ON PRIMITIVE NORMAL ELEMENTS OVER FINITE FIELDS

ANJU

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
OCTOBER 2017

ON PRIMITIVE NORMAL ELEMENTS OVER FINITE FIELDS

by

ANJU

Department of Mathematics

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Delhi
October 2017

Dedicated to

My Family

Certificate

This is to certify that the thesis entitled **"On Primitive Normal Elements over Finite Fields"** submitted by **Ms. Anju** to the Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy**, is a record of the original bonafide research work carried out by her under my supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other University or Institute for the award of any degree or diploma.

Dr. R. K. Sharma
Professor
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi 110 016

Acknowledgements

I am taking this opportunity to express my deep gratitude to all those who have supported me throughout the course of completing my PhD thesis. First and foremost, I would like to thank almighty God for giving me strength, ability and opportunity to undertake this research work and complete it successfully. Without His blessings, this would not have been possible.

I would like to express my deepest gratitude to my thesis supervisor Prof. R. K. Sharma for his patient guidance, enthusiastic encouragement and useful suggestions during the planning and development of this research work. His willingness to give his time so generously has been very much appreciated.

I would like to give my special thanks to my SRC (Student Research Committee) members Prof. A. Mehra, Dr. R. Sarma and Prof. Maithilisaran for sparing their valuable time whenever I approached them for their suggestions. I am greatly indebted to all faculty members of Department of Mathematics IIT Delhi, for their co-operation and support. Many thanks to CSIR-UGC and IIT Delhi authorities for providing me the research fellowship and necessary facilities all through the PhD program. It was fantastic to have the opportunity to do my research work in your facilities.

The co-operation, moral support and constant encouragements, I have always received from my friends and juniors can not be expressed in words and I feel lucky to be blessed with such wonderful people. I immensely express my heartiest thanks to my all close friends for all their lively discussions and support.

I appreciate all my seniors for making me comfortable in the department and motivating in the

initial days of my research. I would like to give my heartily thanks to Dr. Alok Mishra in overcoming the initial hurdles of research orientation. I am highly thankful to my colleagues and friends, Reetu, Meenu, Seema, Swati, Arti Singh, Arti Pandey, Anubha Jindal, Swati Sidana, Chirag, Rohit, Yogesh, Shailesh, Ambrish Awasthi, Manisha Shrivastava for encouraging me and creating joyful environment in this duration. I would like to give a special thanks to Vishal Kumar Yadav for helping me in the initial stage of my research work. I can never forget to thank my friends, Seema Choyal, Anju Dalal, Sapna and Rekha for their never ending support.

Finally, this thesis might not exist at all without unconditional love and support of my family. It was the patience and silent sacrifice of my father and mother, which led me to complete this journey. My achievements are outcome of their dedication and their belief in my potentials. I would like to thank my uncle and aunt for their support and care. Without them, it would not have been possible. Thanks to my brothers Manish and Ashish, my cousins Kajal, Pooja and Sahil for their love and kindness through this long process. Last but not the least, I acknowledge my deep gratitude to my beloved grandfather, grandmother for their everlasting blessings which lead me to reach this milestone.

New Delhi *(Anju)*

Abstract

Primitive elements and normal elements are of great importance in coding theory and cryptography. Primitive elements play a very important role in cryptosystems based on the multiplicative cyclic groups of non zero elements of a finite field. For example ElGamal cryptosystem, and Diffie-Hellman key exchange protocol use this group. Let $\mathbb{F}_{q^n}$ be an extension of the field $\mathbb{F}_q$ of degree n, where $q = p^k$ for some positive integer k and prime p. The advantage of using normal basis representation yields efficient exponentiation, as the q-th powers of elements are given by a cyclic bit-shift of the corresponding coordinate vector. Let $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times 3}(\mathbb{F}_q)$ ($q = 2^k$ for some positive integer k) be a matrix of rank 2. In this thesis, we obtain a sufficient condition for the existence of a primitive element $\alpha \in \mathbb{F}_q$ such that the element $(a\alpha^2+b\alpha+c)/(d\alpha+e)$ is a primitive element of $\mathbb{F}_q$, and using that condition, we prove that every $\mathbb{F}_q$ ($q = 2^k$) contains such a primitive element except for finitely many cases. We also establish existence of a primitive normal element α of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that $(a\alpha^2+b\alpha+c)/(d\alpha+e)$ is a primitive element of $\mathbb{F}_{q^n}$ for $A \in M_{2\times 3}(\mathbb{F}_{q^n})$. Further we discuss existence of a primitive pair $(\alpha, \alpha + \alpha^{-1})$ in $\mathbb{F}_{q^n}$ such that the trace, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ is any prescribed element of $\mathbb{F}_q$. We also consider the problem regarding the existence of a primitive pair of the form $(\alpha, (a\alpha^2 + b\alpha + c)/(d\alpha + e))$, such that $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ and $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^{-1})$ are any prescribed elements of $\mathbb{F}_q$. Finally, we prove that the number of self-dual normal bases generators of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ in

$(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_{q^m}})^{-1}(\beta)$ $(n = mp^l,\ l \geq 1)$, for any self-dual normal basis generator β of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, is independent of the choice of β.

