EXISTENCE OF PRIMITIVE NORMAL ELEMENTS WITH SOME PROPERTIES IN FINITE FIELDS

AAKASH CHOUDHARY

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI

MARCH 2024

EXISTENCE OF PRIMITIVE NORMAL ELEMENTS WITH SOME PROPERTIES IN FINITE FIELDS

by

AAKASH CHOUDHARY

Department of Mathematics

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

Indian Institute of Technology Delhi

March 2024

Dedicated to
my family

Certificate

This is to certify that the thesis entitled "**EXISTENCE OF PRIMITIVE NORMAL ELEMENTS WITH SOME PROPERTIES IN FINITE FIELDS**" submitted by "**Mr. AAKASH CHOUDHARY**" to **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 him 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.

New Delhi
March 2024

Dr. R.K. Sharma
Professor
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi 110016

Acknowledgments

I take immense pleasure in conveying my heartfelt appreciation to everyone who has stood by me throughout my journey in completing my Ph.D. thesis. To begin, I wish to express my deep reverence and heartfelt appreciation to Prof. R.K. Sharma, my thesis supervisor, for introducing me to the captivating realm of mathematics and for providing expert guidance throughout my Ph.D. journey. I am appreciative of the autonomy he granted me in pursuing my research. I owe a debt of gratitude to Dr. Hariom Sharma and Dr. Anju Gupta for their support whenever I sought their assistance.

A special note of gratitude goes out to the members of my Student Research Committee (SRC), namely Prof. Ritumoni Sarma, Prof. Amit Priyadarshi, and Prof. A.K. Shukla. Their dedication, support, cooperation, and precious time devoted to my research work were instrumental in its progress. I would like to thank all of the instructors who taught me during my Ph.D. Coursework. I thank IIT Delhi for all of the resources and financial assistance.

I would like to express my gratitude to my senior colleagues for their warm welcome and encouragement during the early stages of my research. I would like to extend my heartfelt appreciation to my dear friend Jyotsna for her unwavering support and countless insightful discussions. Her valuable insights and thoughtful conversations have been instrumental in shaping my ideas and perspectives. I am also deeply appreciative of my senior, juniors, friends, and peers, including Himanshu, Manuj, Gurdev, Santosh, Gyanendra, Divay, Prabhakar, Tanvi, Sakshi, Anisha, Manisha, for their motivating presence and for creating a joyful atmosphere during this period. It is challenging to individually thank each friend here, but I want them to know that the cherished memories of our friendship will forever reside in the deepest recesses of my heart.

It is impossible to put into words the depth of my love and appreciation for my family, who have consistently provided unwavering support and encouragement. My accomplishments owe everything to the quiet *sacrifices and enduring patience of my parents. I want to express my appreciation to my friends Ashu, Sagar, Devkaran, Mudit for their encouragement and unwavering support.*

Lastly, I wish to express my gratitude to the Lord Hanuman for bestowing upon me the strength, capability, and opportunity to embark on this research endeavor and successfully bring it to fruition.

New Delhi Aakash Chodhary

Abstract

Given q a prime power and $n \in \mathbb{N}$, suppose $\mathbb{F}_{q^n}$ represents a field extension of degree n over $\mathbb{F}_q$. The multiplicative group $\mathbb{F}_{q^n}^*$ of $\mathbb{F}_{q^n}$ is cyclic, and its generator is referred to as a primitive element in $\mathbb{F}_{q^n}$. Let r be a divisor of $q^n - 1$, then an element $\epsilon \in \mathbb{F}_{q^n}$ with multiplicative order $\frac{q^n-1}{r}$ is referred to as a r-primitive in $\mathbb{F}_{q^n}$. It is evident that for a primitive element $\epsilon \in \mathbb{F}_{q^n}$ and $r \mid q^n - 1$, the element ϵ^r is an r-primitive element. There are precisely $\phi(\frac{q^n-1}{r})$ such elements in $\mathbb{F}_{q^n}$, where ϕ is the Euler-totient function. An element $\epsilon \in \mathbb{F}_{q^n}$ is said to be a normal element in $\mathbb{F}_{q^n}$ if the set $V_\epsilon = \{\epsilon, \epsilon^q, \epsilon^{q^2}, \ldots, \epsilon^{q^{n-1}}\}$ acts as a basis for the vector space $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. It is well known that $\epsilon \in \mathbb{F}_{q^n}$ is normal element if the greatest common divisor of the polynomial $\sum_{i=0}^{n-1} \epsilon^{q^i} x^{n-i-1}$ with $x^n - 1$ is 1 in $\mathbb{F}_{q^n}$. Let $0 \leq k \leq n-1$, then an element $\epsilon \in \mathbb{F}_{q^n}$ is said to be a k-normal element if the greatest common divisor of the polynomial $\sum_{i=0}^{n-1} \epsilon^{q^i} x^{n-i-1}$ with $x^n - 1$ has degree k in $\mathbb{F}_{q^n}[x]$. For $\epsilon \in \mathbb{F}_{q^n}$, the trace of ϵ over $\mathbb{F}_q$ denoted by $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\epsilon)$ is defined as $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\epsilon) = \epsilon + \epsilon^q + \epsilon^{q^2} + \cdots + \epsilon^{q^{n-1}}$, and the norm of ϵ over $\mathbb{F}_q$ denoted by $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\epsilon)$, is defined as $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\epsilon) = \epsilon \cdot \epsilon^q \cdot \epsilon^{q^2} \cdots \epsilon^{q^{n-1}}$. This thesis concentrates to work on the existence of primitive pair, the existence of r-primitive k-normal pair and the existence of a finite arithmetic progression of r-primitive elements with first term being k-normal, with prescribed traces and norms in finite fields.

