# Certain types of primitive and normal elements over finite fields

Himangshu Hazarika

Research Scholar
Department of Mathematical Sciences
Tezpur University

# Outlines

# Definitions

## Primitive element

For any finite field $\mathbb{F}_{q^n}$, its multiplicative group $\mathbb{F}_{q^n}^*$ is cyclic. The generators of $\mathbb{F}_{q^n}^*$ are called *primitive elements* of $\mathbb{F}_{q^n}$.

## Normal element

An element $\alpha \in \mathbb{F}_{q^n}$ is called a *normal element* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}(\mathbb{F}_q)$. This basis is called a *normal basis*.

# Existence theorems

## Normal Basis Theorem

**[Lidl R. and Niederreiter H. , Finite Fields, Cambridge University Press, Cambridge 1998, Theorem 2.36]**
For any finite field $\mathbb{F}_q$ and any finite extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, there exist a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

## Primitive Normal Basis Theorem

**[Cohen, S.D. and Huczynska, S. The primitive normal basis theorem-without a computer, Journal of the London Mathematical Society, 67(1):41-56, 2003]**
In the finite field $\mathbb{F}_{q^n}$, there always exists an element which is simultaneously primitive and normal.

# Previous results

## Result 1

[Hansen-Mullen Conjecture, Hansen, T. and Mullen, G. L. Primitive polynomials over finite fields. Mathematics of Computation, 59(200):639-643, 1992]

Let $m$ and $n$ be positive integers with $m \geq 3$ and $m \geq n \geq 1$. For any given element $a \in \mathbb{F}_q$ with $a \neq 0$ $n = 1$, there exists a monic irreducible polynomial over $\mathbb{F}_q$ of degree $m$ such that the coefficient of $x^{n-1}$ is the given element $a$.

# Previous results

## Result 2

[ Wan D., Generators and irreducible polynomials over finite fields. Mathematics of Computation, 66(219):1195-1212, 1997, Theorem 1.6]
If either $m \geq 36$ or $q \geq 19$, then there is a monic irreducible polynomial in $\mathbb{F}_q[x]$ of the form $g(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ with $a_{n-1} = a$, where $m, n, a$ are as in the Hansen-Mullen conjecture.

# Previous results

## Result 3

[ Cohen, S. D. Kloosterman sums and primitive elements in Galois fields. Acta Arithmetica ,94:173-201, 2000, Lemma 1.1]
Let $q$ be a prime power and $n(\geq 5)$ be an integer. Suppose that arbitrary elements $a$ and $b$ of $\mathbb{F}_{q^n}$ are given. Then there exists a primitive element $\alpha$ of $\mathbb{F}_{q^n}$ such that $T_n(\alpha) = a$ and $T_n(1/\alpha) = b$, except when $a = b = 0$ and $(q, n) = (4, 5), (2, 6)$ and $(3, 6)$, where $T_n(\alpha) := \alpha + \alpha^q + \ldots + \alpha^{q^n-1}$.

# Previous results

## Result 4

[ Cohen, S. D. Kloosterman sums and primitive elements in Galois fields. Acta Arithmetica ,94:173-201, 2000, Lemma 1.2]
Suppose that $q$ is a prime power, $n \geq 5$ and $a_{n-1} = a_1 = 0$ or $q \leq 3$, there exists a primitive polynomial of the form

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

## Result 5

[ Cohen, S. D. Kloosterman sums and primitive elements in Galois fields. Acta Arithmetica ,94:173-201, 2000, Theorem 2] For given $p$, there exist fields $\mathbb{F}_{q^n}$ where $\alpha$ is a primitive element but no element of the form $a\alpha + b$ is a primitive element of $\mathbb{F}_{q^n}$, where $a, b \in \mathbb{F}_{q^n}$.

# Previous results

**Result 6**

[Cohen, S.D. Consecutive primitive roots in a finite field. Proceedings of the American Mathematical Society, 93(2):189-197, 1985 , Theorem 1.2]
Suppose $q(> 4)$ is even. Then for any $\beta$ in $\mathbb{F}_q$, there exists a primitive element $\alpha$ in $\mathbb{F}_q$ such that $\alpha + \beta$ is also primitive in $\mathbb{F}_q$.