सारांश

क्रिप्टोग्राफी और कोडिंग के सिद्धांतों में प्रीमिटिव तत्वों और नॉर्मल तत्वों का बहुत महत्वपूर्ण स्थान है। प्रीमिटिव तत्व परिमित फील्ड के शून्य के अतिरिक्त तत्वों के चक्रीय समूह पर आधारित क्रिप्टो निकायों में महत्वपूर्ण भूमिका निभाते हैं। उदाहरण के लिए एलगामल क्रिप्टोसिस्टम और डिफ़ी हैल्ल्मेन कुंजी विनिमय प्रोटोकॉल इस समूह का उपयोग करते हैं। मान लीजिये कि $\mathbb{F}_{q^n}$, $\mathbb{F}_q$ का डिग्री n का एक एक्स्टेंसन है, जहाँ पर किसी धनात्मक पूर्णांक k और अभाज्य संख्या p के लिए, $q = p^k$ है। नॉर्मल प्रतिनिधित्व का उपयोग करने का लाभ यह है कि यह कुशल घातांक प्रदान करता है, चूंकि तत्वों की q-th घात संबंधित वेक्टर निर्देशांक की चक्रीय बिट-शिफ्ट द्वारा दी जाती हैं। मान लीजिये $A = \begin{pmatrix} a & b & c \\ 0 & d & e \end{pmatrix} \in M_{2\times3}(\mathbb{F}_q)$ $(q = 2^k,$ किसी धनात्मक पूर्णांक k के लिए$)$, रैंक 2 का एक आव्यूह है। इस शोध प्रबंध में, हम किसी ऐसे प्रीमिटिव तत्व $\alpha \in \mathbb{F}_q$, जिसके लिए $(a\alpha\text{^}2 + b\alpha + c)/(d\,\alpha + e)$ भी $\mathbb{F}_q$ का प्रीमिटिव तत्व हो जाए, की उपस्थिति के लिए पर्याप्त नियम खोजते हैं, और उस नियम का उपयोग करते हुए हम यह सिद्ध करते हैं कि कुछ सीमित अवस्थाओं के अतिरिक्त, प्रत्येक $\mathbb{F}_q$ $(q = 2^k)$ में ऐसे प्रीमिटिव तत्व उपस्थित हैं। हम $A \in M_{2\times3}(\mathbb{F}_{q^n})$ के लिए $\mathbb{F}_{q^n}$ के $\mathbb{F}_q$ पर एक ऐसे प्रीमिटिव नॉर्मल तत्व α, जिसके लिए $(a\alpha^2 + b\alpha + c) / (d\,\alpha + e)$ भी $\mathbb{F}_{q^n}$ का प्रीमिटिव तत्व हो जाए, की उपस्थिति भी स्थापित करतें हैं। तदोपरांत हम ऐसे प्रीमिटिव युग्म $(\alpha,\alpha+\alpha^{-1})$ की उपस्थिति की भी चर्चा करतें हैं जिसका ट्रेस, $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$, फील्ड $\mathbb{F}_q$ का कोई भी निर्धारित सदस्य हो। हम ऐसे प्रीमिटिव युग्म $(\alpha, (a\alpha^2 + b\alpha + c) /(d\,\alpha + e))$, कि $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ और $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^{-1})$, फील्ड $\mathbb{F}_q$ के कोई भी निर्धारित सदस्य हैं, के अस्तित्व के विषय में भी विचार करते हैं । अंत में हम यह सिद्ध करतें हैं कि $\mathbb{F}_{q^m}$ के $\mathbb{F}_q$ पर किसी सेल्फ-डुयल नॉर्मल बेसिस प्रतिनिधि β के लिए, $(Tr_{\mathbb{F}_{q^n}/\mathbb{F}_{q^m}})^{-1}(\beta)$ $(n = mp^l, l \geq 1)$, में $\mathbb{F}_{q^n}$ के $\mathbb{F}_q$ पर सेल्फ-डुयल नॉर्मल बेसिस प्रतिनिधियों कि संख्या β के चुनाव से स्वतंत्र है।