In this thesis, for $n, m \in \mathbb{N}$ such that $n \geq 7$, $m \leq q^n$ and a rational function $f = f_1/f_2$, where f_1 and f_2 are relatively prime, irreducible polynomials with $\deg(f_1) + \deg(f_2) = m$ in $\mathbb{F}_{q^n}[x]$, we obtained a sufficient condition on (q, n) which guarantees primitive pairing $(\epsilon, f(\epsilon))$ exists in $\mathbb{F}_{q^n}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\epsilon) = a$ and $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(f(\epsilon)) = b$ for any prescribed $a, b \in \mathbb{F}_q$. Further, we demonstrated that for any positive integer $m \leq q^n$ such a pair definitely exists for large n. The scenario when $m = 2$ is handled separately and we verified that such a pair exists for all (q, n) except from possible 71 values of (q, n). We have also given a similar result for $m = 3$. Further in this thesis, for $n, r_1, r_2, m_1, m_2 \in \mathbb{N}$, $k_1, k_2 \in \mathbb{N} \cup \{0\}$, a rational function $F = \frac{F_1}{F_2}$ in $\mathbb{F}_{q^n}(x)$

with $\deg(F_i) \leq m_i$ $(i = 1, 2)$ satisfying some conditions, and $a, b \in \mathbb{F}_q$, we established a sufficient condition that ensures the existence of an r_1-primitive k_1-normal element $\epsilon \in \mathbb{F}_{q^n}$ such that trace of ϵ is a and that of ϵ^{-1} is b with image of ϵ under F is r_2-primitive k_2-normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Further, for $m_1 = 10,\ m_2 = 11,\ r_1 = 3,\ r_2 = 2,\ k_1 = 2,\ k_2 = 1$, we established bounds on q for various n to determine the existence of such elements in $\mathbb{F}_{q^n}$. Furthermore, in finite fields of characteristic 13, we identified all such pairs (q, n) with 10 possible exceptions. We have also derived an explicit lower bound $q_0(n)$ on q for the existence of such elements in $\mathbb{F}_{q^n}$. Furthermore, we established the existence of m-term arithmetic progression $\epsilon, \epsilon + \zeta, \ldots, \epsilon + (m-1)\zeta$ in $\mathbb{F}_{q^n}$ such that its i^{th} term is r_i-primitive and first term being k-normal with prescribed trace of it and its inverse. Further, we demonstrated an example with $m = 3,\ r_i = 5$ $(i = 1, 2, 3)$ and $k = 3$ verifying the existence of such elements with the exception of possible 6 values of (q, n) in fields of characteristics 13. Also in this thesis, for prescribed primitive elements $a, b \in \mathbb{F}_q$, we proved the existence of primitive pairs $(\epsilon, f(\epsilon))$ in $\mathbb{F}_{q^n}$ with norm of ϵ is a and that of $f(\epsilon)$ is b, where $f \in \mathbb{F}_{q^n}(x)$ is a rational function with some restrictions. We also derived a sufficient condition, with an improvement, for the existence of such pairs when $f \in \mathbb{F}_{q^n}(x)$ is even or odd, $q \equiv 3 (\bmod 4)$ and n is an odd positive integer.

