Finite Fields Containing Elements with Certain Special Properties

JYOTSNA SHARMA

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
JUNE 2024

Finite Fields Containing Elements with Certain Special Properties

by

Jyotsna Sharma

Department of Mathematics

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

Indian Institute of Technology Delhi
June 2024

Dedicated to my mother
Late. Smt. Madhu Sharma

Certificate

This is to certify that the thesis entitled "**Finite Fields containing elements with certain special properties**" submitted by "**Ms. Jyotsna Sharma**" 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 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.

Prof. Ritumoni Sarma
Professor
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi 110016

Prof. Shanta Laishram
Professor
Math Stat Unit
Indian Statistical Institute, 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. Ritumoni Sarma and Prof. Shanta Laishram, my thesis supervisors, for introducing me to the captivating realm of mathematics and for providing expert guidance throughout my Ph.D. journey.

A special note of gratitude goes out to the members of my Student Research Committee (SRC), namely Prof. N. Shravan Kumar, Prof. Surjeet Kour, Prof. Amit Priyadarshi and Prof. S. D. Joshi. 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. Moreover, I want to express my sincere gratitude to the Indian Institute of Technology, Delhi, for providing me with crucial resources, facilities, and granting me access to their extensive library and databases. These provisions played a pivotal role in enabling the successful execution of my research. I also want to acknowledge them for generously supporting my research endeavours through the Research Scholar Travel Award (RSTA). This award enabled me to travel to France to present my research work in 32nd Journées Arithmétiques in Nancy, France.

Primarily, I would like to dedicate this section to convey my deep appreciation for my three dear friends: Sakshi, Poonam, and Tanvi. I am deeply grateful to my dear friend Aakash for his unwavering support and the countless insightful discussions he has facilitated. They not only served as my mentors and steadfast supporters throughout my journey but also became my family at IITD. 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 am also deeply appreciative of my senior, juniors, friends, and peers, including Dr. Vidya Sagar, Himanshu, Manuj, Gurdev, Santosh, Gyanendra, Divay, Prabhakar, Manisha, Aakanksha, Anuj, Ankit 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.

I'd like to express my deepest appreciation to my siblings Dr. Priyanka, Monika and Haardik, who have consistently stood by my side, offering unwavering emotional and professional support throughout my journey. They consistently had faith in me and maintained their belief in every choice I made in my life. I'd also like to extend special thanks to Dr. Abhishek Mishra, my nephew Jai, and my nieces Riya and Chhavi, they were by my side throughout my entire Ph.D. journey, providing invaluable support during challenging times.

Above all, I appreciate God for his mercies and continuous sunshine in my life, which provided me the strength and confidence to complete my thesis.

New Delhi Jyotsna Sharma

Abstract

For q, a prime power, $\mathbb{F}_q$ denotes the field of order q. Then, the group $\mathbb{F}_q^\times := \mathbb{F}_q \setminus \{0\}$ of units of $\mathbb{F}_q$ is cyclic and any generator of this group is referred to as a primitive element of the field. In fact, $\mathbb{F}_q$ has exactly $\varphi(q-1)$ primitive elements, φ being Euler's totient function. Let r be a divisor of $(q-1)$. An r-primitive element in $\mathbb{F}_q$ is an element of $\mathbb{F}_q^\times$ of order $(q-1)/r$. Evidently, if α is a primitive element, then for every divisor r of $(q-1)$, α^r is an r-primitive element so that primitive elements are 1-primitive elements. An element α belonging to the degree n extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is referred to as normal over $\mathbb{F}_q$ if $B_\alpha = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ spans $\mathbb{F}_{q^n}$ as an $\mathbb{F}_q$-vector space. It is necessary and sufficient for $\alpha \in \mathbb{F}_{q^n}$ to be normal over $\mathbb{F}_q$ that the polynomials $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}} x + \alpha^{q^{n-1}}$ and $x^n - 1$ are relatively prime over $\mathbb{F}_{q^n}$. Using this equivalence, the notion of k-normal elements was introduced by Huczynska et. al. in 2003; an element $\alpha \in \mathbb{F}_{q^n}$ is k-normal over $\mathbb{F}_q$ if the gcd of the polynomials $g_\alpha(x)$ and $x^n - 1$ in $\mathbb{F}_{q^n}[x]$ has degree k. Equivalently, an element α beloning to $\mathbb{F}_{q^n}$ is k-normal over $\mathbb{F}_q$ if and only if the span of $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ over $\mathbb{F}_q$ is $(n-k)$-dimensional. Observe that 0-normal elements are normal elements. In the recent time, quite a few people worked on elements that are k-normal or r-primitive or both. It is worth mentioning that, primitive elements have wide applications in coding theory and cryptography. If r is small, an r-primitive element may be used as a replacement of a primitive element in many applications. If for a rational function $f(x)$, both α and $f(\alpha)$ are primitive elements in $\mathbb{F}_q$, the pair $(\alpha, f(\alpha))$, is referred to as a primitive pair; in the past, people studied the existence of such pairs.

