\wp(C_m(a)) \equiv m\mathcal{Q}_\wp(a) \pmod{\wp}$ *for all $a, m \in A$.*

Proof. Since the Carlitz module C is an $\mathbb{F}_q$-algebra homomorphism, we see that (i) follows immediately.

We now prove (ii). By **[8,** Proposition 12.11], one can write $C_\wp(x) \in A[x]$ in the form

$$C_\wp(x) = \wp x + [\wp, 1]x^q + \cdots + [\wp, d-1]x^{q^{d-1}} + x^{q^d}, \tag{2.1}$$

where $[\wp, i]$ is a polynomial of degree $q^i(d-i)$ for each $1 \leq i \leq d-1$. Furthermore, we know that $[\wp, i]$ is divisible by $\wp$ for each $1 \leq i \leq d-1$. Hence, we see that

$$\begin{aligned} C_{\wp-1}(m\wp) &= \wp(m\wp) + [\wp, 1](m\wp)^q + \cdots + (m\wp)^{q^d} - m\wp \\ &= \wp\left(m\wp + [\wp, 1]m^q\wp^{q-1} + \cdots + m^{q^d}\wp^{q^d-1} - m\right), \end{aligned}$$

and thus $\mathcal{Q}_\wp(m\wp) \equiv -m \pmod{\wp}$. It thus follows from part (i) that

$$\mathcal{Q}_\wp(a + m\wp) = \mathcal{Q}_\wp(a) + \mathcal{Q}_\wp(m\wp) \equiv \mathcal{Q}_\wp(a) - m \pmod{\wp}.$$

We now prove that (iii) holds. Let m be an arbitrary element in A of degree h, and let $a \in A$. We can write $C_m(x) \in A[x]$ in the form

$$C_m(x) = mx + [m, 1]x^q + [m, 2]x^{q^2} + \cdots + [m, h-1]x^{q^{h-1}} + [m, h]x^{q^h},$$

where $[m,i]$ is a polynomial of degree $q^i(h-i)$ for each $1 \le i \le h$. We see that

$$\begin{aligned}\wp\mathcal{Q}_\wp(C_m(a)) &= C_{\wp-1}(C_m(a)) = C_{m(\wp-1)}(a)\\ &= C_m(C_{\wp-1}(a)) = C_m(\wp\mathcal{Q}_\wp(a))\\ &= m(\wp\mathcal{Q}_\wp(a)) + [m,1](\wp\mathcal{Q}_\wp(a))^q + \cdots + [m,h](\wp\mathcal{Q}_\wp(a))^{q^h},\end{aligned}$$

and thus

$$\mathcal{Q}_\wp(C_m(a)) = m\mathcal{Q}_\wp(a) + [m,1]\wp^{q-1}(\mathcal{Q}_\wp(a))^q + \cdots + [m,h]\wp^{q^h-1}(\mathcal{Q}_\wp(a))^{q^h}.$$

Therefore, we deduce that

$$\mathcal{Q}_\wp(C_m(a)) \equiv m\mathcal{Q}_\wp(a) \pmod{\wp},$$

which proves that (iii) is true. $\square$

Remark 2.2. Let p be an odd prime in $\mathbb{Z}$. Recall that the *Fermat quotient* $q_p : \mathbb{Z} \to \mathbb{Z}$ is defined by $q_p(a) = (a^{p-1}-1)/p$ for each integer a with $\gcd(a,p) = 1$. According to **[1]**, Eisenstein noted that the Fermat quotient q_p satisfies the following properties.

(1) $q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}$;
(2) $q_p(a+mp) \equiv q_p(a) - m/a \pmod{p}$;

and

(3) $q_p(a^m) \equiv mq_p(a) \pmod{p}$.

There are well-known analogies **[3, 8, 10]** between the Carlitz module $a \mapsto C_m(a)$, $m \in A$, and the power map $a \mapsto a^m$, $m \in \mathbb{Z}$. Hence, (i), (ii) and (iii) in Proposition 2.1 are Carlitz module analogues of (1), (2) and (3) mentioned above.