**Result 7**

[Cohen S.D. and Huczynska S., The strong primitive normal bases theorem. Acta Arithmetica, 143(4):299-332, 2010.]
For any prime power $q$ and any integer $m \geq 2$, there exists an element $\alpha \in \mathbb{F}_{q^m}$ such that both $\alpha$ and $\alpha^{-1}$ are primitive normal over $\mathbb{F}_q$ except when $(q, m)$ is one of the pairs $(2, 3), (2, 4), (3, 4), (4, 3), (5, 4)$.

# Review of literature

## Result 8

[Wang, P.P. On existence of some specific elements in finite fields of characteristic 2. Finite fields and their applications, 18(4):800-813, 2012.] There is an element $\alpha$ in $\mathbb{F}_{q^n}$ such that both $\alpha$ and $\alpha + \alpha^{-1}$ are primitive elements of $\mathbb{F}_{q^n}$ if $q = 2^k$, and $n$ is an odd number no less than 13 and $k > 4$.

## Result 9

[Liao, Q., Li, J. and Pu, K. On the existence for some special primitive elements in finite fields, Chinese Annals of Mathematics, series B, 37B:259-266, 2016] There exist a sufficient condition which generalised the above result, i.e., for any odd prime power $q$.

## Result 10

[ Wang, P.P., Cao, X.W. and Feng, R.Q. On the existence of some specific elements in finite fields of characteristic 2. Finite Fields and their Applications, 18(4):800-813, 2012, Theorem 3.1]
There is an element $\alpha$ in $\mathbb{F}_{q^n}$ such that both $\alpha$ and $\alpha + \alpha^{-1}$ are primitive elements of $\mathbb{F}_{q^n}$ if $q = 2^k$, and $n$ is an odd number no less than 13 and $k > 4$.

## Result 11

[ Wang, P.P., Cao, X.W. and Feng, R.Q. On the existence of some specific elements in finite fields of characteristic 2. Finite Fields and their Applications, 18(4):800-813, 2012, Theorem 4.1]
For field of even characteristic and any odd $n$, there is an element $\alpha$ in $\mathbb{F}_{q^n}$ such that $\alpha$ is a primitive normal element and $\alpha + \alpha^{-1}$ is a primitive element of $\mathbb{F}_{q^n}$ if either $n | (q-1)$, and $n \geq 33$, or $n \nmid (q-1)$ and $n \geq 30$, $k \geq 6$ (where $q = 2^k$).

## previous results

### Result 12

[ Cohen, S.D. Pairs of primitive elements in fields of even order. Finite Fields and their Applications, 28:22-42, 2014, Theorem 1.1]
Let $q \geq 8$ be a power of 2. Then $\mathbb{F}_q$ contains an element $\alpha$ such that $\alpha$ and $\alpha + \alpha^{-1}$ both are primitive in $\mathbb{F}_q$.

### Result 13

[ Cohen, S.D. Pairs of primitive elements in fields of even order. Finite Fields and their Applications, 28:22-42, 2014, Theorem 1.2]
Let $q$ be a power of 2 and $n(\geq 3)$ be a positive integer. Then $\mathbb{F}_{q^n}$ contains a normal element $\alpha$ such that both $\alpha$ and $\alpha + \alpha^{-1}$ are primitive in $\mathbb{F}_{q^n}$.

# Previous results

## Result 14

[ Kapetanakis, G. An extension of the (strong) primitive normal basis theorem. Applicable Algebra in Engineering Communication and Computing, 25:311-337, 2014, Theorem 6.1 ]
Let $q$ and $n$ be such that $n' \leq 4$. If $q \geq 23$ and $m \geq 17$, then there exist a primitive normal element $\alpha$ in $\mathbb{F}_{q^n}$ such that $\dfrac{a\alpha + b}{c\alpha + d}$ is also primitive normal element of $\mathbb{F}_{q^n}$, where $a, b, c, d \in \mathbb{F}_{q^n}$.

## Result 15

[ Kapetanakis, G. An extension of the (strong) primitive normal basis theorem. Applicable Algebra in Engineering Communication and Computing, 25:311-337, 2014, Theorem 6.2 ]
Let $q$ and $n$ be such that $n' = q - 1$. Then there exist a primitive normal element $\alpha$ in $\mathbb{F}_{q^n}$ such that $\dfrac{a\alpha + b}{c\alpha + d}$ is also primitive normal element of $\mathbb{F}_{q^n}$, where $a, b, c, d \in \mathbb{F}_{q^n}$.