In this thesis, we deal with the question of the existence of primitive pair; in fact, we improve the known bounds for even or odd rational functions for $q \equiv 3 \pmod 4$. Further, for r_1, $r_2 > 0$ both dividing $(q^n - 1)$, k_1, $k_2 \geq 0$ such that there are polynomials dividing $(x^n - 1)$ with degrees k_1 and k_2, $a, b \in \mathbb{F}_q$ with $a \neq 0$, we study for a rational function $f(x) \in \mathbb{F}_{q^n}(x)$ the existence of an element in $\mathbb{F}_{q^n}$ which is both k_1-normal and r_1-primitive with its norm equal to a and its

trace equal to b such that its image under f is both k_2-normal and r_2-primitive in $\mathbb{F}_{q^n}$. We obtain an implicit condition on q and n for the existence of such a pair. We discuss a few numerical examples. Moreover, if we impose an additional condition on k_1, k_2, namely, $n \geq 2(k_1 + k_2) + 5$, then for every n such that $x^n - 1$ has divisors of degree k_1 and k_2 and for all but finitely many prime powers q such that $r_1, r_2 \mid q^n - 1$, there exists $\alpha \in \mathbb{F}_{q^n}$ with the desired property. Also, in this thesis, we deal with the existence of r-primitive elements in arithmetic progression by using a new formulation of the characteristic function for r-primitive elements belonging to $\mathbb{F}_q$. In fact, we find a condition on q for the existence of $\alpha \in \mathbb{F}_q^\times$ for a given $n \geq 2$ and $\beta \in \mathbb{F}_q^\times$ such that each of $\alpha, \alpha + \beta, \alpha + 2\beta, \ldots, \alpha + (n-1)\beta \in \mathbb{F}_q^\times$ is r-primitive in $\mathbb{F}_q^\times$. Furthermore, as a consequence, the number of arithmetic progressions in $\mathbb{F}_q$ consisting of r-primitive elements of length n, is asymptotic to $\frac{q}{(q-1)^n}\varphi(\frac{q-1}{r})^n$. Besides, using a traditional method, we improved the existence criterion for such arithmetic progressions in $\mathbb{F}_q$ when $q \equiv 3 \pmod 4$.