3. Non-vanishing of Carlitz-Fermat quotients modulo primes.

In this section, using Proposition 2.1, we prove several non-vanishing results of Carlitz-Fermat quotients modulo primes.

Theorem 3.1. *Let $\wp$ be a monic prime in A of degree $d > 0$, and let $\mathcal{Q}_\wp$ be the Carlitz-Fermat quotient of $\wp$. Let a, m be nonzero elements in A such that $\wp$ does not divide m. Assume that $C_m(a) = b\wp$ for some*

$b \in A$. Then

$$\mathcal{Q}_{\wp}(a) \equiv -\frac{b}{m} \pmod{\wp}.$$

Proof. It follows from part Proposition 2.1 (iii) that

$$m\mathcal{Q}_{\wp}(a) \equiv \mathcal{Q}_{\wp}(C_m(a)) = \mathcal{Q}_{\wp}(b\wp) \pmod{\wp}.$$

By parts (i) and (ii) in Proposition 2.1, we deduce that $\mathcal{Q}_{\wp}(b\wp) \equiv -b \pmod{\wp}$, and thus $\mathcal{Q}_{\wp}(a) \equiv -b/m \pmod{\wp}$. □

In **[2]**, the author proves that a Mersenne prime is a non-Wieferich prime in the Carlitz module context. We present here an alternative proof of this result using Theorem 3.1.

Corollary 3.2. *Let $M_P = \alpha C_P(1)$ be a Mersenne prime, where α is an element in $\mathbb{F}_q^{\times}$ and P is a monic prime in A of degree $d > 0$. Then M_P is a non-Wieferich prime.*

Proof. Write $M_P = \beta\wp$, where $\beta \in \mathbb{F}_q^{\times}$ is the leading coefficient of M_P and $\wp$ is a monic prime in A. We see that $C_P(1) = \alpha^{-1}M_P = \alpha^{-1}\beta\wp$. We can write $C_P(x) \in A[x]$ in the form

$$C_P(x) = Px + [P,1]x^q + \cdots + [P,d-1]x^{q^{d-1}} + x^{q^d},$$

where $[P,i]$ is a polynomial in A of degree $q^i(d-i)$ for each $1 \leq i \leq d-1$. Furthermore, it is known **[4,** Proposition 2.4] that $[P,i]$ is divisible by P for each $1 \leq i \leq d-1$. Hence, we deduce that

$$\begin{aligned}\beta\wp &= M_P = \alpha C_P(1)\\ &= \alpha(P + [P,1] + \cdots [P,d-1] + 1) \equiv \alpha \pmod{P},\end{aligned}$$

and thus $\wp \equiv \alpha\beta^{-1} \not\equiv 0 \pmod{P}$.

Since $P, \wp$ are relatively prime, applying Theorem 3.1 with P, $\wp$, 1 and $\alpha^{-1}\beta$ in the roles of m, $\wp$, a and b, respectively, we deduce that

$$Q_{\wp}(1) \equiv -\frac{\alpha^{-1}\beta}{P} \not\equiv 0 \pmod{\wp},$$

and thus $M_P = \beta\wp$ is a non-Wieferich prime. □

Corollary 3.3. *Let a be an element in A, and let m, n be nonzero elements in A. Let H be the unique element in A such that $C_{mn}(a) =$*

$C_n(a)H$. Assume that there exists a monic prime $\wp$ dividing H such that $\wp$ does not divide mn. Write $H = b\wp$ for some $b \in A$. Then

$$\mathcal{Q}_\wp(a) \equiv -\frac{bC_n(a)}{mn} \pmod{\wp}.$$

Proof. We see that $C_{mn}(a) = HC_n(a) = bC_n(a)\wp$. Since $\wp$ does not divide mn, applying Theorem 3.1 with a, $bC_n(a)$, mn and $\wp$ in the roles of a, b, m and $\wp$, respectively, we deduce that

$$\mathcal{Q}_\wp(a) \equiv -\frac{bC_n(a)}{mn} \pmod{\wp}. \qquad \square$$

Corollary 3.4. *We maintain the same notation and assumptions as in Corollary 3.3. Assume that $v_\wp(H) = 1$, where $v_\wp$ denotes the $\wp$-adic valuation. Assume further that m and $C_n(a)$ are relatively prime. Then $\mathcal{Q}_\wp(a) \not\equiv 0 \pmod{\wp}$.*