Contents

i

Certificate **i**

Acknowledgements **iii**

Abstract **v**

List of Tables **xiii**

List of Symbols **xv**

1 Introduction **1**

1.1 A Brief Survey of the Literature 3

1.2 A Brief Overview of the Thesis 6

2 Existence of Primitive Pairs **9**

2.1 Motivation 9

2.2 Preliminaries 10

2.3 Main Results 12

2.3.1 Existence of Primitive Pairs $(\alpha, \lambda_A(\alpha))$ in $\mathbb{F}_q$ 13

2.3.2 $\mathbb{F}_q$ with Primitive Pairs $(\alpha, \lambda_A(\alpha))$ 20

2.3.3 Particular Case: Existence of Primitive Pairs $(\alpha, \alpha^2+\alpha+1)$. 22

3 Existence of Primitive Pairs under Certain Condition 25

3.1 Motivation 26

3.2 Preliminaries 27

3.3 Main Results 30

3.3.1 Existence of Primitive Pairs $(\alpha, \lambda_A(\alpha))$ with α Normal over $\mathbb{F}_q$ 30

3.3.2 $\mathbb{F}_{q^n}$ with Primitive Pairs $(\alpha, \lambda_A(\alpha))$ such that α is Normal over $\mathbb{F}_q$ 35

3.3.3 Particular Case: Primitive pairs $(\alpha, \alpha^2+\alpha+1)$ with α Normal 49

4 Existence of Primitive Pairs with Prescribed Trace I 51

4.1 Motivation 52

4.2 Preliminaries 53

4.3 Main Results 53

4.3.1 Computations 58

5 Existence of Primitive Pairs with Prescribed Trace II 67

5.1 Preliminaries 68

5.2 Main Results 68

5.2.1 Computations 72

6 Self-Dual Normal Bases 79

6.1 Motivation 80

6.2 Preliminaries 81

6.3 Main Results 83

7 Conclusion and Future Research 87

7.1 Contributions of the Thesis 87

7.2 Future Research 90

Bibliography **93**

Appendices **99**

Curriculum Vitae **111**

List of Tables

2.1 Values of k with 2^k satisfying (2.12) 22

3.1 (q, n) such that $n'|q-1$ 45
3.2 (q, n) such that $n' \nmid q-1$ 47

4.1 Pairs $(2^k, n)$ satisfying (4.8) 64

5.1 Pairs $(2^k, n)$ satisfying (5.8) 76

List of Symbols

$\mathbb{N}$	the set of natural numbers
$\mathbb{Z}$	the set of integers
$\mathbb{Q}$	the set of rational numbers
$\mathbb{R}$	the set of real numbers
q	a prime power
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\forall\ x$	for all x
$\lvert S \rvert$	cardinality, i.e., number of elements of the finite set S
$x \in X$	x is a member of X
$x \notin X$	x is not a member of X
$A \subset R$	A is a proper subset of R
$A \subseteq R$	A is a subset of R
$A \nsubseteq R$	A is not a subset of R
$a \equiv b \pmod{n}$	a is congruent to b modulo n
$\gcd(k_1, k_2, \ldots, k_n)$	the greatest common divisor of $k_1, \ldots, k_n$
$\phi(n)$	Euler's phi-function of n
$\mathbb{Z}_n$	the group of integers modulo n
$\mathcal{U}(\mathbb{Z}_n)$	the multiplicative group of integers modulo n

$\langle a \rangle$	the cyclic group generated by a
$=$	equal to
$\neq$	not equal to
$\mathbb{F}_q$, $GF(q)$	finite field with q elements
$\mathbb{F}_q^*$	the multiplicative group of nonzero elements of $\mathbb{F}_q$
$C(n,q)$	the group of $n \times n$ circulant matrices over $\mathbb{F}_q$
$OC(n,q)$	the group of $n \times n$ orthogonal circulant matrices over $\mathbb{F}_q$
$Tr_{\mathbb{F}/K}(\alpha)$	the trace of $\alpha \in \mathbb{F}$ over K
$SDN(n,q)$	the number of self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$
A^T	Transpose of matrix A
Rank(A)	Rank of matrix A
$char(R)$	characteristic of R
$\omega(m)$	number of distinct prime divisors of m
$\Omega_q(f(x))$	number of distinct monic irreducible divisors of $f(x)$ over $\mathbb{F}_q$