ON SOME CLASSES OF IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

by

HALİME ÖMRÜUZUN

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University
August 2016

ON SOME CLASSES OF IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

APPROVED BY

Prof. Dr. Alev Topuzoğlu ....
(Thesis Supervisor)

Assoc. Prof. Dr. Cem Güneri ....

Assist. Prof. Dr. Seher Tutdere ....

DATE OF APPROVAL: 4/8/2016

ON SOME CLASSES OF IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

Halime Ömrüuzun

Mathematics, Master Thesis, August 2016

Thesis Supervisor: Prof. Dr. Alev Topuzoğlu

Keywords: irreducible polynomials, divisibility, self-reciprocal polynomials, prescribed coefficients.

Abstract

In this thesis we describe the work in literature on various aspects of the theory of polynomials over finite fields. We focus on properties like irreducibility and divisibility. We also consider existence and enumeration problems for irreducible polynomials of special types. After the introductory Chapter 1, we collect the well-known results on irreducibility of binomials and trinomials in Chapter 2, where we also present the number of irreducible factors of a fixed degree k of $x^t - a$, due to L. Redei. Chapter 3 is on self-reciprocal polynomials. An infinite family of irreducible, self-reciprocal polynomials over $\mathbb{F}_2$ is presented in Section 3.2. This family was obtained by J. L. Yucas and G. L. Mullen. Divisibility of self-reciprocal polynomials over $\mathbb{F}_2$ and $\mathbb{F}_3$ is studied in Sections 3.3 and 3.4 following the work of R. Kim and W. Koepf. The last chapter aims to give a survey of recent results concerning existence and enumeration of irreducible polynomials with prescribed coefficients.

SONLU CİSİMLER ÜZERİNDEKİ İNDİRGENEMEZ POLİNOMLARIN BAZI ALT SINIFLARI ÜZERİNE

Halime Ömrüuzun

Matematik, Yüksek Lisans Tezi, Ağustos 2016

Tez Danışmanı: Prof. Dr. Alev Topuzoğlu

Anahtar Kelimeler: indirgenemez polinomlar, bölünebilirlik, öz-karşılıklı polinomlar, saptanmış katsayılar.

Özet

Bu tezde sonlu cisimler üzerindeki polinomlar teorisinden bazı konulara dair literatürde bulunan çalışmaları derleyerek detaylı biçimde açıkladık. Polinomların indirgenemezlik ve bölünebilirlik gibi özellikleri üzerine yoğunlaştık. Özel tip indirgenemez polinomların varlık ve sayma problemlerini de ele aldık. Başlangıç bölümünden sonra, iki terimli ve üç terimli polinomların indirgenemezliği hakkında iyi bilinen sonuçları topladık. 2. Bölüm'de ayrıca $x^t - a$ polinomunun sabit bir k dereceli indirgenemez çarpanlarının sayısını L. Redei'nin çalışmalarına dayanarak sunduk. Bölüm 3 öz-karşılıklı polinomlar üzerinedir. Bölüm 3.2'de, $\mathbb{F}_2$ üzerinde indirgenemez, öz-karşılıklı polinomların sonsuz bir ailesini sunduk. Bu aile J. L. Yucas and G. L. Mullen tarafından elde edilmiştir. 3.3 ve 3.4'üncü bölümlerde, $\mathbb{F}_2$ ve $\mathbb{F}_3$ üzerindeki öz-karşılıklı polinomların bölünebilirliğini R. Kim ve W. Koepf'in çalışmaları ışığında ele aldık. En son bölüm saptanmış katsayılı indirgenemez polinomların varlığı ve sayıları üzerindeki yeni sonuçlar hakkında genel bir bakış açısı vermeyi amaçlamaktadır.

To my family

Acknowledgments

First, I would like to thank my advisor Prof. Dr. Alev Topuzoğlu for her motivation, guidance, enthusiasm, encouragement and immense knowledge. Her contributions to my personality have been enormous. I would like to thank Prof. Dr. Henning Stichtenoth for his contribution to my study. I admire his care and patience.

I would also like to thank the members of my thesis committee, Assoc. Prof. Dr. Cem Güneri and Assist. Prof. Dr. Seher Tutdere, for reviewing my master thesis.

My sincere thanks also go to Prof. Dr. Ali Nesin. He always encouraged me throughout my academic career with continuous support. To meet him is a turning point in my life.

I am grateful to my family. They always helped me with enormous tolerance. They were always patient to me during my study. I am deeply grateful for their endless love and patience.

I also would like to thank all my friends, especially Ayşegül Yavuz and Talha Barış. They never left me alone with their lovely friendship.

Last but not least, I would like to thank all members of Sabancı University. I am very lucky for being a member of such a lovely place.

Table of Contents

CHAPTER 1

Introduction

1.1. Basic Concepts and Definitions

We first recall some basic concepts and fix the notation:

> Throughout the thesis, $\mathbb{F}_q$ denotes the finite field with q elements, where $q = p^r$, $r \geq 0$ and p is a prime number.
>
> $\mathbb{F}_q^*$ denotes the multiplicative group of $\mathbb{F}_q$.
>
> By $Tr_{F/K}$ we denote the trace map from $F = \mathbb{F}_{q^n}$ to $K = \mathbb{F}_q$ which is defined as follows:
>
> Let $\alpha \in F = \mathbb{F}_{q^n}$. Then $Tr_{F/K}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{n-1}}$.
>
> Let $f(x) \in \mathbb{F}_q[x]$, $f(x) \neq 0$. The polynomial $f^*(x)$ denotes the reciprocal of $f(x)$ and it is defined by $f^*(x) = x^n f(\frac{1}{x})$ where n is the degree of $f(x)$. A polynomial $f(x)$ is called *self-reciprocal* if $f^*(x) = f(x)$.
>
> For $f(x) \in \mathbb{F}_q[x]$, the order of the polynomial $f(x)$ is the smallest positive integer e such that $f(x) \mid (x^e - 1)$ in $\mathbb{F}_q[x]$. We denote the order of $f(x)$ by $ord(f)$.
>
> As usual ϕ denotes the Euler's phi function. We recall that $\phi(n)$= $\#\{k$: $1 \leq k \leq n$, $gcd(k, n) = 1\}$.

If a polynomial $f(x)$ over $\mathbb{F}_q$ has exactly two non-zero coefficients, then it is called a *binomial*. Similarly, a polynomial $f(x)$ over $\mathbb{F}_q$ with exactly three non-zero coefficients is called a *trinomial*.

We use the Möbius inversion formula, so we recall the Möbius function and the formula for the additive case.

The Möbius function μ is defined for a positive integer n as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is divisible by the square of some prime number,} \\ (-1)^k & \text{if } n = p_1 \dots p_k \text{ and } p_i\text{'s are distinct primes.} \end{cases}$$

Möbius Inversion Formula (additive case): Let f and F be two functions from $\mathbb{N}$ into an additively written abelian group G. Then

$$F(n) = \sum_{d|n} f(d) \quad \text{for all } n \in \mathbb{N}$$

if and only if

$$f(n) = \sum_{d|n} \mu(n/d)F(d) = \sum_{d|n} \mu(d)F(n/d) \text{ for all } n \in \mathbb{N}.$$

1.2. Overview

This thesis is organized as follows:

In Chapter 2, we consider binomials and trinomials over finite fields. In Section 2.1, we start with a well-known criteria on the irreducibility of binomials over $\mathbb{F}_q$. We also present an infinite family of irreducible binomials over $\mathbb{F}_q$ and this result can be found as Corollary 3.2 in [22]. Section 2.2 is concerned with trinomials over $\mathbb{F}_q$. We consider irreducibility of special type of trinomials $x^p - x - a$ over $\mathbb{F}_q$, where p is the characteristic of $\mathbb{F}_q$ and this standard result can be found, for instance, in [22] as Theorem 3.5 and it dates back to the 19-th century. We also present some results about divisibility of trinomials of the form $x^{as} + x^{bt} + 1$ over $\mathbb{F}_2$ in Section 2.2, due to R. Kim and W. Koepf [18]. In Section 2.3, we give enumeration results concerning binomials and trinomials over $\mathbb{F}_q$. The first result yields the number of the irreducible factors of a fixed degree k of a binomial $x^t - a$ over $\mathbb{F}_q$, due to L. Redei [25]. After presenting this result, an example obtaining the irreducible factors of degree 1, 2, 3 and 4 of the binomial $x^5 - 2$ over $\mathbb{F}_3$ is given. The second main result of this section is on the number of irreducible trinomials $x^n + ax^k + b$ over $\mathbb{F}_3$ following the work of O. Ahmadi [1].

In Chapter 3, we consider self-reciprocal polynomials over finite fields. In Section 3.1, we study orders of self-reciprocal irreducible polynomials. In the same section, we present a theorem which gives a classification of self-reciprocal irreducible polynomials over $\mathbb{F}_q$ in relation to their orders. Then by using this classification theorem, we give the number of self-reciprocal irreducible polynomials of degree n over $\mathbb{F}_q$. In Section 3.2, by using the results in Section 3.1, a condition for the existence of an infinite family of self-reciprocal irreducible polynomials over $\mathbb{F}_2$ is determined. The results in both

Section 3.1 and Section 3.2 are from the paper of J. L. Yucas and G. L. Mullen [31]. Results in Section 3.3 are based on the paper [18] of R. Kim and W. Koepf, where divisibility of self-reciprocal trinomials by irreducible polynomials over $\mathbb{F}_2$ is studied. We also give a factorization of self-reciprocal trinomials over $\mathbb{F}_2$ in terms of cyclotomic polynomials. For an irreducible polynomial $f(x)$ of order e over $\mathbb{F}_2$, the number of trinomials of degree less than e, which are divided by $f(x)$ is studied in the same section. In Section 3.4, by using the ideas in Section 3.3, we present some results about divisibility of self-reciprocal trinomials by irreducible polynomials over $\mathbb{F}_3$.

In Chapter 4, we study irreducible polynomials with prescribed coefficients. In Section 4.1, we focus on questions on existence of irreducible polynomials with prescribed coefficients. We state the well-known Hansen-Mullen conjecture. Then we give a brief survey of works concerning existence problems. In Section 4.2, we focus on questions on enumeration of irreducible polynomials with prescribed coefficients. One of the problems is determining the number of monic irreducible polynomials of degree n and with prescribed trace over $\mathbb{F}_q$. This number was first obtained by Carlitz [2], then Yucas [30] proved Carlitz' result by using elementary techniques. In Section 4.2, we present the proof due to Yucas. The question of estimating the number of irreducible polynomials or their subclasses with several prescribed coefficients has been extensively studied and there are still many open problems in this area.

CHAPTER 2

On The Irreducibility of Binomials and Trinomials over Finite Fields

2.1. Binomials over Finite Fields

A binomial of the form $ax^n + bx^k$ in $\mathbb{F}_q[x]$ is divisible by x^{n-k} and it is reducible. Therefore, we can restrict ourselves to binomials of the form $f(x) = ax^t + b$. Moreover, we can assume that $f(x)$ is monic and hence consider $f(x) = x^t - a$ with $a \neq 0$. The following theorem, which is Theorem 3.75 in [21] gives a criteria for irreducibility of binomials.

Theorem 2.1.1 *Suppose that $a \in \mathbb{F}_q^*$ is an element of order e, and $t \geq 2$. Then the binomial $x^t - a$ is irreducible over $\mathbb{F}_q$ if and only if the following conditions are satisfied:*

(i) *For any prime divisor r of t, we have $r \mid e$ and $r \nmid (q-1)/e$,*

(ii) *If $t \equiv 0 \pmod 4$, then $q \equiv 1 \pmod 4$.*

Before giving the proof of Theorem 2.1.1, we need the following theorem from [22].

