

ON THE d TH POWER RESIDUE SYMBOL OF FUNCTION FIELDS

SU HU

ABSTRACT. In this short notice, we prove a new result about the d th power residue symbol of function fields, by modifying the method of W. Kohlen in the paper published in Bull. Korean Math. Soc. **45** (2008), no. 2, 273–275.

W. Kohlen [1] gave a short and elementary proof of the existence of infinitely many primes p such that a given positive integer a congruent to 3 modulo 4 is a quadratic non-residue modulo p .

In this short notice, we prove a new result about the d th power residue symbol of function fields by modifying the method of Kohlen [1]. Let q be a power of an odd prime, $A = \mathbb{F}_q[t]$ be the polynomial ring over the finite field \mathbb{F}_q with q elements. Let \mathbb{F}_q^\times be the group of nonzero elements of \mathbb{F}_q , g be a generator of \mathbb{F}_q^\times and d be any divisor of $q - 1$, thus $\eta = g^{\frac{q-1}{d}}$ becomes an element of order d in \mathbb{F}_q^\times . For any irreducible polynomial P in A , define $|P| = q^{\deg P}$. The d th power residue symbol of $\mathbb{F}_q[t]$ is defined as follows [2].

Definition 1. Let $P \in A$ be an irreducible polynomial. $a \in A$ and P does not divide a . Let $(a/P)_d$ be the unique element of \mathbb{F}_q^\times such that

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

If $P|a$ define $(a/P)_d = 0$. The symbol $(\frac{a}{P})_d$ is called the d th power residue symbol.

Now we can state the following main result of this note.

Theorem 2. *Let a be a nonzero polynomial in $\mathbb{F}_q[t]$ and $d \nmid \deg a$. Then for any $i = 0, 1, 2, \dots, d - 1$, there exist infinitely many primes P in $\mathbb{F}_q[t]$ with $d \nmid \deg P$, such that $(\frac{a}{P})_d = \eta^{i \deg P}$.*

When $d = 2$, we have the following result.

Received September 13, 2008; Revised October 11, 2008.

2000 *Mathematics Subject Classification.* 11T55.

Key words and phrases. d th power residue symbol, polynomial ring.

Corollary 3. *Let a be a nonzero polynomial in $\mathbb{F}_q[t]$ with odd degree. Then there exist infinitely many primes in $\mathbb{F}_q[t]$ with odd degree such that $\left(\frac{a}{P}\right)_2 = -1$.*

Now we modify Kohnen's method to give a short and elementary proof of Theorem 2.

Proof. For $x \in \mathbb{R}, x \geq q$, let

$$(1) \quad m = -g^i \left(\prod_{|f| \leq x, a \not\equiv 0 \pmod{f}} f \right)^d + a^\lambda,$$

where in (1) the product over all primes $|f| \leq x$ that do not divide a and λ is a positive integer with $\lambda \equiv 1 \pmod{d}$ such that

$$\deg a^\lambda > \deg \left(\prod_{|f| \leq x, a \not\equiv 0 \pmod{f}} f \right)^d.$$

Thus $\deg m = \lambda \deg a \equiv \deg a \pmod{d}$ and $d \nmid \deg m$.

Let P be a prime dividing m with $d \nmid \deg P$. Then necessarily, by the definition of m , we must have $|P| > x$.

On the other hand, we find from (1)

$$a^\lambda \equiv g^i \left(\prod_{|f| \leq x, a \not\equiv 0 \pmod{f}} f \right)^d \pmod{P}.$$

Thus

$$a^{\lambda \frac{|P|-1}{d}} \equiv g^{i \frac{|P|-1}{d}} \left(\prod_{|f| \leq x, a \not\equiv 0 \pmod{f}} f \right)^{|P|-1} \pmod{P}.$$

From Fermat's Little Theorem (see the corollary of Proposition 1.8 in [2]), we deduce that

$$a^{\lambda \frac{|P|-1}{d}} \equiv g^{i \frac{|P|-1}{d}} \pmod{P}.$$

From the definition of the d th power residue symbol of $\mathbb{F}_q[t]$, we get

$$\left(\frac{a}{P}\right)_d \equiv a^{\frac{|P|-1}{d}} \equiv a^{\frac{|P|-1}{d} \lambda} \equiv g^{i \frac{|P|-1}{d}} \equiv \eta^{i \deg P} \pmod{P}.$$

Which conclude the proof. □

References

- [1] W. Kohnen, *An elementary proof in the theory of quadratic residues*, Bull. Korean Math. Soc. **45** (2008), no. 2, 273–275.
- [2] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, New York, 2002.

DEPARTMENT OF MATHEMATICAL SCIENCES
 TSINGHUA UNIVERSITY
 BEIJING 100084, P. R. CHINA
E-mail address: hus04@mails.tsinghua.edu.cn