सार

मान लीजिए q एक अभाज्य घात है, और $n \in N$ है। मान लीजिए F_q के डिग्री n के फील्ड एक्सटेंशन का प्रतिनिधित्व F_{q^n} करता है। F_{q^n} का गुणक समूह $F^*_{q^n}$ चक्रीय है, और इसके जनरेटर को F_{q^n} का प्रीमिटिव तत्व कहते है। मान लीजिए r q^n-1 का भाजक है, तो तत्व $\varepsilon \in F_{q^n}$, जिसका मल्टीप्लिकेटिव ऑर्डर $(q^n-1)/r$ है, को r-प्रीमिटिव तत्व कहा जाता है। यह स्पष्ट है कि प्रीमिटिव तत्व $\varepsilon \in F_{q^n}$ और $r \mid (q^n-1)$ के लिए, तत्व ε^r एक r-प्रीमिटिव तत्व है। F_{q^n} में ऐसे तत्वों की संख्या $\varphi((q^n-1)/r)$ होती है, जहाँ φ यूलर का फलन-समीकरण है। एक तत्व $\varepsilon \in F_{q^n}$ को एक नॉर्मल तत्व कहा जाता है यदि सेट $V_\varepsilon=\{\varepsilon, \varepsilon^q, \varepsilon^{q^2}, \dots, \varepsilon^{q^{n-1}}\}$, F_q के ऊपर सदिश समष्टि F_{q^n} के लिए बेसिस के रूप में कार्य करता है। यह सर्वविदित है कि $\varepsilon \in F_{q^n}$ नॉर्मल तत्व है यदि बहुपद $\varepsilon x^{n-1} + \varepsilon^q x^{n-2} + \dots + \varepsilon^{q^{n-2}} x + \varepsilon^{q^{n-1}}$ का सबसे बड़ा सामान्य भाजक $x^n - 1$ के साथ $F_{q^n}[x]$ में 1 है। मान लीजिए $0 \le k \le n-1$, तो एक तत्व $\varepsilon \in F_{q^n}$ को k-नॉर्मल तत्व कहा जाता है, यदि बहुपद $\varepsilon x^{n-1} + \varepsilon^q x^{n-2} + \dots + \varepsilon^{q^{n-2}} x + \varepsilon^{q^{n-1}}$ का सबसे बड़ा सामान्य भाजक $x^n - 1$ के साथ $F_{q^n}[x]$ में डिग्री k का है। $\varepsilon \in F_{q^n}$ के लिए, F_q पर ε का ट्रेस, जिसे $Tr_{F_{q^n}/F_q}(\varepsilon)$ से निरूपित करते हैं, $Tr_{F_{q^n}/F_q}(\varepsilon) = \varepsilon + \varepsilon^q + \varepsilon^{q^2} + \dots + \varepsilon^{q^{n-1}}$ के रूप परिभाषित है, तथा F_q पर ε का नॉर्म, जिसे $N_{F_{q^n}/F_q}(\varepsilon)$ से निरूपित करते हैं, $N_{F_{q^n}/F_q}(\varepsilon) = \varepsilon * \varepsilon^q * \varepsilon^{q^2} * \dots * \varepsilon^{q^{n-1}}$ के रूप परिभाषित है। इस थीसिस में, फाइनाइट फील्ड्स में प्रीमिटिव युग्मन की अस्तित्व, r-प्रीमिटिव k-नॉर्मल युग्मन की अस्तित्व और एक सीमित अंकगणितीय प्रगति जिसके सारे घटक r_i-प्रीमिटिव तथा पहला घटक k-नॉर्मल है, निर्धारित ट्रेस और नॉर्म के साथ की अस्तित्व के काम पर ध्यान केंद्रित है।