सार

एक अभाज्य घात q के लिए, $\mathbb{F}_q$ उस आकार के क्षेत्र को दर्शाता है। तब $\mathbb{F}_q$के गुणा के अन्तर्गत $\mathbb{F}_q^\times := \mathbb{F}_q \setminus \{0\}$ चक्रीय समूह होता है। इस समूह का जनक (generator) इस क्षेत्र का एक प्रिमिटिव सदस्य कहलाता है। वास्तव में, $\mathbb{F}_q$ में $\varphi(q-1)$ प्रिमिटिव सदस्य होते हैं, जहाँ φ ऑइलर का टोशेंट (Euler's totient) फलन है। मान लें $(q-1)$ का एक भाजक r है। $\mathbb{F}_q$ में एक r- प्रिमिटिव सदस्य वह सदस्य होता है जिसका ऑर्डर $(q-1)/r$ होता है। स्पष्टतः, यदि α एक प्रिमिटिव सदस्य है, तो $(q-1)$ के हर भाजक r के लिए, α^r एक r- प्रिमिटिव सदस्य होता है । इसीलिए प्रिमिटिव सदस्य 1- प्रिमिटिव सदस्य होते हैं।अगर $\mathbb{F}_q$ पर $\mathbb{F}_{q^n}$ एक n डिग्री एक्स्टेंशन है, तब $\alpha \in \mathbb{F}_{q^n}$ को $\mathbb{F}_q$ पर नॉर्मल सदस्य कहा जाता है यदि $B_\alpha = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ वेक्टर स्पेस $\mathbb{F}_{q^n}$ को क्षेत्र $\mathbb{F}_q$ पर विस्तारित करता है। $\mathbb{F}_q$ पर $\alpha \in \mathbb{F}_{q^n}$ नॉर्मल होने के लिये यह आवश्यक और पर्याप्त है कि बहुपद $g_\alpha(x) = \alpha x^{n-1} + \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ और $x^n - 1$, $\mathbb{F}_{q^n}$ पर आपस में अभाज्य हों। इस समकक्षता का उपयोग करते हुए, हजंसका (Huczynska) और अन्य ने 2003 में k-नॉर्मल सदस्यों की धारणा को प्रस्तुत किया । $\mathbb{F}_q$ पर, एक सदस्य $\alpha \in \mathbb{F}_{q^n}$, k-नॉर्मल होता है यदि $\mathbb{F}_{q^n}[x]$ में $g_\alpha(x)$ और $x^n - 1$ का उच्चत्तम सामान्य भाजक k डिग्री का हो। अर्थात्, एक सदस्य $\alpha \in \mathbb{F}_{q^n}$, $\mathbb{F}_q$ पर k-नॉर्मल होता है यदि और केवल यदि $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ से विस्तार की हुई वेक्टर स्पेस का $\mathbb{F}_q$-डायमेंशन $(n-k)$ हो। ध्यान दें कि 0-नॉर्मल सदस्य नॉर्मल सदस्य होते हैं। हाल ही में, कई लोगों ने उन सदस्यों पर काम किया है जो k-नॉर्मल या r-प्रिमिटिव या दोनों होते हैं। यह उल्लेखनीय है कि प्रिमिटिव सदस्यों का कोडिंग थ्योरी और क्रिप्टोग्राफी में व्यापक अनुप्रयोग है। यदि r छोटा है, तो कई अनुप्रयोगों में एक r-प्रिमिटिव सदस्य का उपयोग एक प्रिमिटिव सदस्य के स्थान पर किया जा सकता है। यदि एक रेशनल फंक्शन $f(x) \in \mathbb{F}_q(x)$ के लिए, α और $f(\alpha)$ दोनों ही $\mathbb{F}_q$ में प्रिमिटिव सदस्य होते हैं, तो जोड़ी $(\alpha, f(\alpha))$ को प्रिमिटिव जोड़ी कहा जाता है। अतीत में, कई लोगों ने ऐसी जोड़ियों के अस्तित्व का अध्ययन किया था।