Theorem 2.1.2 *Let $t \in \mathbb{Z}^+$ and $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n and order e. Then $f(x^t)$ is irreducible over $\mathbb{F}_q$ if and only if the following conditions are satisfied:*

(i) *$gcd\left(t, \frac{q^n-1}{e}\right) = 1$,*

(ii) *For any prime divisor r of t, we have $r \mid e$,*

(iii) *If $t \equiv 0 \pmod 4$, then $q^n \equiv 1 \pmod 4$.*

Proof of Theorem 2.1.1: Suppose that the conditions (i) and (ii) are satisfied. Consider the polynomial $f(x) = x - a$. This is an irreducible polynomial of degree 1 and order e over $\mathbb{F}_q$. By condition (i), any prime divisor of t divides e but not $(q-1)/e$. Note that $n = 1$ in our case. So conditions (i) and (ii) of Theorem 2.1.2 are satisfied. By assumption, if $t \equiv 0 \pmod 4$, then $q \equiv 1 \pmod 4$. So the third condition in

Theorem 2.1.2 is also satisfied. Hence, the polynomial $f(x^t) = x^t - a$ is irreducible over $\mathbb{F}_q$.

Now suppose the condition (i) is not satisfied. Then there exists a prime divisor r of t that either divides $(q-1)/e$ or does not divide e. For the first case, we have $rs = (q-1)/e$ for some integer s. Consider the subgroup of $\mathbb{F}_q^*$ consisting of r-th powers. This subgroup has order $(q-1)/r = es$. So it contains the subgroup of order e of $\mathbb{F}_q^*$ generated by a. In particular, for some $b \in \mathbb{F}_q^*$, $a = b^r$ and so $x^t - a = x^{t_1 r} - b^r$ has the factor $x^{t_1} - b$. Therefore, the polynomial $x^t - a$ is not irreducible. For the second case, r does not divide $(q-1)/e$ and also does not divide e. It follows that r does not divide $q-1$. Since r is a prime number, this means that $gcd(r, q-1) = 1$. Then $r_1 r \equiv 1 \pmod{q-1}$ for some integer r_1, and then $x^t - a = x^{t_1 r} - a^{r_1 r}$. So the polynomial $x^t - a$ has the factor $x^{t_1} - a^{r_1}$. It follows that $x^t - a$ is not irreducible over $\mathbb{F}_q$. Now assume (i) is satisfied, but (ii) is not satisfied. We show that the binomial $x^t - a$ can not be irreducible over $\mathbb{F}_q$. By assumption $t = 4t_2$ for some integer t_2 and $q \not\equiv 1 \pmod 4$. By part (i), 2 divides e. So $e \equiv 0 \pmod 4$ or $e \equiv 2 \pmod 4$. Since e is the order of element a in $\mathbb{F}_q^*$, we have $e \mid (q-1)$. But $q \not\equiv 1 \pmod 4$. Therefore, we get $e \equiv 2 \pmod 4$. Note that $a^{e/2} = -1$ since e is the order of a in $\mathbb{F}_q^*$. So we have $x^t - a = x^t + a^{(e/2)+1} = x^t + a^d$, where $d = (e/2) + 1$ is even. Note that e is even and divides $q-1$ and then q is odd. Moreover, $q \equiv 3 \pmod 4$. Then $a^d = 4(2^{-1}a^{d/2})^2 = 4(2^{-1}a^{d/2})^{q+1} = 4c^4$, where $c = (2^{-1}a^{d/2})^{(q+1)/4}$. We get the following factorization: $x^t - a = x^{4t_2} + 4c^4 = (x^{2t_2} + 2cx^{t_2} + 2c^2)(x^{2t_2} - 2cx^{t_2} + 2c^2)$. Hence, the binomial $x^t - a$ is not irreducible. This completes the proof. □

The following result is Corollary 3.4.6 in [23] which follows from Theorem 2.1.1. We give a proof for the sake of completeness.

Corollary 2.1.3 *Let $a \in \mathbb{F}_q$ and t be an odd number. Then the binomial $x^t - a$ is irreducible over $\mathbb{F}_q$ if and only if $a \neq b^r$ for any $b \in \mathbb{F}_q$ and for any prime divisor r of t.*

Proof: Suppose that a is an r-th power in $\mathbb{F}_q$ for some prime divisor r of t. Then there exists an element $b \in \mathbb{F}_q$ such that $a = b^r$. So we have $x^t - a = x^{t_1 r} - b^r$ and $x^t - a$ has the factor $x^{t_1} - b$. For the converse, we use Theorem 2.1.1. Since t is an odd number, we don't need to check the second condition. Let e be the order of a in $\mathbb{F}_q^*$. To show that (i) is satisfied, let r be a prime divisor of t. If $r \mid (q-1)/e$, as in the proof of Theorem 2.1.1, a is an r-th power. If r does not divide both $(q-1)/e$ and e, then r does not divide $q-1$ and so there exists an integer r_1 such that $r_1 r \equiv 1 \pmod{q-1}$. It follows that $a = a^{r_1 r} = (a^{r_1})^r$ and a is again an r-th power. □

Example 2.1.1 *Consider the finite field $\mathbb{F}_3$ and the polynomial $x^9 - 2$ over $\mathbb{F}_3$. We have $2 \equiv 2^3 \pmod 3$. So the element 2 is a 3-rd power of an element in $\mathbb{F}_3$ for the prime divisor 3 of 9. By Corollary 2.1.3, the polynomial $x^9 - 2$ is not irreducible over $\mathbb{F}_3$. Indeed, we have the factorization $x^9 - 2 = x^9 - 2^3 = (x^3 - 2)(x^6 + 2x^3 + 1)$.*

The following result is Corollary 3.2 from [22].

Corollary 2.1.4 *Let e be the order of $a \in \mathbb{F}_q^*$ and r be a prime factor of $q-1$, where $r \nmid (q-1)/e$. Suppose that $q \equiv 1 \pmod 4$ if $r = 2$ and $k \geq 2$. Then $x^{r^k} - a$ is irreducible over $\mathbb{F}_q$ for any $k \geq 0$.*

Proof: We show the conditions in Theorem 2.1.1 are satisfied. The only prime factor of r^k is r and by assumption $r \mid (q-1)$ and it does not divide $(q-1)/e$. It follows that $r \mid e$. Therefore, the condition (i) is satisfied. We need to show that $q \equiv 1 \pmod 4$ if $r^k \equiv 0 \pmod 4$. But it follows from the assumption. So the condition (ii) is also satisfied. This completes the proof. □

Example 2.1.2 *Consider the polynomial $x^{5^k} - 2$ over $\mathbb{F}_{11}$. The element 2 has order 10 in $\mathbb{F}_{11}^*$. Note that 5 is a prime divisor of $q-1 = 11-1 = 10$ and it does not divide $(q-1)/e = (11-1)/10 = 1$. We don't need the condition $q \equiv 1 \pmod 4$ since r is not equal to 2. So by Corollary 2.1.4, $x^{5^k} - 2$ is irreducible over $\mathbb{F}_{11}$ for any non-negative integer k.*

2.2. Trinomials over Finite Fields

The following theorem is on the irreducibility of the trinomials $x^p - x - a$ in $\mathbb{F}_q[x]$, where p is the characteristic of $\mathbb{F}_q$. It is well-known and can be found, for instance, in [22] as Theorem 3.5.

Theorem 2.2.5 *Let $\mathbb{F}_q$ be a finite field with characteristic p and $a \in \mathbb{F}_q$. Then $x^p - x - a$ is irreducible over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_q/\mathbb{F}_p}(a) \neq 0$.*

Proof: Let $q = p^m$ and γ be a root of $x^p - x - a$. Then we have

$$\begin{aligned}
\gamma^p &= \gamma + a \\
\gamma^{p^2} &= (\gamma + a)^p = \gamma^p + a^p = \gamma + a + a^p \\
&\vdots \\
\gamma^{p^m} &= (\gamma + a + a^p + \ldots + a^{p^{m-2}})^p \\
&= \gamma^p + a^p + a^{p^2} + \ldots + a^{p^{m-1}} \\
&= \gamma + a + a^p + a^{p^2} + \ldots + a^{p^{m-1}} = \gamma + Tr_{\mathbb{F}_q/\mathbb{F}_p}(a).
\end{aligned}$$

It follows that $\gamma^q = \gamma + Tr_{\mathbb{F}_q/\mathbb{F}_p}(a)$ and so $Tr_{\mathbb{F}_q/\mathbb{F}_p}(a) = 0$ if and only if $\gamma^q = \gamma$; that is every root of $x^p - x - a$ is in $\mathbb{F}_q$. This implies that $x^p - x - a$ splits into linear factors over $\mathbb{F}_q$ if and only if $Tr_{\mathbb{F}_q/\mathbb{F}_p}(a) = 0$.

Now suppose that $\theta = Tr_{\mathbb{F}_q/\mathbb{F}_p}(a) \neq 0$. Then $\theta \in \mathbb{F}_p$, and as above we get

$$\gamma^{q^i} = \gamma + i\theta, \ i = 1, 2, \ldots$$

where γ is a root of $x^p - x - a$. Therefore, γ has p distinct conjugates over $\mathbb{F}_q$ and the minimal polynomial of γ over $\mathbb{F}_q$ has degree p. So the minimal polynomial of γ is $x^p - x - a$. Hence, $x^p - x - a$ is an irreducible polynomial over $\mathbb{F}_q$. □

Remark 2.2.1 *Note that the polynomial $f(x)$ is irreducible over $\mathbb{F}_q$ if and only if $f(bx)$ is irreducible over $\mathbb{F}_q$, where $b \in \mathbb{F}_q^*$. Therefore, Theorem 2.2.5 yields a criteria for $b^p x^p - bx - a$.*

Now we present some results about divisibility of trinomials of the form $x^{as} + x^{bt} + 1$ over $\mathbb{F}_2$. The following theorem can be found in [18] as Theorem 5.

Theorem 2.2.6 *Suppose that $f(x)$ is an irreducible polynomial over $\mathbb{F}_2$ with $ord(f) > 1$ and $a, b, s, t \in \mathbb{Z}^+$, where $as > bt$. If $f(x) \mid (x^{as} + x^{bt} + 1)$, then e does not divide as, bt and $as - bt$.*

Proof: Let α be a root of $f(x)$ in some extension of $\mathbb{F}_2$. Suppose that $ord(f) = e \mid as$. Then we have $\alpha^{as} = 1$. Thus $f(x) \mid (x^{as} + 1)$. Since $e > 1$ and $f(0) \neq 0$, we have that $f(x) \nmid x^{bt}$. Therefore $f(x)$ can not divide the trinomial $x^{as} + x^{bt} + 1$. The case where $e \mid bt$ is very similar. Now assume that $e \mid (as - bt)$. Then for any root α of $f(x)$, we have $\alpha^{as-bt} = 1$. Thus $f(x) \mid (x^{as-bt} + 1)$. But then $x^{as} + x^{bt} + 1 = x^{bt}(x^{as-bt} + 1) + 1$ is not divisible by $f(x)$; otherwise $f(x) \mid 1$. □

If $a = b = 1$ and $f(x) = x^2 + x + 1$, then the converse of Theorem 2.2.6 is also true.

