GLASNIK MATEMATIČKI
Vol. 46(66)(2011), 11 – 14

kTH POWER RESIDUE CHAINS OF GLOBAL FIELDS

Su Hu and Yan Li
Tsinghua University, China

Abstract. In 1974, Vegh proved that if k is a prime and m a positive integer, there is an m term permutation chain of kth power residue for infinitely many primes (E.Vegh, kth power residue chains, J. Number Theory 9 (1977), 179-181). In fact, his proof showed that $1, 2, 2^2, \ldots, 2^{m-1}$ is an m term permutation chain of kth power residue for infinitely many primes. In this paper, we prove that for any "possible" m term sequence $r_1, r_2, ..., r_m$, there are infinitely many primes p making it an m term permutation chain of kth power residue modulo p, where k is an arbitrary positive integer. From our result, we see that Vegh's theorem holds for any positive integer k, not only for prime numbers. In fact, we prove our result in more generality where the integer ring $\mathbb{Z}$ is replaced by any S-integer ring of global fields (i.e., algebraic number fields or algebraic function fields over finite fields).

1. Introduction

Let K be a global field (i.e., algebraic number field or algebraic function field with a finite constant field). Let S be a finite set of primes of K (if K is an algebraic number field, S contains all the archimedean primes). Let A be the ring of S-integers of K, that is

$$A = \{a \in K | \mathrm{ord}_P(a) \geq 0, \forall P \notin S\}.$$

If K is a number field and S is the set of the archimedean primes of K, then A is just the usual integer ring O_K of K, i.e. the integral closure of $\mathbb{Z}$ in K. It is well known that A is a Dedekind domain. Let P be a nonzero prime ideal of A and k a positive integer. A sequence of elements in A

$$r_1, r_2, \cdots, r_m \tag{1.1}$$

2010 *Mathematics Subject Classification.* 11A15, 11R04, 11R58.
Key words and phrases. kth power residue chain, global field, Chebotarev's density theorem.

for which the $\frac{m(m+1)}{2}$ sums

$$\sum_{k=i}^{j} r_k, 1 \leq i \leq j \leq m,$$

are distinct kth power residues modulo P, is called a chain of kth power residue modulo P. If

$$r_i, r_{i+1}, \cdots, r_m, r_1, r_2, \cdots, r_{i-1}$$

is a chain of kth power residue modulo P for $1 \leq i \leq m$, then we call (1.1) a cyclic chain of kth power residue modulo P. If

$$r_{\sigma(1)}, r_{\sigma(2)}, \cdots, r_{\sigma(m)}$$

is a chain of kth power residues for all permutations $\sigma \in S_m$, then we call (1.1) a permutation chain of kth power residue modulo P. These definitions are generalizations of the classical definitions of kth power residue chains of integers modulo a prime number (see [5]).

Let k, p be prime numbers. In 1974, using Kummer's result on kth power character modulo p with preassigned values, Vegh ([5]) proved the following result for kth power residue chains of integers.

THEOREM 1.1 (Vegh [5]). *Let k be a prime and m a positive integer. There is an m term permutation chain of kth power residue for infinitely many primes.*

By using the result of Mills ([2, Theorem 3]), he showed that this result also holds if the prime k is replaced by other kinds of integers (for example k odd, $k = 4$, or $k = 2Q$, where $Q = 4n + 3$ is a prime). It should be noted that Gupta ([1]) exhibited quadratic residue chains for $2 \leq m \leq 14$ and cyclic quadratic residues for $3 \leq m \leq 6$.

The main result of this paper is the following theorem.

THEOREM 1.2. *Let k and m be arbitrary positive integers. Let $r_1, r_2, ..., r_m$ be a sequence of elements of A such that for all permutations $\sigma \in S_m$,*

$$\text{(1.2)} \qquad \textit{the } m(m+1)/2 \textit{ sums } \sum_{k=i}^{j} r_{\sigma(k)} \ (1 \leq i \leq j \leq m) \textit{ are distinct.}$$

Then $r_1, r_2, ..., r_m$ is an m term permutation chain of kth power residue for infinitely many prime ideals.

REMARK 1.3. By the definition of permutation chain, the condition (1.2) is necessary for $r_1, r_2, ..., r_m$ being a permutation chain of kth power residue.

In Section 2 and 3, we will prove Theorem 1.2 for number fields and function fields, respectively. As a corollary, we get the following theorem which is the generalization of Vegh's Theorem to the case that k is an arbitrary positive integer and A is any S-integer ring of global fields.

