LERCH'S THEOREMS OVER FUNCTION FIELDS

Yotsanan Meemark
Department of Mathematics, Faculty of Science, Chulalongkorn University, Bangkok 10330, THAILAND
yotsanan.m@chula.ac.th

Sirawich Chinwarakorn
Department of Mathematics, Faculty of Science, Chulalongkorn University, Bangkok 10330, THAILAND
eternalaimay@hotmail.com

Received: 7/8/09, Accepted: 11/13/09, Published: 3/5/10

Abstract
In this work, we state and prove Lerch's theorems for Fermat and Euler quotients over function fields defined analogously to the number fields.

1. Results

The Fermat's little theorem states that if p is a prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \mod p$. This gives rise to the definition of the *Fermat quotient of* p *with base* a,

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

which is an integer. This quotient has been widely investigated and applied by many authors (see, e.g., [1, 2, 3, 7]). In 1905, Lerch [4] introduced and studied a generalization of the Fermat quotient for an arbitrary composite modulus $m \geq 2$ based on Euler's theorem, so called the Euler quotient. The following congruence is due to Lerch [1, 4]:

Theorem 1. [Lerch, 1905] *If a and $m \geq 2$ are relatively prime integers, then*

$$q(a,m) = \frac{a^{\phi(m)}-1}{m} \equiv \sum_{\substack{r=1 \\ \gcd(r,m)=1}}^{m} \frac{1}{ar}\left[\frac{ar}{m}\right] \mod m,$$

where $[x]$ denotes the greatest integer $\leq x$.

It is well-known that the ring of integers $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}_q[x]$, the ring of polynomials over the finite field $\mathbb{F}_q$ in an indeterminate x. Over a function field, we have not only the result parallel to Fermat's little theorem, but we also have Euler's theorem on A (see, Chapters 1 and 3 of [5]).

Let $\mathbb{F}_q$ be a finite field with q elements and set $A = \mathbb{F}_q[x]$. Let $a \in A$ and P be irreducible over A. Write $|P|$ for $q^{\deg P}$. If P does not divide a, we know that $a^{|P|-1} \equiv 1 \mod P$, which is analogous to Fermat's little theorem. Fix $d \mid q-1$. For P not dividing a, let $(\frac{a}{P})_d$ be the unique element of $\mathbb{F}_q^{\times}$ such that $a^{\frac{|P|-1}{d}} \equiv (\frac{a}{P})_d$ mod P. If $P \mid a$, we let $(\frac{a}{P})_d = 0$. The symbol $(\frac{a}{P})_d$ is called the *d-th power residue symbol*. We define thus the polynomial

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

called the *Fermat quotient of degree d for P with base a*. For $d = 1, aq_1(a, P) = \dfrac{a^{|P|} - a}{P}$ is the Fermat quotient studied in [6] by Sauerberg and Shu.

Another extension of the Fermat quotient, called the Euler quotient, is defined from Euler's theorem as follows: For a and f polynomials in A with $\gcd(a, f) = 1$, one has a result parallel to Euler's theorem, namely,

$$a^{\Phi(f)} \equiv 1 \mod f,$$

where $\Phi(f)$ denotes the cardinality of the unit group $(A/fA)^{\times}$. Following Lerch [4] and Agoh et al. [1], the *Euler quotient for f with base a* is given by the polynomial

$$q(a, f) = \frac{a^{\Phi(f)} - 1}{f}.$$

Observe that $\Phi(P) = |P| - 1$ if P is irreducible. Hence the Euler quotient is a generalization of the Fermat quotient $q_1(a, P)$.

In this work, we study function field analogs of Lerch's theorem for Euler and Fermat quotients. We present our versions of Lerch's congruence for Euler and Fermat quotients in Theorems 2 and 3, respectively.

Theorem 2. *For polynomials a and f in A with $\gcd(a, f) = 1$, we have*

$$q(a, f) \equiv \sum_{\substack{\deg(r)<\deg(f) \\ \gcd(r,f)=1}} \frac{1}{ar} \left[\frac{ar}{f}\right] \mod f.$$

Here $\left[\dfrac{ar}{f}\right]$ is the quotient when f divides ar.

Proof. For a polynomial r with $\deg r < \deg f$ and $\gcd(r, f) = 1$, we put $ar \equiv c$ mod f with $c \in A$ and $\deg(c) < \deg(f)$. Then $ar = kf + c$ for some polynomial k, and hence $k = [\frac{ar}{f}]$. Note that as c goes through all polynomials with degree less than $\deg f$ and relatively prime to f, so does r. Let C denote the product of all such polynomials c. It follows that

$$C = \prod_{\substack{\deg(r)<\deg(f)\\ \gcd(r,f)=1}} \left(ar - f\left[\frac{ar}{f}\right]\right) = a^{\Phi(f)} C \prod_{\substack{\deg(r)<\deg(f)\\ \gcd(r,f)=1}} \left(1 - \frac{f}{ar}\left[\frac{ar}{f}\right]\right).$$

Thus we find

$$\begin{aligned} 1 &= a^{\Phi(f)} \prod_{\substack{\deg(r)<\deg(f)\\ \gcd(r,f)=1}} \left(1 - \frac{f}{ar}\left[\frac{ar}{f}\right]\right) \\ &\equiv a^{\Phi(f)} \left(1 - f \sum_{\substack{\deg(r)<\deg(f)\\ \gcd(r,f)=1}} \frac{1}{ar}\left[\frac{ar}{f}\right]\right) \mod f^2 \\ &\equiv a^{\Phi(f)} - f \sum_{\substack{\deg(r)<\deg(f)\\ \gcd(r,f)=1}} \frac{1}{ar}\left[\frac{ar}{f}\right] \mod f^2. \end{aligned}$$

That is,

$$a^{\Phi(f)} - 1 \equiv f \sum_{\substack{\deg(r)<\deg(f)\\ \gcd(r,f)=1}} \frac{1}{ar}\left[\frac{ar}{f}\right] \mod f^2.$$

Dividing both sides by f, we have

$$q(a,f) = \frac{a^{\Phi(f)} - 1}{f} \equiv \sum_{\substack{\deg(r)<\deg(f)\\ \gcd(r,f)=1}} \frac{1}{ar}\left[\frac{ar}{f}\right] \mod f$$

and we are done. □

Lerch's theorem for the Fermat quotient of degree d is slightly different which results from the presence of the d-th power residue symbol.