Corollary 2.2.7 *The polynomial $x^2 + x + 1$ divides the trinomial $x^n + x^k + 1$ of degree n if and only if 3 does not divide n, k and $n - k$.*

Proof: Note that the order of $x^2 + x + 1$ is 3. So by Theorem 2.2.6, if $x^2 + x + 1$ divides the trinomial $x^n + x^k + 1$, then 3 does not divide n, k and $n - k$. Conversely, assume that n, k and $n - k$ are not divisible by 3. Then we have two cases:

$$n \equiv 2 \pmod 3,\ k \equiv 1 \pmod 3,\ n - k \equiv 1 \pmod 3$$

or

$$n \equiv 1 \pmod 3,\ k \equiv 2 \pmod 3,\ n - k \equiv 2 \pmod 3.$$

We give a proof for the first case and the second case is very similar. Suppose that $n \equiv 2 \pmod 3$, $k \equiv 1 \pmod 3$, $n - k \equiv 1 \pmod 3$ and let α be a root of $x^2 + x + 1$. By assumption $n = 3n_1 + 2$ and $k = 3k_1 + 1$ for some integers n_1 and k_1. Then we have

$$\alpha^n + \alpha^k + 1 = \alpha^{3n_1+2} + \alpha^{3k_1+1} + 1 = \alpha^2 + \alpha + 1 = 0.$$

Since α was arbitrary, it follows that $x^2 + x + 1$ divides the trinomial $x^n + x^k + 1$. □

2.3. Enumeration Results

2.3.1. Binomials

An interesting problem which has been only recently considered is estimating the number of irreducible binomials over $\mathbb{F}_q$. The recent work [16] of R. Heyman and I. E. Shparlinski focuses on this problem. They considered the number $N(t, q)$ of irreducible binomials $x^t - a \in \mathbb{F}_q[x]$. This is the first study of the behaviour of $N(t, q)$. Now, we focus on a problem of different nature and give the number of irreducible factors of a fixed degree k of a binomial $x^t - a$ over $\mathbb{F}_q$. This result is due to Schwarz [27]. We follow the shorter proof by L. Redei given in [25].

Lemma 2.3.8 *Let $m, n \geq 1$ be integers and $a, b \in \mathbb{F}_q^*$. Then $gcd(x^m - a, x^n - b)$ in an arbitrary field has degree 0 or $d = gcd(m, n)$. Moreover, $gcd(x^m - a, x^n - b)$ has degree $d = gcd(m, n)$ if and only if $a^{n/d} = b^{m/d}$.*

Proof: When $m = n$, the statement is obviously true. Hence, the statement holds if $m + n = 2$, i.e., when $m = 1$ and $n = 1$. Now suppose $m \neq n$ and $m, n \geq 1$. We proceed by induction on the degree of the sum of the binomials. Assume that the statement is true for all couples of binomials with a sum of degrees $< m + n$. We show that the statement holds when the sum has degree $m + n$. Without loss of generality, we can assume that $m > n$. From the equality

$$(x^m - a) - x^{m-n}(x^n - b) = b\left(x^{m-n} - \frac{a}{b}\right)$$

we get

$$gcd(x^m - a, x^n - b) = gcd\left(x^{m-n} - \frac{a}{b}, x^n - b\right)$$

The sum of the polynomials $x^{m-n} - \frac{a}{b}$ and $x^n - b$ has degree $m - n + n = m < m + n$. So by the induction assumption the statement is true for these polynomials and note that $gcd(m - n, n) = gcd(m, n) = d$. It follows that $gcd(x^m - a, x^n - b)$ has degree 0 or d. Moreover, the polynomial $gcd\left(x^{m-n} - \frac{a}{b}, x^n - b\right)$ has degree d if and only if

$$\left(\frac{a}{b}\right)^{n/d} = b^{(m-n)/d}.$$

Hence, the polynomial $gcd(x^m - a, x^n - b)$ has degree d if and only if $a^{n/d} = b^{m/d}$. □

Theorem 2.3.9 *Let $S_k(t, q)$ be the set of all irreducible factors of degree k of $x^t - a$ in $\mathbb{F}_q[x]$. Put $\#S_k(t, q) = \sigma_k(t, q)$ and assume that the characteristic p of $\mathbb{F}_q$ does not divide t. Then*

$$\sigma_k(t, q) = \frac{1}{k} \sum_{l|k} \mu\left(\frac{k}{l}\right) d_l$$

where $d_l = gcd(t, q^l - 1)$ and the sum is taken over all l satisfying $a^{d'_l} = 1$ with $d'_l = \frac{q^l - 1}{d_l}$.

Proof: For convenience we put $\sigma_k(t,q) = \sigma_k$. Note that $gcd(x^t - a, x^{q^k-1} - 1) = \prod_{\substack{h\in S_d(t,q)\\ d|k}} h(x)$, since for an irreducible polynomial $f(x)$ of degree m over $\mathbb{F}_q$ we have that $f(x) \mid (x^{q^n} - x)$ if and only if $m \mid n$. The polynomial $x^t - a$ has no multiple factors since $p \nmid t$ and so

$$\sum_{l|k} l\sigma_l = deg(gcd(x^t - a, x^{q^k-1} - 1))$$

where deg denotes the degree of polynomial. Then, $deg(gcd(x^t - a, x^{q^k-1} - 1)) = 0$ or $deg(gcd(x^t - a, x^{q^k-1} - 1)) = gcd(t, q^k - 1) = d_k$ by Lemma 2.3.8. The second case occurs if and only if the equality $a^{d'_k} = 1$ holds, where $d'_k = \frac{q^k-1}{d_k}$. Now let

$$\chi_k = \begin{cases} 1 & \text{if } a^{d'_k} = 1, \text{ where } d'_k = \frac{q^k-1}{d_k}, \\ 0 & \text{otherwise.} \end{cases}$$

So we have

$$deg(gcd(x^t - a, x^{q^k-1} - 1)) = \sum_{l|k} l\sigma_l = d_k\chi_k.$$

Using the Möbius inversion formula, we get

$$k\sigma_k = \sum_{l|k} \mu\left(\frac{k}{l}\right) d_l\chi_l.$$

So,

$$\sigma_k = \frac{1}{k}\sum_{l|k} \mu\left(\frac{k}{l}\right) d_l\chi_l.$$

This is equivalent to what we wanted to prove. □

Example 2.3.3 *Let $q = 3$. Note that the characteristic of the field is 3. Consider the binomial $x^5 - 2 \in \mathbb{F}_3[x]$. With the notation of Theorem 2.3.9, we have $t = 5$, $a = 2$ and $3 \nmid 5$. By Corollary 2.1.3, the binomial $x^5 - 2$ is irreducible over $\mathbb{F}_3$ if and only if 2 is not an r-th power of an element in $\mathbb{F}_3$ for any prime divisor r of 5. In this case r can only be 5. So to check the irreducibility of the binomial $x^5 - 2$ over $\mathbb{F}_3$, it suffices to check whether 2 is a 5-th power of an element in $\mathbb{F}_3$ or not. We have $2^5 \equiv 2 \pmod 3$. It follows that 2 is a 5-th power in the field $\mathbb{F}_3$. Hence, $x^5 - 2$ is reducible over $\mathbb{F}_3$. Indeed, we have the factorization $x^5 - 2 = (x-2)(x^4 + 2x^3 + x^2 + 2x + 1)$. The polynomial $x^4 + 2x^3 + x^2 + 2x + 1$ has no root in $\mathbb{F}_3$. Moreover, one can easily show that $x^4 + 2x^3 + x^2 + 2x + 1$ can not be written as a product of two polynomials which have both degree 2. It follows that $x^4 + 2x^3 + x^2 + 2x + 1$ is irreducible over $\mathbb{F}_3$. Now let us find the number of irreducible factors of $x^5 - 2$ of degree 1 and degree 4 just by using the formula stated in Theorem 2.3.9. The number of irreducible factors of degree 1 of the polynomial $x^5 - 2$ is given by*

$$\frac{1}{1}\sum_{l|1} \mu\left(\frac{1}{l}\right) d_l.$$

We have $d_1 = (5, 3^1 - 1) = 1$ *and* $d_1' = 2$. *Note that* $2^{d_1'} = 2^2 = 1$. *Hence, we get*

$$\frac{1}{1}\sum_{l|1}\mu\left(\frac{1}{l}\right)d_l = \mu(1)d_1 = 1.$$

Now we will find the number of irreducible factors of degree 4 *of the polynomial* $x^5 - 2$ *in* $\mathbb{F}_3[x]$. *This number is given by*

$$\frac{1}{4}\sum_{l|4}\mu\left(\frac{4}{l}\right)d_l.$$

By an easy computation, we see that $d_2 = 1$, $d_4 = 5$, $d_2' = 8$ *and* $d_4' = 16$. *Then we get* $2^{d_2'} = 1$ *and* $2^{d_4'} = 1$. *Finally,*

$$\frac{1}{4}\sum_{l|4}\mu\left(\frac{4}{l}\right)d_l = \frac{1}{4}(\mu(4)d_1 + \mu(2)d_2 + \mu(1)d_4) = \frac{1}{4}(0 - 1 + 5) = 1.$$

In the same way one can find the number of irreducible factors of degree 2 *or* 3 *of* $x^5 - 2$ *and see that those numbers are equal to* 0.

2.3.2. Trinomials

Now we give some results about the distribution of irreducible trinomials over $\mathbb{F}_3$. We start by the Corollary 2 in [1] which follows from Theorem 2.1.2.

Corollary 2.3.10 *Let* $f(x) \in \mathbb{F}_q[x]$ *be a polynomial of degree* n, *where* n *is odd and* $q \equiv 3 \pmod 4$. *Then* $f(x^{2^r})$ *is reducible over* $\mathbb{F}_q$ *for any* $r \geq 2$.

Proof: We can assume that $f(x)$ is an irreducible polynomial; otherwise we take an irreducible factor of $f(x)$ with odd degree. We show that the condition (iii) in Theorem 2.1.2 is not satisfied. Since $t = 2^r$ and $r \geq 2$, $4 \mid t$. But $4 \nmid (q^n - 1)$. Because, $q^n - 1 \equiv 3^n - 1 \equiv 3 - 1 = 2 \pmod 4$ since n is an odd number. Therefore, the polynomial $f(x^{2^r})$ is reducible over $\mathbb{F}_q$. □

Lemma 2.3.11 *Suppose that* $f(x)$ *is an irreducible polynomial over* $\mathbb{F}_q$ *of degree* n *and let* $\theta \in \mathbb{F}_{q^n}^*$ *be such that* $f(\theta x) \in \mathbb{F}_q[x]$. *Let* β *be a root of* $f(x)$ *in a certain extension of* $\mathbb{F}_q$. *Then* $f(\theta x)$ *is irreducible over* $\mathbb{F}_q$ *if and only if* $\theta^{-1}\beta$ *is not in any proper subfield of* $\mathbb{F}_{q^n}$.

Proof: Suppose that $f(\theta x)$ is irreducible over $\mathbb{F}_q$. Observe that $f(\theta x)$ has degree n and $\theta^{-1}\beta$ is a root of $f(\theta x)$, since β is a root of the polynomial $f(x)$. It follows that $\theta^{-1}\beta$ is not in any proper subfield of $\mathbb{F}_{q^n}$.

Conversely, suppose that $f(\theta x)$ is reducible. Let $g(x)$ be a monic irreducible factor of $f(\theta x)$ of degree $m < n$ and suppose that this irreducible factor has root $\theta^{-1}\beta$. So

$g(x)$ is the minimal polynomial of $\theta^{-1}\beta$ over $\mathbb{F}_q$. We have the chain of finite fields $\mathbb{F}_{q^n} \supseteq \mathbb{F}_q(\theta^{-1}\beta) \supseteq \mathbb{F}_q$. It follows that $[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\theta^{-1}\beta)][\mathbb{F}_q(\theta^{-1}\beta) : \mathbb{F}_q]$. But $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ and $[F_q(\theta^{-1}\beta) : \mathbb{F}_q] = m$. So we get $m \mid n$. Then $\mathbb{F}_{q^m}$ is a proper subfield of $\mathbb{F}_{q^n}$ and it contains $\theta^{-1}\beta$. □

Now we state two lemmas, Lemma 4 and 5 in [1], which will be used to prove the results that follow.

Lemma 2.3.12 *Assume that q is odd, $n = 2^r n'$, where n' is odd and $r \geq 1$. Then 2^{r+2} divides $q^n - 1$ and 2^r divides $\frac{q^n-1}{q-1}$.*

Lemma 2.3.13 *Assume that q is odd and $n = 2^r n'$, where n' is odd. Let $r \geq s \geq 0$. Then for any $\alpha \in \mathbb{F}_q^*$ there exists $\theta \in \mathbb{F}_{q^n}$ such that $\theta^{2^s} = \alpha$.*

The following theorem is Theorem 6 in [1].