# Previous results

## Result 16

[ Kapetankis, G. Normal bases and primitive elements over finite fields. Finite Fields and their Applications, 26:123-143, 2014, Theorem 1.4 ]

Let q be a prime power, $n \geq 2$ an integer and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $a, b, c, d \in \mathbb{F}_q$ and $A \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ if $q = 2$ and $n$ is odd. There exists some primitive $\alpha$ in $\mathbb{F}_{q^n}$, such that both $\alpha$ and $(a\alpha + b)/(c\alpha + d)$ produce a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, unless one of the following holds:

- $q = 2,\ n = 3$ and $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.
- $q = 3,\ n = 4$ and $A$ is anti diagonal.
- $(q, n)$ is (2, 4), (4,3), (5,4) and $d = 0$.

# Previous results

## Result 17

[ Booker, A. R., Cohen, S. D., Sutherland, N. and Trudgian, T. Primitive values of quadratic polynomialsin a finite field. Mathematics of computation, 88(318):1903-1912, 2019, Theorem 1]
For all $q > 211$, there always exists a primitive root $\alpha$ in the finite field $\mathbb{F}_q$ such that $Q(\alpha)$ is also a primitive root, where $Q(x) = ax^2 + bx + c$ is a quadratic polynomial with $a, b, c \in \mathbb{F}_q$ such that $b^2 - 4ac \neq 0$.

# Definition

## Character

Let $G$ be a finite abelian group and $S := \{z \in \mathbb{C} : |z| = 1\}$ be the multiplicative group of all complex numbers with modulus 1 . Then a character $\chi$ of $G$ is a homomorphism from $G$ into the group $S$, i.e $\chi(a_1 a_2) = \chi(a_1)\chi(a_2)$ for all $a_1, a_2 \in G$.

# Definition

## Characters

In a finite field $\mathbb{F}_{q^n}$, there are two types of characters of a finite field $\mathbb{F}_{q^n}$, namely *additive character* for $\mathbb{F}_{q^n}$ and *multiplicative character* for $\mathbb{F}_{q^n}^*$.
For any divisor $d$ of $q^n - 1$, there are exactly $\phi(d)$ characters of order $d$ in $\widehat{\mathbb{F}_{q^n}^*}$.

## The Canonical Additive Character

The function $\chi_1$ defined by $\chi_1(\alpha) = \exp^{2\pi i Tr(\alpha)/p}$ for all $\alpha \in \mathbb{F}_{q^n}$ is a special character of the additive group $\mathbb{F}_{q^n}$ and called the canonical additive character.

For $b$ in $\mathbb{F}_{q^n}$, the character $\chi_b(\alpha) = \chi_1(b\alpha)$, for all $\alpha \in \mathbb{F}_{q^n}$.

# definition

## e-free element

Since $\mathbb{F}_{q^n}^*$ can be seen as $\mathbb{Z}$-module, then for any divisor $e$ of $q^n - 1$, an element $\alpha \in \mathbb{F}_{q^n}^*$ is called $e - free$, if for any $d|e, \alpha = \beta^d$ where $\beta \in \mathbb{F}_{q^n}$ implies $d = 1$ i.e, if $\gcd(d, \frac{q^n-1}{ord_{q^n}(\alpha)}) = 1$.

## g-free element

The additive group $\mathbb{F}_{q^n}$ can be seen as $\mathbb{F}_q[x]$-module under the rule

$$F \circ \alpha = \sum_{i=0}^{n} a_i \alpha^{q^i}; \text{ for } \alpha \in \mathbb{F}_{q^n} \text{ where } F(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{F}_q[x].$$

For $\alpha \in \mathbb{F}_{q^n}$, the $\mathbb{F}_q$-order of $\alpha$ is the monic $\mathbb{F}_q$-divisor $g$ of $x^n - 1$ of minimal degree such that $go\alpha = 0$.