इस थीसिस में, $n, m \in N$ इस प्रकार कि $n \ge 7$, $m \le q^n$ और एक परिमेय फलन $f = f_1/f_2$, जहां f_1 और f_2 अपेक्षाकृत अभाज्य, अप्रासंगिक बहुपद है जिसका $F_{q^n}[x]$ में डिग्री(f_1)+डिग्री$(f_2)=m$ है, के लिए हमने (q, n) पर एक पर्याप्त शर्त प्राप्त की है जो गारंटी देती है कि F_{q^n} में प्रीमिटिव युग्मन $(\varepsilon, f(\varepsilon))$ इस प्रकार मौजूद है कि किसी निर्धारित $a, b \in F_q$ के लिए $Tr_{F_{q^n}/F_q}(\varepsilon)=a$ और $Tr_{F_{q^n}/F_q}(f(\varepsilon))=b$ है। इसके अलावा, हमने प्रदर्शित किया है कि किसी भी धनात्मक पूर्णांक $m \le q^n$ के लिए ऐसा युग्मन निश्चित रूप से बड़े n के लिए मौजूद है। केस $m = 2$ को अलग से संभाला गया है और हमने सत्यापित किया है कि ऐसा युग्मन सभी (q, n) के लिए मौजूद है, (q, n) के संभावित 71 मानों को छोड़कर। हमने $m = 3$ के लिए भी ऐसा ही परिणाम दिया है। आगे इस थीसिस में, $n, r_1, r_2, m_1, m_2 \in N$, $k_1, k_2 \in N \cup \{0\}$, एक परिमेय फलन $F=F_1/F_2 \in F_{q^n}(x)$ जिसमे डिग्री$(F_i) \le m_i$ $(i = 1, 2)$ और कुछ शर्तों के साथ, और $a, b \in F_q$, के लिए, हमने ऐसी पर्याप्त स्थिति स्थापित कि जो r_1-प्रीमिटिव k_1-नॉर्मल तत्व $\varepsilon \in F_{q^n}$ के अस्तित्व को सुनिश्चित करती है, जिसमे ε का ट्रेस a और ε^{-1} का ट्रेस b, और F_{q^n} में $F(\varepsilon)$ r_2-प्रीमिटिव k_2-नॉर्मल हो। इसके अलावा, $m_1=10$, $m_2=11$, $r_1=3$, $r_2=2$, $k_1=2$, $k_2=1$ के लिए, हमने F_{q^n} में ऐसे तत्वों के अस्तित्व को निर्धारित करने के लिए विभिन्न n के लिए हमने q पर बाउंड्स स्थापित किये। इसके अलावा, कैरैक्टरिस्टिक्स 13 के फाइनाइट फील्ड्स में हमने 10 संभावित अपवादों के साथ ऐसे सभी युग्मन (q,n) की पहचान की। हमने F_{q^n} में ऐसे तत्वों के अस्तित्व के लिए q के ऊपर एक स्पष्ट निचला सीमा $q_o(n)$ को भी निर्धारित किया है। इसके अतिरिक्त, हमने F_{q^n} में m–अंकीय अंकगणितीय प्रगति $\varepsilon, \varepsilon+\zeta, \dots, \varepsilon+(m-1)\zeta$ का अस्तित्व स्थापित किया है जिसका iवां तत्व r_i-प्रीमिटिव, पहला तत्व k-नॉर्मल है, और जहाँ ε और उसके इनवर्स का ट्रेस पूर्व निर्धारित है। आगे, हमने $m=3$, $r_i=5$ $(i=1,2,3)$ और $k=3$ के साथ एक उदाहरण प्रस्तुत किया, जिसमें कैरैक्टरिस्टिक्स 13 के फाइनाइट फील्ड में (q,n) के संभावित 6 मूल्यों को छोड़कर, ऐसे तत्वों की मौजूदगी का सत्यापन किया। इस थीसिस में, निर्दिष्ट प्रीमिटिव तत्वों $a, b \in F_q$ के लिए,

हमने सिद्ध किया कि F_{q^n} में **प्रीमिटिव युग्मन** $(\varepsilon, f(\varepsilon))$ का अस्तित्व है जिसमें ε का नार्म a और $f(\varepsilon)$ का नार्म b है, जहाँ $f \in F_{q^n}(x)$ कुछ प्रतिबंधों के साथ एक रेशनल फ़ंक्शन है। हमने एक पर्याप्त शर्त भी निकाली है, सुधार के साथ, ऐसे युग्मों के अस्तित्व के लिए जब $f \in F_{q^n}(x)$ सम या विषम हो, $q \equiv 3 (mod 4)$ और n एक विषम धनात्मक पूर्णांक है।

Contents

List of Tables

List of Symbols

Symbol	Meaning
$\mathbb{N}$	The set of natural numbers
$\mathbb{Z}$	The set of Integers
q	a prime power
$\in$	belongs to
$\notin$	does not belong to
$\subseteq$	subset
$\nsubseteq$	not a subset
$\cup, \cap$	union, intersection
$\|A\|$	cardinality of the set A
$A \setminus B$	set difference of A and B
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\gcd(a, b)$	the greatest common divisor of a and b
$\phi(n)$	Euler function of positive integer n
$\mathbb{F}_q$	Finite field with q elements
$\mathbb{F}_q^*$	The multiplicative group of Finite field $\mathbb{F}_q$
$\omega(n)$	number of distinct prime divisors of positive integer n
$\omega(f(x))$	number of distinct irreducible factors of polynomial $f(x)$ over $\mathbb{F}_q$
$W(n)$	number of square-free divisors of positive integer n
$W(f(x))$	number of square-free factors of polynomial $f(x)$ over $\mathbb{F}_q$
$\square$	end of a proof