इस थीसिस में, हम प्रिमिटिव जोड़ी के अस्तित्व के प्रश्न को सुलझाने का प्रयत्न करते हैं। वास्तव में, हम $q \equiv 3 \pmod 4$ के लिए सम या विषम रेशनल फंक्शन के लिए ज्ञात सीमाओं को बेहतर करते हैं। इसके अलावा, यदि $r_1, r_2 > 0$, दोनों $(q^n - 1)$ को विभाजित करते हों, $k_1, k_2 \geq 0$ ऐसे हों कि $x^n - 1$ के गुणनखंडों के डिग्री k_1 और k_2 हों, और $a, b \in \mathbb{F}_q$ जहां $a \neq 0$ हो, हम एक रेशनल फंक्शन $f(x) \in \mathbb{F}_{q^n}(x)$ के लिए एक सदस्य के अस्तित्व का अध्ययन करते हैं जो $\mathbb{F}_{q^n}$ में k_1-नॉर्मल और r_1- प्रिमिटिव दोनों है जिसका नॉर्म a है और ट्रेस b है ताकि f के तहत α की छवि $\mathbb{F}_{q^n}$ में k_2-नॉर्मल और r_2- प्रिमिटिव दोनों हो। हम ऐसे जोड़े के अस्तित्व के लिए q और n पर एक निहित (implicit) शर्त प्राप्त करते हैं। हम कुछ संख्यात्मक उदाहरणों पर भी चर्चा करते हैं। इसके अलावा, यदि हम k_1, k_2पर एक अतिरिक्त शर्त लागू करते हैं, अर्थात् , $n \geq 2(k_1 + k_2) + 5$, तो प्रत्येक n के लिए और लगभग सभी अभाज्य घातों q के लिए, वांछित गुण रखने वाले $\alpha \in \mathbb{F}_{q^n}$ के अस्तित्व का अध्ययन करते हैं। इस शोध में, हम एक नये करैक्टरस्टिक फंक्शन का उपयोग करके $\mathbb{F}_q$ में अंकगणितीय प्रगति में r-प्राइमिटिव सदस्यों के अस्तित्व का अध्यन करते हैं। वास्तव में, एक दिए गए $n \geq 2$ और $\beta \in \mathbb{F}_q^\times$ के लिए हम $\alpha \in \mathbb{F}_q^\times$ के अस्तित्व के

लिए q पर एक शर्त पाते हैं ताकि प्रत्येक सदस्य $\alpha, \alpha + \beta, \alpha + 2\beta, \ldots, \alpha + (n-1)\beta \in \mathbb{F}_q^{\times}$, r-प्रिमिटिव हो। इसके अलावा, परिणामस्वरूप, $\mathbb{F}_q$ में r- प्रिमिटिव सदस्यों के n लंबाई वालीं अंकगणितीय प्रगति की संख्या, लगभग (asymptotically) $\frac{q}{(q-1)^n}\ \varphi\left(\frac{q-1}{r}\right)^n$ है। इसके अलावा, पारंपरिक विधि का उपयोग करते हुए, हमने ऐसे अंकगणितीय प्रगति के अस्तित्व के निम्न सीमा को बेहतर किया है जब $q \equiv 3\ (mod\ 4)$ हो।

Contents

List of Tables

List of Symbols

Symbol	Meaning
$\mathbb{N}$	The set of natural numbers
$\mathbb{Z}$	The set of integers
$\mathbb{C}$	The set of complex numbers
q	a prime power
$\in$	belongs to
$\notin$	does not belong to
$\cup, \cap$	union, intersection
$\lvert A \rvert$	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
(a, b)	The greatest common divisor of a and b
$\varphi(n)$	Euler's totient function of positive integer n
$\mathbb{F}_q$	Finite field with q elements
$\mathbb{F}_q^\times$	The multiplicative group of the field $\mathbb{F}_q$
$\omega(n)$	The number of distinct prime divisors of positive integer n
$\omega(f(x))$	The number of distinct irreducible factors of polynomial $f(x)$ over $\mathbb{F}_q$
$W(n)$	The number of square-free divisors of positive integer n
$W(f(x))$	The number of square-free factors of polynomial $f(x)$ over $\mathbb{F}_q$
$\mu(n)$	Möbius function for integer n
$\mu_q(f(x))$	Möbius function for rational function $f(x)$ in $\mathbb{F}_q(x)$