COROLLARY 1.4. *Let k and m be arbitrary positive integers. In A, there is an m term permutation chain of kth power residues for infinitely many prime ideals.*

Proof of Corollary 1.4. Number field case: let P be a prime ideal of A and p the prime number lying below P and put

$$r_i = p^{i-1}, \quad i = 1, 2, \cdots m. \tag{1.3}$$

Function field case: let t be any element of A which is transcendental over the constant field of K and put

$$r_i = t^{i-1}, \quad i = 1, 2, \cdots m. \tag{1.4}$$

It is easy to see $r_1, r_2, ..., r_m$ satisfy the condition of Theorem 1.2.

Our main tool for proving Theorem 1.2 is the following Chebotarev's density theorem for global fields (Theorem 13.4 of [3] and Theorem 9.13A of [4]).

THEOREM 1.5 (Chebotarev). *Let L/K be a Galois extension of global fields with* $\mathrm{Gal(L/K) = H}$. *Let $C \subset H$ be a conjugacy class and S_K be the set of primes of K which are unramified in L. Then*

$$\delta(\{\mathfrak{p} \in S_K | (\mathfrak{p}, L/K) = C\}) = \frac{\#C}{\#H},$$

where δ means Dirichlet density. In particular, every conjugacy class C is of the form $(\mathfrak{p}, L/K)$ for infinitely many places $\mathfrak{p}$ of K.

2. PROOF OF THE MAIN RESULT FOR NUMBER FIELDS

Let

$$\mathscr{E} = \{\sum_{k=i}^{j} r_{\sigma(k)} |\ \sigma \in S_m,\ 1 \le i \le j \le m\}. \tag{2.1}$$

Define

(2.2)

$$\mathscr{P} = \{P \mid P \text{ is a prime ideal of } A \text{ and } \exists\ c_i, c_j \in \mathscr{E}, c_i \neq c_j \text{ s.t. } P | c_i - c_j\}.$$

It is easy to see that $\mathscr{P}$ is a finite set of prime ideals of A and the elements in $\mathscr{E}$ modulo P are not equal if $P \notin \mathscr{P}$.

Let ζ_k be a primitive kth roots of unity. Let $L = K(\zeta_k, \sqrt[k]{\mathscr{E}})$. Then L/K is a Kummer extension. By Chebotarev's density theorem, there are infinitely many prime ideals P in A such that P splits completely in L. Let B be the integral closure of A in L and $\mathfrak{P}$ be a prime ideal of B lying above P. Then

$$\frac{B}{\mathfrak{P}} \cong \frac{A}{P}. \tag{2.3}$$

But we have

$$c \equiv (\sqrt[k]{c})^k \bmod \mathfrak{P},\ \forall c \in \mathscr{E}, \tag{2.4}$$

that is, c is a kth power residue in $B/\mathfrak{P}$. From (2.3), c is also a kth power residue in A/P.

Let $\mathscr{M}$ be the infinite set of all the prime ideals of A which split completely in L. From the above discussion, it follows that the infinite set $\mathscr{M} - \mathscr{P}$ satisfies our requirement. That is to say all the elements in $\mathscr{E}$ are distinct kth power residues for any prime P in $\mathscr{M} - \mathscr{P}$. Hence, $r_1, r_2, ..., r_m$ is an m term permutation chain of kth power residue for all the prime ideals $P \in \mathscr{M} - \mathscr{P}$.

3. Proof of the main result for function fields

Let K be a global function field with a constant field $\mathbb{F}_q$, where $q = p^s$, p is a prime number.

1) If $(k, p) = 1$. We can prove that the sequence $r_1, r_2, ..., r_m$ is a permutation chain of kth power residue for infinitely many prime ideals of A by the same reasoning as in the Section 2.

2) If $p|k$. Let $k = p^t k'$ and $(k', p) = 1$. Let P be a prime ideal of A and a be any element of A. Since the characteristic of the residue field is p, it is easy to see that a is a kth power residue modulo P if and only if a is a k'th power residue modulo P. Since the theorem holds for k' from 1), it also holds for k. Thus, we have finished the proof in this case.

References

[1] H. Gupta, *Chains of quadratic residues*, Math. Comp. **25** (1971), 379–382.
[2] W. H. Mills, *Characters with preassigned values*, Canad. J. Math. **15** (1963), 169–171.
[3] J. Neukrich, Algebraic number theory, Springer-Verlag, Berlin, 1999.
[4] M. Rosen, Number theory in function fields, Springer-Verlag, New York, 2002.
[5] E. Vegh, *kth–power residue chains*, J. Number Theory **9** (1977), 179–181.

S. Hu
Department of Mathematical Sciences
Tsinghua University
Beijing 100084
China
E-mail: hus04@mails.tsinghua.edu.cn

Y. Li
Department of Mathematical Sciences
Tsinghua University
Beijing 100084
China
E-mail: liyan_00@mails.tsinghua.edu.cn

Received: 15.11.2009.