Let $g$ be a divisor of $x^n - 1$. If, $\alpha = ho\beta$ where $\beta \in \mathbb{F}_{q^n}$, $h$ is a divisor of $g$ imply $h = 1$, then $\alpha$ is called $g$-free in $\mathbb{F}_{q^n}$

# Vinogradov's formula

## Characteristic function for e-free element

Cohen and Huczynska in *The primitive normal basis theorem without a computer,* [J. Lond. Math. Soc. **67**(1) (2003) 41-56]
For any $e|q^n - 1$, defined the character function for the subset of $e$-free elements of $\mathbb{F}_{q^n}^*$ by

$$\rho_e : \alpha \mapsto \theta(e) \sum_{d|e} \left( \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\alpha) \right)$$

where $\theta(e) := \frac{\phi(e)}{e}$.

## Characteristic function for g-free element

The character function for the set of $g$-free elements in $\mathbb{F}_{q^n}$, for any $g|x^n - 1$ is given by

$$\kappa_g : \alpha \mapsto \Theta(g) \sum_{f|g} \left( \frac{\mu'(f)}{\Phi(f)} \sum_{\psi_f} \psi_f(\alpha) \right)$$

where $\Theta(g) := \frac{\Phi_q(g)}{q^{deg(g)}}$

## Lenstra-Schoof

Let $N_{q^n}(m_1, m_2, g_1, g_2)$ be the number of $\alpha \in \mathbb{F}_{q^n}$, such that $\alpha$ is $m_1$-free, $F(\alpha)$ is $m_2$-free, $\alpha$ is $g_1$-free and $F(\alpha)$ is $g_2$-free, where $m_1, m_2$ are positive integers and $g_1, g_2$ are any polynomials over $\mathbb{F}_q$. We use the notations $\chi_1$ and $\psi_1$ to denote the trivial multiplicative and additive characters respectively.
Then $N_{q^n}$ is obtained as follows

$$N_{q^n}(m_1, m_2, g_1, g_2) = \sum_{\alpha \in \mathbb{F}_{q^n}^*} \rho_{m_1}(\alpha)\rho_{m_2}(F(\alpha))\kappa_{g_1}(\alpha)\kappa_{g_2}(F(\alpha))$$

# Extension of Characters (L-S method)

$$N_{q^n}(q^n - 1, q^n - 1, x^n - 1, x^n - 1)$$
$$= \sum_{\alpha \in \mathbb{F}_{q^n}^*} \rho_{q^n-1}(\alpha)\rho_{q^n-1}(F(\alpha))\kappa_{x^n-1}(\alpha)\kappa_{x^n-1}(F(\alpha))$$
$$= \theta(q^n - 1)^2 \Theta(x^n - 1)^2 \sum_{\alpha \in \mathbb{F}_{q^n}^*} \sum_{d,h|q^n-1} \sum_{g,f|x^n-1} \frac{\mu(d)\mu(h)\mu'(g)\mu'(f)}{\phi(d)\phi(h)\Phi(g)\Phi(f)}$$
$$\sum_{\chi_d,\chi_h} \sum_{\psi_g,\psi_f} \chi_d(\alpha)\chi_h(F(\alpha))\psi_g(\alpha)\psi_f(F(\alpha))$$
$$= \theta(q^n - 1)^2 \Theta(x^n - 1)^2 (\sum_{i=1}^{16} S_i)$$

## one sum to explain them all

If $S_{16}$ is taken over $d \neq 1, h \neq 1, g \neq 1, f \neq 1$, then

$$|S_{16}| \leq \sum_{\substack{1 \neq d,h | q^n-1 \\ d,h \text{ square free}}} \sum_{\substack{1 \neq g,f | x^n-1 \\ g,f \text{ square free}}} \frac{1}{\phi(d)\phi(h)\Phi(g)\Phi(f)} \sum_{\chi_d,\chi_h} \sum_{\psi_g,\psi_f} \left| \sum_{\alpha \in \mathbb{F}_{q^n}} \chi_d(\alpha)\chi_h(F(\alpha))\psi_g(\alpha)\psi_f(F(\alpha)) \right|$$

$$\leq \sum_{\substack{1 \neq d,h | q^n-1 \\ d,h \text{ square free}}} \sum_{\substack{1 \neq g,f | x^n-1 \\ g,f \text{ squarefree}}} \frac{1}{\phi(d)\phi(h)\Phi(g)\Phi(f)} \sum_{\chi_d,\chi_h} \sum_{\psi_g,\psi_f} \left| \sum_{\alpha \in \mathbb{F}_{q^n}} \chi_d(\alpha)\chi_h(F(\alpha))\psi_g(\alpha)\psi_f(F(\alpha)) \right|$$