Theorem 2.3.14 *Let $n = 2^r n'$ and $k = 2^s k'$, where n' and k' are odd, $r > s \geq 0$. Let q be odd and $\alpha \in \mathbb{F}_q^*$. Then $x^n + ax^k + b \in \mathbb{F}_q[x]$ is irreducible over $\mathbb{F}_q$ if and only if*

$$\alpha^{2^{r-s}n'} x^n + a\alpha^{k'} x^k + b \in \mathbb{F}_q[x]$$

is irreducible over $\mathbb{F}_q$.

Proof: Assume that $f(x) = x^n + ax^k + b \in \mathbb{F}_q[x]$ is irreducible over $\mathbb{F}_q$. By Lemma 2.3.13, there exists $\theta \in \mathbb{F}_{q^n}^*$ such that $\theta^{2^s} = \alpha$. We show that $g(x) = f(\theta x) = \alpha^{2^{r-s}n'} x^n + a\alpha^{k'} x^k + b \in \mathbb{F}_q[x]$ is irreducible over $\mathbb{F}_q$. By Lemma 2.3.11, it suffices to show that $\theta^{-1}\beta$ is not in any proper subfield of $\mathbb{F}_{q^n}$, where β is a root of $f(x)$ in $\mathbb{F}_{q^n}$.

To the contrary, suppose that $(\theta^{-1}\beta)^{q^l-1} = 1$, where l is a proper divisor of n, and let $l = 2^v l'$, where $v \leq r$ and $l' \mid n'$. By Lemma 2.3.12, we have $2^v \mid \frac{q^l-1}{q-1}$. If $v \geq s$, then $2^s \mid \frac{q^l-1}{q-1}$ and we get

$$\beta^{q^l-1} = \theta^{q^l-1} = \theta^{2^s(q-1)t} = 1$$

for some t, and this yields a contradiction since β can not be in any proper subfield of $\mathbb{F}_{q^n}$. Suppose $v < s$ and let $w = s - v$. We have $q^l - 1 \mid q^{2^w l} - 1$. Since $\beta^{q^l-1} = \theta^{q^l-1}$, we have $\beta^{q^{2^w l}-1} = \theta^{q^{2^w l}-1} = \theta^{q^{2^s l'}-1} = \theta^{2^s(q-1)t'} = 1$ for some t', and then $n \mid 2^w l$. But we have $r > s$. This is a contradiction. Observe that $f(x) = g(\theta^{-1}x)$ and $\theta^{-2^s} = \alpha^{-1} \in \mathbb{F}_q^*$. So the proof of the converse is similar and the result follows. □

Corollary 2.3.15 *Suppose that n, k, r, s are as in Theorem 2.3.14. Then $x^n + ax^k + b$ is irreducible over $\mathbb{F}_q$ if and only if $x^n - ax^k + b$ is irreducible over $\mathbb{F}_q$.*

Proof: Take $\alpha = -1$ in Theorem 2.3.14. □

Corollary 2.3.16 *The trinomial $x^n - x^k + 1$ of degree n is reducible over $\mathbb{F}_3$, where $n \equiv 0 \pmod 4$.*

Proof: Suppose that $n = 2^r n'$ and $k = 2^s k'$, where n' and k' are odd numbers and $s \geq r$. Consider the polynomial $g(x) = x^{n'} - x^{2^{s-r}k'} + 1$. Then $g(x)$ is a polynomial of odd degree and by Corollary 2.3.10, $g(x^{2^r}) = x^n - x^k + 1$ is reducible over $\mathbb{F}_3$. Also note that the assumption $q \equiv 3 \pmod 4$ in Corollary 2.3.10 holds. If $r > s$, consider the polynomial $x^n + x^k + 1$. This is a reducible polynomial over $\mathbb{F}_3$, since it has 1 as a root. By Corollary 2.3.15, $f(x) = x^n - x^k + 1$ is also reducible over $\mathbb{F}_3$. □

The following is Theorem 11 in [1].

Theorem 2.3.17 *Let $x^n + ax^k + b \in \mathbb{F}_3[x]$ be irreducible over $\mathbb{F}_3$, where $n \equiv 0 \pmod 4$. Let $n = 2^r n'$ and $k = 2^s k'$, where n' and k' are odd numbers. Then we have $r > s$.*

Proof: Let $x^n + ax^k + b \in \mathbb{F}_3[x]$, where $n = 2^r n'$ and $k = 2^s k'$, n' and k' are odd numbers, and $s \geq r \geq 2$. Then if we let $f(x) = x^{n'} + ax^{2^{s-r}k'} + b$, we have $x^n + ax^k + b = f(x^{2^r})$ and from Corollary 2.3.10, it follows that $x^n + ax^k + b$ is reducible over $\mathbb{F}_3$. □

The following theorem is about the number of irreducible trinomials over $\mathbb{F}_3$ and is given in [1] as Theorem 12.

Theorem 2.3.18 *Let $m \in \mathbb{Z}^+$ be fixed, $a, b \in \mathbb{F}_3$, $l \in \{0, 4, 8\}$ and $0 \leq c \leq 5$. Let S_1 be the set of all irreducible trinomials $x^n + ax^k + b \in \mathbb{F}_3[x]$, where $n \equiv l \pmod{12}$, $k \equiv c \pmod 6$, and $n \leq m$ and S_2 be the set of all irreducible trinomials $x^n + ax^k + b \in \mathbb{F}_3[x]$, where $n \equiv l \pmod{12}$, $k \equiv l - c \pmod 6$ and $n \leq m$. Then $\#S_1 = \#S_2$.*

Proof: When $a, b = 1$ we have the trinomial $x^n + x^k + 1$ over $\mathbb{F}_3$. But this trinomial is always reducible over $\mathbb{F}_3$ since it has 1 as a root. Thus suppose that $a = 1$, $b = -1$. The other cases are very similar. Let $x^n + x^k - 1$ be an irreducible trinomial over $\mathbb{F}_3$, where $n \equiv l \pmod{12}$, $k \equiv c \pmod 6$ for given $l \in \{0, 4, 8\}$ and $0 \leq c \leq 5$. Then by Theorem 2.3.17, the largest power of 2 which divides n is greater than the largest power of 2 which divides k. Thus by Corollary 2.3.15, $x^n - x^k - 1$ is irreducible over $\mathbb{F}_3$. Now the reciprocal $-x^n - x^{n-k} + 1$ of $x^n - x^k - 1$ is also irreducible over $\mathbb{F}_3$. Then $x^n + x^{n-k} - 1$ is irreducible over $\mathbb{F}_3$. But in this case we have $n \equiv l \pmod{12}$ and $n - k \equiv c \pmod 6$. Since $n \equiv l \pmod{12}$, we have $n \equiv l \pmod 6$. Then $k \equiv n - c \equiv l - c \pmod 6$. This gives a bijection between S_1 and S_2, hence the result follows. □

CHAPTER 3

On Some Classes of Self-reciprocal Polynomials over Finite Fields

We recall that for a polynomial $f(x)$ of degree n over $\mathbb{F}_q$, the reciprocal of $f(x)$ is the polynomial $f^*(x)$ of degree n over $\mathbb{F}_q$ given by $f^*(x) = x^n f(\frac{1}{x})$, and a polynomial $f(x)$ is called *self-reciprocal* if $f^*(x) = f(x)$. We note that $f(x)$ is irreducible over $\mathbb{F}_q$ if and only if the reciprocal polynomial $f^*(x)$ is irreducible over $\mathbb{F}_q$. Moreover, if $f(x) \in \mathbb{F}_q[x]$ is monic, irreducible and self-reciprocal of degree $n \geq 2$, then n has to be even, since the set of all roots of $f(x)$ is closed under taking inverses.

Self-reciprocal polynomials have many applications in coding theory, they are also used in combinatorics. We start with the orders of self-reciprocal irreducible polynomials over finite fields. Results in Section 3.1 and Section 3.2 are based on the paper of J. L. Yucas and G. L. Mullen [31].

3.1. Orders of Self-reciprocal Irreducible Polynomials

We denote the set of all monic polynomials of degree n in $\mathbb{F}_q[x]$ by $\mathcal{M}_n(q)$ and denote the set of all irreducible polynomials in $\mathcal{M}_n(q)$ by $\mathcal{I}_n(q)$. Throughout this section, we assume that $n = 2m$. We begin by presenting some elementary number-theoretic results.

Proposition 3.1.1 *Let $a \in \mathbb{Z}^+$, where $a > 2$ and suppose that $a \mid (q^t + 1)$ for some $t \in \mathbb{Z}^+$. Let s be such that $a \mid (q^s + 1)$, but $a \nmid (q^k + 1)$ if $k < s$. Then we have:*

(i) *a divides $q^u + 1$ if and only if $u = u's$, where u' is an odd integer.*

(ii) *a divides $q^u - 1$ if and only if $u = u's$, where u' is an even integer.*

Proof: Since s is the smallest positive integer such that $a \mid (q^s + 1)$, i.e., $q^s \equiv -1 \pmod{a}$, the multiplicative order of q mod a is $2s$.

To prove (i), assume that a divides q^u+1. Then we have $q^u \equiv -1 \pmod{a}$. Clearly, u can not be an even multiple of s. Otherwise, we get $q^u \equiv 1 \pmod{a}$, so $1 \equiv -1 \pmod{a}$. But this is impossible since $a > 2$. To prove the converse, suppose that

$u = (2j+1)s$ for some non-negative integer j. Then we have $q^u+1 = q^{(2j+1)s}+1 \equiv q^s+1 \pmod{a}$. Since $a \mid (q^s+1)$, the result follows.

To prove (ii), assume $a \mid (q^u-1)$. Then $q^u \equiv 1 \pmod{a}$. Since the order of q mod a is $2s$, it follows that $(2s) \mid u$. Hence, $u = u's$, where u' is an even integer. Conversely, assume that $u = u's$, where u' is an even integer. Then $(2s) \mid u$, so $q^u \equiv 1 \pmod{a}$ and $a \mid (q^u-1)$. □

Proposition 3.1.2 *Let $a \in \mathbb{Z}^+$. Suppose that there exist $r, k \in \mathbb{Z}^+$, where r is even, such that $a \mid (q^r-1)$ and $a \mid (q^k+1)$. Then $a \mid (q^{r/2^l}+1)$ for some $l \in \mathbb{Z}^+$.*

Proof: When $a = 1$ or $a = 2$, the result is obviously true. We can assume $a > 2$. Let s be the smallest positive integer such that $a \mid (q^s+1)$. Such an s exists since $a \mid (q^k+1)$ for some $k \in \mathbb{Z}^+$ by assumption. By Proposition 3.1.1, r is an even multiple of s. Write $r = 2^l ts$ for some $l, t \in \mathbb{Z}^+$, where t is odd. By Proposition 3.1.1, $a \mid (q^{ts}+1)$ since ts is an odd multiple of s. Also note that $ts = r/2^l$. This completes the proof. □

Proposition 3.1.3 *Let $f(x) \in \mathcal{I}_n(q)$ be a self-reciprocal polynomial. Then $ord(f) \mid (q^k+1)$ for some positive integer k dividing m.*

Proof: Let $\alpha \in \mathbb{F}_{q^n}$ be a root of $f(x)$. Then $f(1/\alpha) = 0$ since $f(x)$ is self-reciprocal. Note that $1/\alpha$ is a conjugate of α, so we can write $1/\alpha = \alpha^{q^t}$ for some $t \in \mathbb{Z}^+$. Then $\alpha^{q^t+1} = 1$ and thus $ord(\alpha) \mid (q^t+1)$. Since $\alpha \in \mathbb{F}_{q^n}$, $ord(\alpha) \mid (q^n-1)$. By Proposition 3.1.2, $ord(\alpha) \mid (q^{n/2^l}+1)$ for some $l \in \mathbb{Z}^+$. We have $(n/2^l)2^{l-1} = m$ and $(n/2^l) \mid m$. So just take $k = n/2^l$. □

Now, we introduce the set $D_m = \{r \in \mathbb{Z}^+ : r \mid q^m+1, \text{ but } r \nmid q^k+1 \text{ for } 0 \le k < m\}$. We recall that $n = 2m$. Observe that $1, 2 \notin D_m$ for any m. Also, if $f(x)$ is an irreducible polynomial of degree $n \ge 2$, then $ord(f) \ne 1, 2$.