Proof. By Corollary 3.3, we know that

$$\mathcal{Q}_\wp(a) \equiv -\frac{bC_n(a)}{mn} \pmod{\wp}.$$

We prove that $bC_n(a) \not\equiv 0 \pmod{\wp}$. Indeed, we know that $1 = v_\wp(H) = v_\wp(b\wp) = 1 + v_\wp(b)$, and thus $v_\wp(b) = 0$. Hence, $b \not\equiv 0 \pmod{\wp}$.

We can write $C_m(x) \in A[x]$ in the form

$$C_m(x) = mx + [m,1]x^q + \cdots + [m, \deg(m)]x^{q^{\deg(m)}},$$

where $[m,i]$ is a polynomial of degree $q^i(\deg(m) - i)$ for each $1 \leq i \leq \deg(m) - 1$ and $[m, \deg(m)]$ is the leading coefficient of m. Then we see that

$$\begin{aligned} C_{mn}(a) &= C_m(C_n(a)) \\ &= C_n(a)(m + [m,1](C_n(a))^{q-1} + \cdots + [m, \deg(m)](C_n(a))^{q^{\deg(m)}-1}). \end{aligned}$$

Since $C_{mn}(a) = C_n(a)H$, we deduce that

$$H = m + [m,1](C_n(a))^{q-1} + \cdots + [m, \deg(m)](C_n(a))^{q^{\deg(m)}-1}.$$

Since $\gcd(m, C_n(a)) = 1$, it follows from the equation of H that $H \equiv m \not\equiv 0 \pmod{\mathfrak{q}}$ for each prime $\mathfrak{q}$ dividing $C_n(a)$. Hence, H and

$C_n(a)$ are relatively prime, and therefore $C_n(a) \not\equiv 0 \pmod{\wp}$. This implies that $bC_n(a) \not\equiv 0 \pmod{\wp}$, and hence

$$\mathcal{Q}_{\wp}(a) \equiv -\frac{bC_n(a)}{mn} \not\equiv 0 \pmod{\wp}. \qquad \square$$

Remark 3.5. Corollary 3.3 and Corollary 3.4 are Carlitz analogues of Corollary 2 and Corollary 3 in [**5**], respectively.

REFERENCES

1. L.E. Dickson, *History of the theory of numbers*, Volume I: *Divisibility and primality*, Chelsea Publishing Company, New York, 1966.

2. N.N. Dong Quan, *Carlitz module analogues of Mersenne primes, Wieferich primes, and certain prime elements in cyclotomic function fields*, J. Num. Theor. **145** (2014), 181–193.

3. D. Goss, *Basic structures of function field arithmetic*, Ergeb. Math. Grenzg. **35**, Springer-Verlag, Berlin, 1996.

4. D.R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91.

5. W. Johnson, *On the nonvanishing of Fermat quotients* $\pmod{p}$, J. reine angew. Math. **292** (1977), 196–200.

6. V. Mauduit, *Quotients de Fermat-Carlitz*, C.R. Acad. Sci. Paris **321** (1995), 1139–1141.

7. ______, *Carmichael-Carlitz polynomials and Fermat-Carlitz quotients*, in *Finite fields and applications*, Lond. Math. Soc. Lect. Note **233**, Cambridge University Press, Cambridge, 1996.

8. M. Rosen, *Number theory in function fields*, Grad. Texts Math. **210**, Springer-Verlag, New York, 2002.

9. D.S. Thakur, *Iwasawa theory and cyclotomic function fields*, in *Arithmetic geometry* Contemp. Math. **174**, American Mathematical Society, Philadelphia, 1994.

10. ______, *Function field arithmetic*, World Scientific Publishing Co., Inc., River Edge, NJ, 2004.

11. ______, *Fermat versus Wilson congruences, arithmetic derivatives and zeta values*, preprint, 2014.

Department of Mathematics, University of Texas at Austin, Austin, TX 78712

Email address: **dongquan.ngoc.nguyen@gmail.com**