# Handy bound

( L.Fu and D.Q.Wan, A class of incomplte character sums, *Q.J.Math.Soc*, **43**, (1968) 21-39., Theorem 5.6) Let $f_1(x), f_2(x), \ldots, f_k(x) \in \mathbb{F}_{q^n}[x]$ be distinct irreducible polynomials and $g(x)$ be rational function over $\mathbb{F}_{q^n}$. Let $\chi_1, \chi_2. \ldots, \chi_k$ be multiplicative characters and $\psi$ be a nontrivial additive character of $\mathbb{F}_{q^n}$. Suppose that $g(x)$ is not of the form $r(x)^q - r(x)$ in $\mathbb{F}_{q^n}[x]$. Then

$$\left| \sum_{\substack{\alpha \in \mathbb{F}_{q^n} \\ f_i(\alpha) \neq 0, g(\alpha) \neq \infty}} \chi_1(f_1(\alpha))\chi_2(f_2(\alpha)) \ldots \chi_k(f_k(\alpha))\psi(g(\alpha)) \right| \leq (n_1 + n_2 + n_3 + n_4 - 1)q^{n/2} ,$$

where $n_1 = \sum_{j=1}^{k} deg(f_j)$, $n_2 = \max(\deg(g), 0)$, $n_3$ is the degree of denominator of $g(x)$ and $n_4$ is sum of degrees of those irreducible polynomials dividing the denominator of $g$, but distinct from $f_j(x)$, $j = 1, 2, \ldots, k$.

# Back to the theorem

Our aim is to find pair $(q, n)$ such that $N_{q^n}(q^n - 1, q^n - 1, x^n - 1, x^n - 1) > 0$
From above we have a sufficient condition for
$N_{q^n}(q^n - 1, q^n - 1, x^n - 1, x^n - 1) > 0$ is

$$\begin{aligned} q^n - 1 > &(q^{n/2} + 1)(2^\omega - 1) + (C_1 q^{n/2}(2^\omega - 1)^2) + (2^\Omega - 1) \\ &+ (q^{n/2}(2^\omega - 1)(2^\Omega - 1)) + (C_2 q^{n/2} + 1)(2^\omega - 1) \\ &+ (C_3 q^{n/2}(2^\omega - 1)^2(2^\Omega - 1)) + (C_4 q^{n/2} + 1)(2^\Omega - 1) \\ &+ (C_5 q^{n/2}(2^\omega - 1)(2^\Omega - 1)) + (C_6 q^{n/2} + 1)(2^\omega - 1)(2^\Omega - 1) \\ &+ (C_7 q^{n/2}(2^\omega - 1)^2(2^\Omega - 1)) + (2^\Omega - 1)^2 \\ &+ (C_8 q^{n/2}(2^\omega - 1)(2^\Omega - 1)^2) + (C_9 q^{n/2} + 1)(2^\omega - 1)(2^\Omega - 1)^2 \\ &+ (C_{10} q^{n/2}(2^\omega - 1)^2(2^\Omega - 1)^2) \end{aligned}$$

Which holds if $q^{n/2} > C.2^{2\omega + 2\Omega}$. [4.1]
Which is our desired result.

# Final output

## For $f(x) = x^2 + x + 1$

[Anju Gupta and R.K. Sharma, On primitive normal elements over finite fields, Asian-European Journal of Mathematics, Vol. 11, No. 2 (2018)]

- Let $q = p^k$, where $k$ is a positive integer and $p > 3$ is a prime and $n$ be a positive integer with $n|q-1$. If $n \geq 39$, then $(q, n) \in N$.
- Let $q = p^k$, where k is a positive integer and $p > 3$ is a prime and $n$ be a positive integer with $n \nmid q-1$. If $p \geq 5, k \geq 3$ and $n \geq 48$, then $(q, n) \in N$.

# Sieve Technique

In "Sieve" method, some new notations are used

- Define $Q := Q(q, n)$ to be the square free part of $\frac{(q^n-1)}{(q-1)\, gcd(n, q^n-1)}$
- For any integer $m$, we denote $m_0$ as the radical of $m$. Then for $w \in \mathbb{F}_{q^n}$ we have $w$ is $m$-free if and only if $w$ is $m_0$-free.
  Same is for $x^n - 1$ i.e $g \in \mathbb{F}_{q^n}$ is $x^n - 1$-free if and only if it is $x^{n_0} - 1$-free.