Proposition 3.1.4 *Let $f(x) \in \mathcal{I}_n(q)$ be a self-reciprocal polynomial and let $\alpha \in \mathbb{F}_{q^n}$ be a root of $f(x)$. Then α is a primitive d-th root of unity for some $d \in D_m$.*

Proof: Firstly, we prove that if $k \mid m$ and $ord(\alpha) \mid (q^k+1)$, then $k = m$. Note that $ord(\alpha)$ divides $q^{2k}-1 = (q^k-1)(q^k+1)$. Then we get $\alpha^{q^{2k}-1} = 1$ and thus $\alpha \in \mathbb{F}_{q^{2k}}$. Now suppose that $f(x) = \prod_{i=0}^{n-1}(x-\alpha^{q^i}) = g(x)h(x)$, where $g(x) = \prod_{i=0}^{2k-1}(x-\alpha^{q^i})$ and $h(x) = \prod_{i=2k}^{n-1}(x-\alpha^{q^i})$.

For $1 \le j \le n-1$, consider the map $T_j : \mathbb{F}_{q^{2k}} \to \mathbb{F}_q$ defined by

$$T_j(\alpha) = \sum_{0 \le i_1 < i_2 < \ldots < i_j < 2k-1} \alpha^{q^{i_1}} \alpha^{q^{i_2}} \ldots \alpha^{q^{i_j}}.$$

The coefficients of $g(x)$ are determined by $T_j(\alpha)$ and so $g(x) \in \mathbb{F}_q[x]$. Also we have $f(x) \in \mathbb{F}_q[x]$. It follows that $h(x) \in \mathbb{F}_q[x]$. This shows that if $k < m$, $f(x)$ has a non-trivial factorization, i.e., $f(x)$ is reducible over $\mathbb{F}_q$.

Now we prove the proposition. By Proposition 3.1.3, $ord(\alpha) \mid (q^k+1)$ for some $k \in \mathbb{Z}^+$, where $k \mid m$. By the fact above $ord(\alpha) \mid (q^m+1)$. We show that $ord(\alpha) \in D_m$. Let s be the smallest positive integer such that $ord(\alpha) \mid (q^s+1)$. By Proposition 3.1.1, m is an odd multiple of s and then $s \mid m$. Therefore, we have $s = m$ and $ord(\alpha) \in D_m$. □

Corollary 3.1.5 *Let $f(x) \in \mathcal{I}_n(q)$ be a self-reciprocal polynomial. Then $ord(f) \in D_m$.*

Proposition 3.1.6 *Suppose that $d \in D_m$ and β is a primitive d-th root of unity. Then β^{q^i} is a primitive d-th root of unity for each $i \in \{0, 1, \ldots, n-1\}$. Moreover, if $i \neq j$, then $\beta^{q^i} \neq \beta^{q^j}$.*

Proof: Let $0 \leq i \leq n-1$. Since $d \in D_m$, $d \mid (q^m+1)$, $(d, q^i) = 1$ and so β^{q^i} is a primitive d-th root of unity. If $\beta^{q^i} = \beta^{q^j}$ for some $0 \leq i < j \leq n-1$, then $\beta^{q^j - q^i} = 1$ and so d divides $q^j - q^i = q^i(q^{j-i}-1)$. Since d and q^i are relatively prime, $d \mid (q^{j-i}-1)$. By Proposition 3.1.1, $j - i = km$ for some even positive integer k. But then $j = km + i \geq 2m + i \geq 2m = n$. A contradiction to $0 < j \leq n-1$. □

Proposition 3.1.7 *Let $d \in D_m$ and β be a primitive d-th root of unity. Consider the polynomial $f_\beta(x)$ defined by $f_\beta(x) = \prod_{i=0}^{n-1}(x - \beta^{q^i})$. Then $f_\beta(x)$ is a self-reciprocal element of $\mathcal{I}_n(q)$ with $ord(f_\beta) = d$.*

Proof: We have $d \in D_m$. Then $d \mid (q^m+1)$, so we have $\beta^{q^m+1} = 1$. Hence, $\beta^{q^i}\beta^{q^{m+i}} = 1$ for $0 \leq i \leq n-1$ and $\prod_{i=0}^{n-1} \beta^{q^i} = 1$. By using these facts we get:

$$\begin{aligned}
x^n f_\beta\left(\frac{1}{x}\right) &= x^n \prod_{i=0}^{n-1}\left(\frac{1}{x} - \beta^{q^i}\right) = \prod_{i=0}^{n-1}(1 - x\beta^{q^i}) \\
&= \left(\prod_{i=0}^{n-1}\beta^{q^i}\right)\left(\prod_{i=0}^{n-1}\left(\frac{1}{\beta^{q^i}} - x\right)\right) \\
&= \prod_{i=0}^{n-1}(\beta^{q^{m+i}} - x) = \prod_{i=0}^{n-1}(x - \beta^{q^{m+i}}) \\
&= \prod_{i=0}^{n-1}(x - \beta^{q^i}) = f_\beta(x).
\end{aligned}$$

Therefore, $x^n f_\beta\left(\frac{1}{x}\right) = f_\beta(x)$ and $f_\beta(x)$ is a self-reciprocal polynomial. Now we show that $f_\beta(x)$ is an irreducible polynomial over $\mathbb{F}_q$. Let $g(x)$ be an irreducible factor of $f_\beta(x)$ of degree r, where $1 \leq r \leq n$. Let γ be a root of $g(x)$. Since $g(x)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree r, we have $\gamma \in \mathbb{F}_{q^r}$. It follows that $\gamma^{q^r-1} = 1$. Since γ is a root of $g(x)$ and $g(x)$ is a factor of $f_\beta(x)$, γ is also a root of the polynomial $f_\beta(x)$. Hence, γ is a primitive d-th root of unity. Consequently, $d \mid (q^r - 1)$. But $d \in D_m$, so by Proposition 3.1.1, r is an even multiple of m and $r \geq 2m$. On the other hand, $r \leq n = 2m$ and we get $r = 2m = n$. Therefore, the polynomial $f_\beta(x)$ itself is an irreducible polynomial over $\mathbb{F}_q$. Note that $f_\beta(x)$ has order d, since its roots are primitive d-th roots of unity. □

The following theorem gives a classification of the self-reciprocal irreducible polynomials in relation to D_m.

Theorem 3.1.8 *Let $f(x) \in \mathcal{I}_n(q)$. Then the following statements are equivalent:*

(i) *$f(x)$ is self-reciprocal.*

(ii) *$ord(f) \in D_m$.*

(iii) *$f(x) = f_\beta(x)$ for some primitive d-th root of unity β, where $d \in D_m$.*

Proof: By Corollary 3.1.5, (i) implies (ii). Part (iii) implies (i) follows from Proposition 3.1.7. Now we prove that (ii) implies (iii). Suppose that $ord(f) \in D_m$. Let α be a root of $f(x)$. It follows that $ord(\alpha) \in D_m$. By Proposition 3.1.6, $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are all distinct primitive d-th roots of unity, where $d = ord(\alpha)$. Since $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are all roots of $f(x)$, we get $f(x) = f_\alpha(x)$. □

We recall that $n = 2m$ for the following theorem.

Theorem 3.1.9 **(i)** *There are $\phi(d)/n$ self-reciprocal polynomials in $\mathcal{I}_n(q)$ of order d for each $d \in D_m$.*

(ii) *The number of self-reciprocal polynomials in $\mathcal{I}_n(q)$ is*

$\frac{1}{n} \sum_{d \in D_m} \phi(d)$.

Proof: There are $\phi(d)$ primitive d-th roots of unity. It follows that there are $\phi(d)/n$ distinct polynomials $f_\beta(x)$ and by Theorem 3.1.8, any self-reciprocal irreducible polynomial of degree n and order d, where $d \in D_m$ corresponds to some $f_\beta(x)$. This proves part (i). Part (ii) follows from counting the distinct $f_\beta(x)$ for each $d \in D_m$. □

3.2. An Infinite Family of Self-reciprocal Irreducible Polynomials over $\mathbb{F}_2$

We recall that $\mathcal{I}_n(q)$ is the set of all monic irreducible polynomials of degree n in $\mathbb{F}_q[x]$. The following theorem shows the existence of an infinite family of self-reciprocal polynomials in $\mathcal{I}_n(2)$ under some conditions.

Theorem 3.2.10 *Let $m \geq 3$ be an odd integer, $n = 2m$ and $f(x) \in \mathcal{I}_n(2)$, where $ord(f) = 2^m + 1$. Define $f_j(x) = f(x^{3^j})$ for integers $j \geq 0$. Then $\{f_j(x)\}_j$ is an infinite family of self-reciprocal polynomials in $\mathcal{I}_n(2)$.*

Proof: Since $ord(f) = 2^m + 1$, we have $ord(f) \in D_m$. So by Theorem 3.1.8, $f(x)$ is self-reciprocal. Note that $f_j(x)$ is a polynomial of degree $n3^j$. Then we have

$$\begin{aligned} f(x) &= x^n f\left(\frac{1}{x}\right) = f^*(x), \text{ and so} \\ f(x^{3^j}) &= (x^{3^j})^n f\left(\frac{1}{x^{3^j}}\right), \text{ which implies that} \\ f_j(x) &= x^{n3^j} f_j\left(\frac{1}{x}\right) = f_j^*(x). \end{aligned}$$

Therefore, $f_j(x)$ is self-reciprocal for each j. Now we show that $f_j(x)$ is an irreducible polynomial over $\mathbb{F}_2$ for each j. We use Theorem 2.1.2. We just take $t = 3^j$. Since m is an odd integer, $2^m \equiv 2 \pmod 3$ and then 3 divides $2^m + 1$ and 3 does not divide $(2^n - 1)/(2^m + 1) = 2^m - 1$. By Theorem 2.1.2, $f_j(x)$ is an irreducible polynomial over $\mathbb{F}_2$. □

Now we present some results about divisibility of self-reciprocal trinomials by irreducible polynomials over $\mathbb{F}_2$ and $\mathbb{F}_3$. The results in Section 3.3 are based on the paper of R. Kim and W. Koepf [18]. In Section 3.4, we study divisibility of self-reciprocal trinomials by irreducible polynomials over $\mathbb{F}_3$ by using the results in Section 3.3.

3.3. Factorization of Self-reciprocal Trinomials by Irreducible Polynomials over $\mathbb{F}_2$

It can be easily checked that a self-reciprocal trinomial over $\mathbb{F}_2$ must be of the form $x^{2m} + x^m + 1$, where $m \in \mathbb{Z}^+$. We begin with a lemma which is used in the proof of the theorem, which gives a characterization of irreducible factors of self-reciprocal trinomials over $\mathbb{F}_2$. This characterization is in terms of the orders of irreducible factors.