Theorem 3. *Let $a \in A$ and P be an irreducible polynomial over A. If P does not divide a, then*

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

where $\left[\frac{ar}{P}\right]$ *is the quotient when* P *divides* ar,

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

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

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

Proof. For a polynomial r with $\deg r < \deg P, \gcd(r,P) = 1$ and $(\frac{r}{P})_d = 1$, we put $ar \equiv c \mod P$ with $\deg(c) < \deg(P)$. Then $ar = kP + c$ for some polynomial k, and so $k = \left[\frac{ra}{P}\right]$ and $(\frac{c}{p})_d = (\frac{ar}{p})_d = (\frac{a}{p})_d$. Let C_a denote the product of all such polynomials c. Thus we get

$$\begin{aligned} C_a &= \prod_{\substack{\deg(r)<\deg(P),\\ (\frac{r}{P})_d=1}} \left(ar - P\left[\frac{ar}{P}\right]\right) \\ &= a^{\frac{|P|-1}{d}} \prod_{\substack{\deg(r)<\deg(P),\\ (\frac{r}{P})_d=1}} r \prod_{\substack{\deg(r)<\deg(P),\\ (\frac{r}{P})_d=1}} \left(1 - \frac{P}{ar}\left[\frac{ar}{P}\right]\right). \end{aligned}$$

Write $R = \prod_{\substack{\deg(r)<\deg(P),\\ (\frac{r}{P})_d=1}} r$. The above expression can be simplified as

$$\begin{aligned} \frac{C_a}{R} &= a^{\frac{|P|-1}{d}} \prod_{\substack{\deg(r)<\deg(P),\\ (\frac{r}{P})_d=1}} \left(1 - \frac{P}{ar}\left[\frac{ar}{P}\right]\right) \\ &\equiv a^{\frac{|P|-1}{d}} \left(1 - \sum_{\substack{\deg(r)<\deg(P),\\ (\frac{r}{P})_d=1}} \frac{P}{ar}\left[\frac{ar}{P}\right]\right) \mod P^2. \end{aligned}$$

Hence we find

$$\begin{aligned} & a^{\frac{|P|-1}{d}} P \sum_{\substack{\deg(r)<\deg(P),\\ (\frac{r}{P})_d=1}} \frac{1}{ar}\left[\frac{ar}{P}\right] \\ &\equiv a^{\frac{|P|-1}{d}} - \tfrac{C_a}{R} \mod P^2 \\ &= \left(a^{\frac{|P|-1}{d}} - \left(\tfrac{a}{P}\right)_d\right) - \left(\tfrac{C_a}{R} - \left(\tfrac{a}{P}\right)_d\right) \mod P^2. \end{aligned}$$

Since $a^{\frac{|P|-1}{d}} R \equiv C_a \mod P$,

$$\frac{C_a}{R} \equiv a^{\frac{|P|-1}{d}} \equiv \left(\frac{a}{P}\right)_d \mod P.$$

Dividing both sides by P, we obtain

$$\left(\frac{a}{P}\right)_d \sum_{\substack{\deg(r)<\deg(P),\\ (\frac{r}{P})_d=1}} \frac{1}{ar}\left[\frac{ar}{P}\right] \equiv \frac{a^{\frac{|P|-1}{d}} - \left(\frac{a}{P}\right)_d}{P} - \left(\frac{\frac{C_a}{R} - \left(\frac{a}{P}\right)_d}{P}\right) \mod P,$$

and finally reach

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

To prove the last statement, we observe that as r runs through all polynomials of degree less than $\deg P$ with $(\frac{r}{P})_d = 1$, αr runs through polynomials of degree less than $\deg P$ with $(\frac{\alpha r}{P})_d = (\frac{\alpha}{P})_d = (\frac{a}{P})_d$. Thus $C_a = C_\alpha$ and it follows that

$$\frac{C_a}{R} = \frac{C_\alpha}{R} = \alpha^{\frac{|P|-1}{d}} = \left(\frac{\alpha}{P}\right)_d = \left(\frac{a}{P}\right)_d.$$

Recall from Proposition 3.2 of [5] that $(\frac{\alpha}{P})_d = \alpha^{\frac{q-1}{d}\deg P}$. Therefore we have the congruence

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

as desired. □

Acknowledgment This work grows out of the second author's senior project at Chulalongkorn University written under the direction of the first author to which he expresses his gratitude. The research was supported in part by the Junior Science Talent Project (JSTP). The authors would also like to thank the referee for valuable comments and suggestions which improved the paper.

References

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

[2] H.-Q. Cao and H. Pan, A congruence involving product of q-binomial coefficients, *J. Number Theory* **121** (2006) 224-233.

[3] E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. of Math.* **39** (1938), 350-360.

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

[5] M. Rosen, *Number Theory in Function Fields*, Springer, New York, 2002.

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

[7] A. Wieferich, Zum letzten Fermat'schen Theorem, *J. Reine Angew. Math.* **136** (1909), 293-302.