## Use of Radicals

**Introducing the seive**. Let $e$ be a divisor of $q-1$. If Rad($e$)= Rad($q-1$) then we consider $s=0$ and $\delta=1$. Otherwise if Rad($e$)<Rad($q-1$), then let $p_1, p_1, \ldots, p_s$, $s \geq 1$, be the primes dividing $q-1$ but not $e$ and set $\delta = 1 - \sum_{i=1}^{s} 2p_i^{-1}$. It is essential to choose $e$ such that $\delta$ is positive.

### Sieveing inequality

Now we have the following results, in which all conditions we imposed on $a, b, c$ are satisfied.

- $N(q-1, q-1) \geq \sum_{i=1}^{s} N(p_i e, e) + \sum_{i=1}^{s} N(e, p_i e) - (2s-1)N(e,e)$ and from this, we have
- $N(q-1, q-1) \geq$ $\sum_{i=1}^{s} \{[N(p_i e, e) - \theta(p_i)N(e,e)] - [N(e, p_i e) - \theta(p_i)N(e,e)]\} + \delta N(e,e). (1)$

# Output

**For $f(x) = ax^2 + bx + c$**

We have the sufficient condition as
$q > \left\{ \left( \frac{2s-1}{\delta} + 2 \right) \left( 2W \left( W - \frac{3}{2} \right) + \frac{3W}{2\sqrt{q}} \right) + 1 + \frac{3W}{2\sqrt{q}} \right\}^2$

This inequality is completely dependent on $e$ and easier for calculation.

# Precision

Following are the conclusions from the inequality which are given in "Primitive values of quadratic polynomials in a finite field", by A.R.Booker and S.D.Cohen [Math. Comp.v88, Number 318, Oct 2018, (1903-1912) ]

- For $q > 211$, there exist primitive element $\alpha$ over $\mathbb{F}_q$ such that $a\alpha^2 + b\alpha + c$ is also primitive over $\mathbb{F}_q$, where $b^2 - 4ac \neq 0$.
- For the fields of characteristic less than 211, there are 1453 exceptions .

Hence, in this method the results are more precise.

# References


- Cortellini, E. Finite fields and cryptology. *Computer Scientific Journal of Moldova*, 11(2):150-167, 2003.
- Kapetanakis, G. An extension of the (strong) primitive normal basis theorem. *Applicable Algebra in Engineering Communication and Computing*, 25:311-337, 2014.
- Cohen, S.D. Consecutive primitive roots in a finite field. *Proceedings of the American Mathematical Society*, 93(2):189-197, 1985.
- Cohen, S.D. and Huczynska, S. The primitive normal basis theorem without a computer. *Journal of the London Mathematical Society. Second Series*, 67(1):41-56, 2003.
- Cohen, S.D. and Huczynska, S. The strong primitive normal basis theorem. *Acta Arithmetica*, 143(4):299-332, 2010.

# References


- Cohen, S.D. Pairs of primitive elements in fields of even order. *Finite Fields and their Applications*, 28:22-42, 2014.
- Castro, F.N. and Moreno, C.J. Mixed exponential sums over finite fields. *Proceedings of the American Mathematical Society* , 128(9):2529-2537, 2000.
- Kapetankis, G. Normal bases and primitive elements over finite fields. *Finite Fields and their Applications*, 26:123-143, 2014.
- Garefalakis, T. and Kapetanakis, G. On the existence of primitive completely normal bases of finite fields. *Journal of Pure and Applied Algebra*, 223(3):909-921, (2018)

# References

- Lenstra, H.W., and Schoof, R.J. Primitive Normal Bases for Finite Fields. *Mathematics of Computation*, 48:217-231, 1987.
- Carlitz, L. Primitive roots in a finite fields. *Transactions of the American Mathematical Society*, 73(3):314-318, 1952.
- Lidl R. and Niederreiter H., *Finite Fields*. Cambridge University Press, Cambridge, 2nd edition, 1997.
- Anju and Sharma, R.K. On primitive normal elements over finite fields. *Asian-European Journal of Mathematics* , 11(2), 2018
- James G. and Liebeck M., *Representations and Characters of Groups*, 2nd edn. (Cambridge University Press, Cambridge, 2001)

# THANK YOU