Lemma 3.3.11 *Let $f(x)$ be an irreducible polynomial with $ord(f) = e$ and assume that $f(x)$ divides the self-reciprocal trinomial $x^{2m} + x^m + 1$. Then there exists a unique self-reciprocal trinomial of degree $< e$ and is divisible by $f(x)$.*

Proof: Let α be a root of $f(x)$ in some extension of $\mathbb{F}_2$. Since $f(x)$ divides the trinomial $x^{2m}+x^m+1$, α is also a root of this trinomial. Hence, we have $\alpha^{2m}+\alpha^m+1 = 0$. Let $m = eq + r$, where q, r are integers and $0 < r < e$. Observe that r can not be 0; otherwise we get $\alpha^{2m} + \alpha^m + 1 = 1 + 1 + 1 = 3 = 0$ which is not possible. Suppose that $2r < e$. Then $x^{2r} + x^r + 1$ is a self-reciprocal trinomial of degree $< e$ and $f(x)$ divides this trinomial since $\alpha^{2m} + \alpha^m + 1 = \alpha^{2r} + \alpha^r + 1 = 0$. Now assume that $2r > e$. Let $r_1 = 2r - e$. Then $0 < r - r_1 = e - r < r$ and

$$0 = \alpha^{2m} + \alpha^m + 1 = \alpha^r + \alpha^{r_1} + 1.$$

Also, we have

$$0 = (\alpha^{-1})^{2m} + (\alpha^{-1})^m + 1 = \alpha^{-r} + \alpha^{-r_1} + 1.$$

Then multiplying by α^r both sides of the equation $\alpha^{-r} + \alpha^{-r_1} + 1 = 0$, we have $\alpha^r + \alpha^{r-r_1} + 1 = 0$. So we have $\alpha^{r-r_1} = \alpha^{r_1}$. From this we get $\alpha^{r-2r_1} = 1$. Since the order of α is e, it follows that $e \mid (r - 2r_1)$. But $r - 2r_1 = r - (4r - 2e) = 2e - 3r < e$. Hence $r - 2r_1 = 0$ and $r = 2r_1$. Therefore, $f(x)$ divides the self-reciprocal trinomial $x^{2r_1} + x^{r_1} + 1$ and this polynomial has degree $2r_1 = r < e$. Moreover, since $\alpha^{2r_1}+\alpha^{r_1}+1 = 0$, we have $\alpha^{3r_1} = 1$ which implies that $e \mid (3r_1)$. On the other hand, we have $2r_1 < e$, so $e = 3r_1$. Now, we show the uniqueness. Suppose that m_1 is another integer such that $f(x)$ divides $\alpha^{2m_1} + \alpha^{m_1} + 1$, where $2m_1 < e$. Then by the same discussion we get $e = 3m_1$. Therefore, $e = 3r_1 = 3m_1$ and $r_1 = m_1$. □

The following theorem characterizes irreducible divisors of self-reciprocal trinomials over $\mathbb{F}_2$, based on $ord(f)$.

Theorem 3.3.12 *Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_2$. Then $f(x)$ divides a self-reciprocal trinomial over $\mathbb{F}_2$ if and only if $ord(f)$ is divisible by 3.*

Proof: Suppose that $f(x)$ divides the self-reciprocal trinomial $x^{2m} + x^m + 1$. By Lemma 3.3.11, $f(x)$ divides a self-reciprocal trinomial $x^{2r} + x^r + 1$ which has degree $2r < e$, where e is the order of $f(x)$. Let α be a root of $f(x)$. Since $f(x)$ divides $x^{2r} + x^r + 1$, we have $\alpha^{2r} + \alpha^r + 1 = 0$. As in the proof of Lemma 3.3.11, we get $e = 3r$. Hence e is a multiple of 3. Conversely, suppose that e is a multiple of 3. Let $e = 3r$ for some $r \in \mathbb{Z}^+$. If α is a root of $f(x)$, then $\alpha^e = \alpha^{3r} = 1$; that is $0 = \alpha^{3r} - 1 = (\alpha^r - 1)(\alpha^{2r} + \alpha^r + 1)$. Note that $\alpha^r - 1 \neq 0$ since $r < e$. Therefore, we get $\alpha^{2r} + \alpha^r + 1 = 0$. This means that $f(x)$ divides the self-reciprocal trinomial $x^{2r} + x^r + 1$. □

Example 3.3.4 *Consider the polynomial $x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$. This is an irreducible polynomial over $\mathbb{F}_2$ of order 5. Then the order of this polynomial is not a* *multiple of* 3*. By Theorem 3.3.12,* $x^4+x^3+x^2+x+1$ *can not divide a self-reciprocal trinomial* $x^{2m}+x^m+1$*. To see this more clearly, suppose that* $x^4+x^3+x^2+x+1$ *divides a self-reciprocal trinomial* $x^{2m}+x^m+1$*, where* $2m < 5$*. Let* α *be a root of* $x^4+x^3+x^2+x+1$*. Note that the order of* α *is* 5*. By assumption, we have* $\alpha^{2m}+\alpha^m+1=0$*. It follows that* $\alpha^{3m}=1$*. Then we have* $5 \mid (3m)$*. In particular,* $5 \leq 3m$*. It follows that* $5=3m$*, which is not possible.*

The following theorem gives a factorization of self-reciprocal trinomials over $\mathbb{F}_2$.

Theorem 3.3.13 *For any given odd number* m*, we have*

$$x^{2m}+x^m+1=\prod_{\substack{n\mid m\\ 3n\nmid m}} Q_{3n} \tag{3.1}$$

where Q_{3n} *denotes the* $3n$*-th cyclotomic polynomial over* $\mathbb{F}_2$*.*

Proof: Assume that $n \mid m$ but $3n \nmid m$. Note that Q_{3n} is the product of all irreducible polynomials of order $3n$. Let $f(x)$ be an irreducible polynomial of order $3n$ and let α be a root of $f(x)$. Thus we have $\alpha^{3n}=1$ and since $3n \mid 3m$, we get $\alpha^{3m}=1$. It follows that $(\alpha^m-1)(\alpha^{2m}+\alpha^m+1)=0$. Since $3n \nmid m$, $\alpha^m-1\neq 0$ and $\alpha^{2m}+\alpha^m+1=0$. So $f(x)$ divides the trinomial $x^{2m}+x^m+1$. Since any irreducible factor of Q_{3n} divides $x^{2m}+x^m+1$, Q_{3n} divides $x^{2m}+x^m+1$. So it suffices to show that both sides of the equation (3.1) have the same degree; that is

$$\sum_{\substack{n\mid m\\ 3n\nmid m}} \phi(3n)=2m.$$

By using the formula $\sum_{d\mid m}\phi(d)=m$ for the Euler's function ϕ, we get

$$\begin{aligned}\sum_{\substack{n\mid m\\ 3n\nmid m}} \phi(3n) &= \sum_{n\mid m}\phi(3n)-\sum_{3n\mid m}\phi(3n)\\ &= \sum_{3n\mid 3m}\phi(3n)-\sum_{3n\mid m}\phi(3n)\\ &= 3m-m=2m.\end{aligned}$$

□

Example 3.3.5 *Consider the self-reciprocal trinomial* $x^{42}+x^{21}+1$*. By Theorem 3.3.13, we have*

$$x^{42}+x^{21}+1=\prod_{\substack{n\mid 21\\ 3n\nmid 21}} Q_{3n}.$$

Positive divisors of 21 *are* $1,3,7$ *and* 21*. Because of the condition* $3n\nmid 21$*, we just take the divisors* 3 *and* 21*. So we have the factorization:*

$$x^{42}+x^{21}+1=Q_9Q_{63}.$$

Note that the degree of $x^{42}+x^{21}+1 = \phi(9)+\phi(63) = 6+36 = 42$, where $\phi(9)+\phi(63)$ is the degree of the polynomial Q_9Q_{63}.

Corollary 3.3.14 *If m is an odd number and $m = 3^k n$, $3 \nmid n$ for $k \geq 0$, then $x^{2m} + x^m + 1$ is divisible by the self-reciprocal irreducible trinomial $x^{2.3^k} + x^{3^k} + 1$.*

Proof: The trinomial $x^{2.3^k} + x^{3^k} + 1$ has order 3^{k+1} and it is irreducible over $\mathbb{F}_2$. Since $Q_{3^{k+1}}$ is the product of irreducible polynomials of order 3^{k+1}, it follows that $x^{2.3^k} + x^{3^k} + 1$ divides $Q_{3^{k+1}}$. Observe that $3^k \mid m$ but $3^{k+1} \nmid m$. By Theorem 3.3.13, $Q_{3^{k+1}}$ divides the trinomial $x^{2m}+x^m+1$, thus $x^{2.3^k} + x^{3^k} + 1$ divides $x^{2m}+x^m+1$. □

Example 3.3.6 *Let $m = 3^2.5 = 45$. Then m is odd, $n = 5$ and 5 is not divisible by 3. Note that $k = 2$. Then by Corollary 3.3.14, the self-reciprocal irreducible trinomial $x^{2.3^2} + x^{3^2} + 1 = x^{18}+x^9+1$ divides the trinomial $x^{90}+x^{45}+1$. Indeed, we have the factorization*

$$x^{90}+x^{45}+1 = (x^{18}+x^9+1)(x^{72}+x^{63}+x^{45}+x^{36}+x^{27}+x^9+1).$$

Remark 3.3.1 *Theorem 3.3.13 can be generalized for an arbitrary m in the following way: Let $m = 2^k n$, where $2 \nmid n$. Then we have*

$$x^{2m}+x^m+1 = \left(\prod_{\substack{n_1 \mid n \\ 3n_1 \nmid n}} Q_{3n_1} \right)^{2^k}.$$

Lemma 3.3.15 *Let $f(x)$ be an irreducible polynomial of order e over $\mathbb{F}_2$. Assume that $f(x)$ divides a trinomial $x^n + x^k + 1$. Then it divides at least one trinomial of degree $< e$.*

Proof: Assume that $f(x)$ divides $x^n + x^k + 1$. Let α be a root of $f(x)$. Then $\alpha^n + \alpha^k + 1 = 0$. Since $\alpha^e = 1$, this gives $\alpha^{n'} + \alpha^{k'} + 1 = 0$, where $n \equiv n' \pmod{e}$ and $k \equiv k' \pmod{e}$. So we can choose n' and k' on the range from 0 to $e-1$. Observe that n' and k' can not be 0. If both n' and k' are 0, we get $1 = 0$. Now suppose that $n' = 0$ but $k' \neq 0$. If α is a root of $f(x)$, then we get $1 + \alpha^{k'} + 1 = 0$. It follows that $\alpha = 0$. It is impossible since $f(x)$ is an irreducible polynomial and it divides a trinomial. The case $k' = 0$ and $n' \neq 0$ is similar. So $f(x)$ divides the trinomial $x^{n'} + x^{k'} + 1$ and this trinomial has degree less than e. □

Theorem 3.3.16 *Suppose that $f(x)$ is an irreducible polynomial of order e over $\mathbb{F}_2$ and $f(x)$ divides at least one trinomial over $\mathbb{F}_2$. Then*

$$N_f = \frac{1}{2} deg(gcd(1+x^e, 1+(1+x)^e))$$

where N_f denotes the number of trinomials of degree less than e, which are divided by $f(x)$.

Proof: Let $1+x^e = g_1(x)g_2(x)\dots g_t(x)$ be a product of all irreducible polynomials which have order dividing e. By substituting $1+x$ to x, we get

$$1+(1+x)^e = g_1(x+1)g_2(x+1)\dots g_t(x+1).$$

Let α be a root of $f(x)$. Then $1, \alpha, \alpha^2, \dots, \alpha^{e-1}$ are roots of $g_1(x), g_2(x), \dots, g_t(x)$. Thus $0, 1+\alpha, 1+\alpha^2, \dots, 1+\alpha^{e-1}$ are roots of $g_1(x+1), g_2(x+1), \dots, g_t(x+1)$. By assumption $f(x)$ divides at least one trinomial over $\mathbb{F}_2$; that is there exists at least one pair (i,j) such that $1 \le i, j < e$, where $i \neq j$ and $\alpha^i = \alpha^j + 1$. The number of such pairs is equal to the number of common roots of $1+x^e$ and $1+(1+x)^e$. This number is equal to the degree of the polynomial $gcd(1+x^e, 1+(1+x)^e)$. Note that $gcd(1+x^e, 1+(1+x)^e)$ does not have any multiple roots. The different pairs (i,j) and (j,i) correspond to the same trinomial, so the result follows. □

The case $N_f = 1$ yields an interesting result.

Theorem 3.3.17 *If $N_f = 1$, then $f(x)$ divides a self-reciprocal trinomial over $\mathbb{F}_2$.*

Proof: Let $e = ord(f)$. By Theorem 3.3.12, it suffices to show that e is a multiple of 3. To the contrary, assume that e is not a multiple of 3 and $f(x)$ divides the trinomial $x^n + x^k + 1$, where $n < e$. Then since e is not a multiple of 3, $x^n + x^k + 1$ can not be self-reciprocal; that is $n \neq 2k$. Let α be a root of $f(x)$. Then α^{-1} is a root of $f^*(x)$. Since $f^*(x)$ divides $x^n + x^{n-k} + 1$, we have

$$\alpha^{-n} + \alpha^{-(n-k)} + 1 = 0.$$

It follows that

$$\alpha^{e-n} + \alpha^{e-n+k} + 1 = 0.$$

Note that $0 < e-n, e-n+k < e$, $e-n \neq e-n+k$. Therefore $f(x)$ divides the trinomial $x^{e-n} + x^{e-n+k} + 1$. Since e is odd, $e-n \neq n$. Now assume that $e-n = k$. Then we have $\alpha^{n+k} = \alpha^e = 1$. If we multiply both sides of the equation $\alpha^n + \alpha^k + 1 = 0$ by α^k, we have

$$\alpha^{2k} + \alpha^k + 1 = 0.$$

Since α was arbitrary, this means that $f(x)$ divides the self-reciprocal trinomial $x^{2k} + x^k + 1$. That contradicts to the assumption that e is not a multiple of 3. Therefore $e-n \neq k$. Thus $f(x)$ divides $x^n + x^k + 1$ and $x^{e-n} + x^{e-n+k} + 1$ and they are two different trinomials of degree less than e. Therefore, $N_f \geq 2$. □

3.4. Divisibility of Self-reciprocal Trinomials by Irreducible Polynomials over $\mathbb{F}_3$

Firstly, we determine self-reciprocal trinomials over $\mathbb{F}_3$. Suppose that $ax^n + bx^m + c$ is a self-reciprocal trinomial, where $a, b, c \in \mathbb{F}_3$. Then we have $ax^n + bx^m + c =$

$x^n\left(\frac{a}{x^n}+\frac{b}{x^m}+c\right) = a+bx^{n-m}+cx^n$. It follows that $a=c$ and $n=2m$. Therefore, self-reciprocal trinomials over $\mathbb{F}_3$ must be of the form $x^{2m}+x^m+1$, $2x^{2m}+x^m+2$, $x^{2m}+2x^m+1$ or $2x^{2m}+2x^m+2$. Observe that $2x^{2m}+2x^m+2 = 2(x^{2m}+x^m+1)$ and $2x^{2m}+x^m+2 = 2x^{2m}+4x^m+2 = 2(x^{2m}+2x^m+1)$. So it suffices to consider divisibility of self-reciprocal trinomials which have the forms $x^{2m}+x^m+1$ and $x^{2m}+2x^m+1$ over $\mathbb{F}_3$.

Lemma 3.4.18 *Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_3$ of order e and assume that $f(x)$ divides the self-reciprocal trinomial $x^{2m}+x^m+1$, where e does not divide m. Then there exists a unique self-reciprocal trinomial which has degree $< e$ and is divisible by $f(x)$.*

Proof: Let α be a root of $f(x)$ in some extension of $\mathbb{F}_3$. Since $f(x) \mid (x^{2m}+x^m+1)$, α is also a root of this trinomial. Hence we have $\alpha^{2m}+\alpha^m+1=0$. Let $m=eq+r$, where q, r are integers and $0<r<e$. Observe that r can not be 0 since e does not divide m. Suppose that $2r<e$. Then $x^{2r}+x^r+1$ is a self-reciprocal trinomial of degree $<e$ and $f(x)$ divides this trinomial since $\alpha^{2m}+\alpha^m+1 = \alpha^{2r}+\alpha^r+1=0$. Now assume that $2r>e$. Let $r_1=2r-e$. Then $0<r-r_1=e-r<r$ and

$$0=\alpha^{2m}+\alpha^m+1=\alpha^r+\alpha^{r_1}+1.$$

Also, we have

$$0=(\alpha^{-1})^{2m}+(\alpha^{-1})^m+1=\alpha^{-r}+\alpha^{-r_1}+1$$

Then multiplying by α^r both sides of the equation $\alpha^{-r}+\alpha^{-r_1}+1=0$, we have $\alpha^r+\alpha^{r-r_1}+1=0$. So we have $\alpha^{r-r_1}=\alpha^{r_1}$. From this we get $\alpha^{r-2r_1}=1$. Since the order of α is e, it follows that $e \mid (r-2r_1)$. But $r-2r_1 = r-(4r-2e) = 2e-3r<e$. Hence $r-2r_1=0$ and $r=2r_1$. Therefore $f(x)$ divides the self-reciprocal trinomial $x^{2r_1}+x^{r_1}+1$ and this polynomial has degree $2r_1=r<e$. Moreover, since $\alpha^{2r_1}+\alpha^{r_1}+1=0$, we have $\alpha^{3r_1}=1$, which implies that $e \mid (3r_1)$. On the other hand, we have $2r_1<e$, so $e=3r_1$. Now, we show the uniqueness. Suppose that m_1 is another integer such that $f(x) \mid (x^{2m_1}+x^{m_1}+1)$, where $2m_1<e$. Then by the same discussion we get $e=3m_1$. Therefore $e=3r_1=3m_1$ and $r_1=m_1$. □

Theorem 3.4.19 *Suppose that $f(x)$ is an irreducible polynomial of order e over $\mathbb{F}_3$, where e does not divide m. If $f(x) \mid (x^{2m}+x^m+1)$, then e is a multiple of 3 and if e is a multiple of 3, then $f(x)$ divides a self-reciprocal trinomial of the form $x^{2r}+x^r+1$.*

Proof: Suppose that $f(x)$ divides the self-reciprocal trinomial $x^{2m}+x^m+1$. By Lemma 3.4.18, $f(x)$ divides a self-reciprocal trinomial $x^{2r}+x^r+1$ which has degree $2r<e$. Let α be a root of $f(x)$. Since $f(x) \mid (x^{2r}+x^r+1)$, we have $\alpha^{2r}+\alpha^r+1=0$. As in the proof of Lemma 3.4.18, we get $e=3r$. Hence e is a multiple of 3. Conversely, suppose that e is a multiple of 3. Let $e=3r$ for some $r\in\mathbb{Z}^+$. Let α be a root of $f(x)$.

Then $\alpha^e = \alpha^{3r} = 1$; that is $0 = \alpha^{3r} - 1 = (\alpha^r - 1)(\alpha^{2r} + \alpha^r + 1)$. Since $r < e$, $\alpha^r - 1 \neq 0$. Therefore $\alpha^{2r} + \alpha^r + 1 = 0$. This means that $f(x)$ divides the self-reciprocal trinomial $x^{2r} + x^r + 1$. □

Now we give a criteria for divisibility of self-reciprocal trinomials of the form $x^{2m} + 2x^m + 1$ by irreducible polynomials over $\mathbb{F}_3$. Observe that $x^{2m} + 2x^m + 1 = (x^m + 1)^2$. Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_3$ and suppose that $f(x) \mid (x^m + 1)^2$, then $f(x) \mid (x^m + 1)$. So it suffices to consider divisibility of binomial $x^m + 1$ by irreducible polynomials over $\mathbb{F}_3$.

Lemma 3.4.20 *Let $f(x)$ be an irreducible polynomial of order e over $\mathbb{F}_3$. Suppose that e does not divide m and $m \equiv n \pmod{e}$. Then $f(x)$ divides the binomial $x^m + 1$ over $\mathbb{F}_3$ if and only if $e \mid 2n$.*

Proof: Assume that $f(x) \mid (x^m + 1)$. Then for any root α of $f(x)$ we have $\alpha^m + 1 = 0$. Note that $m = ek + n$ for some integer k. It follows that

$$\alpha^m + 1 = \alpha^{ek+n} + 1 = \alpha^n + 1 = 0.$$

Therefore, $\alpha^n = -1$ and $\alpha^{2n} = 1$. Hence, the order e of $f(x)$ divides $2n$.

Conversely, let $m \equiv n \pmod{e}$ and suppose that $e \mid 2n$. Then for any root α of $f(x)$, we have $\alpha^{2n} = 1$. Then $(\alpha^n - 1)(\alpha^n + 1) = 0$. Since $n < e$ and $n \neq 0$, $\alpha^n - 1 \neq 0$. It follows that $\alpha^n + 1 = 0$. This means that $f(x)$ divides the binomial $x^n + 1$ over $\mathbb{F}_3$. But then $f(x)$ divides the binomial $x^m + 1$ since $m \equiv n \pmod{e}$. □

CHAPTER 4

Irreducible Polynomials with Prescribed Coefficients

So far we focused on problems like the irreducibility, divisibility, enumeration of binomials, trinomials and self-reciprocal polynomials. Another line of active research is on the existence/enumeration of irreducible polynomials with prescribed coefficients. One, of course, may also consider these questions for subclasses of irreducible polynomials like primitive or self-reciprocal irreducible polynomials. We refer to Chapter 3 of [26], Section 3.5 of [23] and the papers [3, 9] and the references therein for an extensive survey of results on these and related problems.

As we did in Chapter 3, we denote the monic polynomials of degree n in $\mathbb{F}_q[x]$ by $\mathcal{M}_n(q)$ and the irreducible polynomials in $\mathcal{M}_n(q)$ by $\mathcal{I}_n(q)$. Putting

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n \tag{4.1}$$

we refer to a_i, $1 \leq i \leq n$, as the i-th coefficient of $f(x)$. We call $\{a_1, \ldots, a_k\}$ the first k coefficients and $\{a_{n-l+1}, \ldots, a_n\}$ the last l coefficients of $f(x)$. For obvious reasons, $-a_1$ and $(-1)^n a_n$ are called the trace and norm, respectively.

In this chapter, we give a brief survey of results concerning polynomials in $\mathcal{I}_n(q)$ with prescribed coefficients with emphasis on the recent work.

4.1. Questions on Existence

We start by stating the well-known Hansen-Mullen conjecture, going back to 1992. This conjecture, now a theorem, is on the existence of irreducible polynomials in $\mathcal{M}_n(q)$ with any arbitrary coefficients being prescribed.

Hansen-Mullen Conjecture: Let $a \in \mathbb{F}_q$, $n \geq 2$ and $1 \leq i \leq n$ be fixed. Then there exists an irreducible polynomial $f(x) = x^n + \sum_{i=1}^{n} a_i x^{n-i} \in \mathbb{F}_q[x]$ with $a_i = a$ except for $a_n = a = 0$ or q is even and $(n, i, a) = (2, 1, 0)$.

Hansen and Mullen proved this conjecture for $i = n - 1$ and Cohen [4] proved it for $i = 1$. Wan [29] proved that it is true for $q > 19$ and $n \geq 36$. The cases $q \leq 19$ or $n < 36$ were settled by the use of computations by Ham and Mullen [14] and by Cohen and Presern [7, 8] independently. An alternative proof of a very different nature of Hansen-Mullen conjecture has been given recently by A. Tuxanidy and Q. Wang [28].

This existence question can be extended in various ways. One may consider several coefficients to be prescribed or subclasses of $\mathcal{I}_n(q)$. An interesting result, for example, was obtained by T. Garefalakis and G. Kapetanakis [11], where they considered the Hansen-Mullen conjecture for self-reciprocal polynomials. We state it below and it is Theorem 4.2 in [11].

Theorem 4.1.1 *Let n, i be natural numbers, where $n \geq 2$, $1 \leq i \leq n$, and $a \in \mathbb{F}_q$. There exists a self-reciprocal polynomial $f(x) \in \mathcal{I}_n(q)$ in the form 4.1 with $a_i = a$, if the inequality $q^{(n-k-1)/2} \geq \frac{16}{5}i(i+5) + \frac{1}{2}$ holds.*

This result was improved in Theorem 1 of [12] recently by using computations:

Theorem 4.1.2 *Let q be odd and $a \in \mathbb{F}_q$, $n \geq 1$. There exists a self-reciprocal polynomial $f(x) \in \mathcal{I}_{2n}(q)$ such that $a_i = a$ except $(q, n, i, a) = (3, 3, 5, 0)$ and $(q, n, i, a) = (3, 4, 6, 0)$.*

Another subclass of irreducible polynomials in $\mathcal{M}_n(q)$ is the set $\mathcal{P}_n(q)$ of primitive polynomials. Han [15] and Cohen and Mills [6] addressed the problem of existence of primitive polynomials with the first and second coefficients prescribed. We recall that a polynomial $f(x) \in \mathbb{F}_q[x]$ is primitive, if it is the minimal polynomial of a primitive element over $\mathbb{F}_q$. The existence of polynomials in $\mathcal{P}_n(q)$ with prescribed trace $-a_1 = a \in \mathbb{F}_q$ was obtained in [4] and [17], the exceptional cases being $(a, n) = (0, 3)$ for $q = 4$ and $(a, n) = (0, 2)$ when q is arbitrary. When q is odd and $n \geq 7$ Han [15] showed that a polynomial $f(x) \in \mathcal{P}_n(q)$ exists with arbitrarily prescribed first and second coefficients. Cohen and Mills [6] extended this result to the cases $n = 5, 6$.

The questions concerning the existence of polynomials in $\mathcal{I}_n(q)$ with more prescribed coefficients have attracted considerable attention. When coefficients are fixed to be zero, one can consider trinomials $x^n + x + b \in \mathcal{I}_n(q)$, for instance. Their existence for sufficiently large q with respect to n was obtained, for instance, by Cohen [5]. A very interesting result in this direction is due to T. Garefalakis [10]. He showed that there exists a polynomial $f(x) \in \mathcal{I}_n(q)$ with roughly $n/3$ consecutive coefficients prescribed to be zero. Recent work of Panario and Tzanakis [24] also addresses related problems, i.e., the existence of $f(x) \in \mathcal{I}_n(q)$ with many prescribed coefficients, including the case, where some coefficients are zero.

4.2. Questions on Enumeration

The number $N_n(q)$ of polynomials in $\mathcal{I}_n(q)$ is well-known and is easy to obtain. Consider the polynomial $x^{q^n} - x$ over $\mathbb{F}_q$, where $n \in \mathbb{Z}^+$. Then we have

$$x^{q^n} - x = \prod_{\alpha \in \mathbb{F}_{q^n}} (x - \alpha) = \prod_{\substack{f \in \mathcal{I}_d(q) \\ d|n}} f(x). \tag{4.2}$$

If we take degrees on both sides of the equation (4.2) and apply the Möbius inversion formula, we get

$$N_n(q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

The number of polynomials in $\mathcal{I}_n(q)$ with prescribed coefficients (trace and/or norm) was obtained by Carlitz [2] and Kuzmin [20]. Yucas [30] proved Carlitz' result by using elementary arguments. We give the proof below.

Throughout this section, we put $-a_1 = tr(f)$ for a polynomial $f(x)$ as in (4.1).

For $\gamma \in \mathbb{F}_q$, let $I_\gamma(n,q)$ denote the set of all monic irreducible polynomials over $\mathbb{F}_q$ of degree n and trace γ. Denote the cardinality of $I_\gamma(n,q)$ by $N_\gamma(n,q)$.

Lemma 4.2.3 *Let $\gamma, \delta \in \mathbb{F}_q^*$. Then there exists a bijection between $I_\gamma(n,q)$ and $I_\delta(n,q)$; that is $N_\gamma(n,q) = N_\delta(n,q)$.*

Proof: Consider the map $\Psi : I_\gamma(n,q) \to I_\delta(n,q)$ defined by

$$\Psi(f(x)) = \left(\frac{\delta}{\gamma}\right)^n f\left(\frac{\gamma}{\delta}x\right).$$

Firstly, we show that any element in $I_\gamma(n,q)$ is mapped to an element in $I_\delta(n,q)$ by Ψ. So let $f(x) \in I_\gamma(n,q)$. Write $f(x) = x^n - \gamma x^{n-1} + a_2 x^{n-2} + \ldots + a_n$, where $a_i \in \mathbb{F}_q$ for $i = 2, \ldots, n$. Then we have

$$\Psi(f(x)) = \left(\frac{\delta}{\gamma}\right)^n \left(\left(\frac{\gamma}{\delta}x\right)^n - \gamma\left(\frac{\gamma}{\delta}x\right)^{n-1} + a_2\left(\frac{\gamma}{\delta}x\right)^{n-2} + \ldots + a_n\right) = x^n - \delta x^{n-1} + \ldots + \frac{\delta^n}{\gamma^n} a_n.$$

Therefore, $tr(\Psi(f)) = \delta$. Note that $\Psi(f(x))$ is a monic irreducible polynomial of degree n over $\mathbb{F}_q$. Hence $\Psi(f(x)) \in I_\delta(n,q)$. Now we show that the map Ψ is a bijection. The map Ψ is one-to-one: Suppose that $\Psi(f(x)) = \Psi(g(x))$ for $f(x), g(x) \in I_\gamma(n,q)$. Let

$$f(x) = x^n - \gamma x^{n-1} + a_2 x^{n-2} + \ldots + a_n$$
$$g(x) = x^n - \gamma x^{n-1} + b_2 x^{n-2} + \ldots + b_n$$

where a_i and b_i are in $\mathbb{F}_q$. Then by assumption

$$x^n - \delta x^{n-1} + \ldots + \frac{\delta^n}{\gamma^n} a_n = x^n - \delta x^{n-1} + \ldots + \frac{\delta^n}{\gamma^n} b_n$$

Thus $a_i = b_i$ for $i = 2, \ldots, n$. It follows that $f(x) = g(x)$. Now we show that Ψ is onto. To this end, let $g(x) \in I_\delta(n,q)$. We want to show that there exists $f(x) \in I_\gamma(n,q)$ such that $\Psi(f(x)) = g(x)$. Consider the polynomial $f(x) = \left(\frac{\gamma}{\delta}\right)^n g\left(\frac{\delta}{\gamma}x\right)$. Then we have

$$\Psi(f(x)) = \Psi\left(\left(\frac{\gamma}{\delta}\right)^n g\left(\frac{\delta}{\gamma}x\right)\right) = \left(\frac{\gamma\delta}{\delta\gamma}\right)^n g\left(\frac{\gamma}{\delta}\frac{\delta}{\gamma}x\right) = g(x).$$

This shows that Ψ is an onto map and hence Ψ is a bijection between $I_\gamma(n,q)$ and $I_\delta(n,q)$. Thus we have $N_\gamma(n,q) = N_\delta(n,q)$. □

Now consider the following integer recurrence:

$$D(1) = 1$$

$$D(n) = q^{n-1} + D(n/p) \text{ for } n > 1.$$

When n is not divisible by p, $D(n/p)$ is defined to be 0.

Lemma 4.2.4 *Let $n = p^k m$ and $p \nmid m$. Then*

$$D(n) = \sum_{i=0}^{k} q^{p^{k-i}m-1}.$$

Proof: We proceed by induction on k. When $k = 0$, we have $n = m$ and both sides of the equation are equal to q^{n-1}. Now suppose that $k > 0$ and the equality holds for $k-1$. We show that the equality holds for k.

$$\begin{aligned} D(n) &= D(p^k m) = q^{p^k m-1} + D(p^{k-1}m) \\ &= q^{p^k m-1} + \sum_{i=0}^{k-1} q^{p^{k-1-i}m-1} = \sum_{i=0}^{k} q^{p^{k-i}m-1}. \end{aligned}$$

□

Let $\gamma \in \mathbb{F}_q$ and $n \in \mathbb{Z}^+$. Define the polynomial $q_{n,\gamma}(x)$ over $\mathbb{F}_q$ by

$$q_{n,\gamma}(x) = -\gamma + x + x^q + x^{q^2} + \ldots + x^{q^{n-1}}.$$

The following lemma gives factorization of $x^{q^n} - x$ in terms of the polynomials $q_{n,\gamma}(x)$, where $\gamma \in \mathbb{F}_q$.

Lemma 4.2.5

$$x^{q^n} - x = \prod_{\gamma \in \mathbb{F}_q} q_{n,\gamma}(x).$$

Proof: We have

$$x^q - x = \prod_{\gamma \in \mathbb{F}_q} (x - \gamma).$$

If we replace x by $x + x^q + x^{q^2} + \ldots + x^{q^{n-1}}$ in this equation, we get

$$(x+x^q+x^{q^2}+\ldots+x^{q^{n-1}})^q-(x+x^q+x^{q^2}+\ldots+x^{q^{n-1}}) = \prod_{\gamma \in \mathbb{F}_q}(x+x^q+x^{q^2}+\ldots+x^{q^{n-1}}-\gamma).$$

It follows that

$$x^{q^n} - x = \prod_{\gamma \in \mathbb{F}_q} q_{n,\gamma}(x).$$

□

Let $\widetilde{I}(n,q)$ denote the set of all monic irreducible polynomials over $\mathbb{F}_q$ which have degree dividing n.

Lemma 4.2.6 *Let $\gamma \in \mathbb{F}_q^*$. Consider the set*

$$H_{n,\gamma} = \{h(x) \in \widetilde{I}(n,q) : p \nmid n/deg(h) \ and \ (n/deg(h))tr(h) = \gamma\}.$$

Then we have

$$q_{n,\gamma}(x) = \prod_{h \in H_{n,\gamma}} h(x).$$

Proof: Let $r(x)$ be an irreducible factor of $q_{n,\gamma}(x)$ of degree d. We show that $r(x)$ is an element of the set $H_{n,\gamma}$. Since $q_{n,\gamma}(x)$ divides $x^{q^n} - x$ we see that d divides n. Let $\alpha \in \mathbb{F}_{q^d}$ be a root of $r(x)$. Then

$$tr(r) = Tr_{F/K}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{d-1}}.$$

where $F = \mathbb{F}_{q^d}$ and $K = \mathbb{F}_q$. Since d divides n and α is also a root of $q_{n,\gamma}(x)$ we see that n/d is not divisible by p and $(n/d)Tr_{F/K}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{n-1}} = \gamma$. Thus we have $(n/d)tr(r) = \gamma$. Therefore, $r(x)$ belongs to $H_{n,\gamma}$. Now we want to show that any polynomial $h(x) \in H_{n,\gamma}$ divides $q_{n,\gamma}(x)$. So suppose that $h(x)$ is a monic irreducible polynomial of degree d and assume that $d \mid n$, n/d is not divisible by p and $(n/d)tr(h) = \gamma$. Let $\alpha \in \mathbb{F}_{q^d}$ be any root of $h(x)$. Then $(n/d)Tr_{F/K}(\alpha) = \gamma = \alpha + \alpha^q + \ldots + \alpha^{q^{n-1}}$. So α satisfies the polynomial $q_{n,\gamma}(x)$. Since α was arbitrary, it follows that $h(x)$ divides $q_{n,\gamma}(x)$. □

Let $q_{n,\gamma}(x) = g_1(x)g(x)$, where

$$g_1(x) = \prod_{\substack{h \in H_{n,\gamma} \\ d=n}} h(x) \qquad \text{and} \qquad g(x) = \prod_{\substack{h \in H_{n,\gamma} \\ d<n}} h(x).$$

Then

$$g_1(x) = \prod_{h \in G_1} h(x),$$

where

$$G_1 = \{h(x) \in \widetilde{I}(n,q) : deg(h) = n \text{ and } tr(h) = \gamma\}.$$

Let

$$G_2 = \{h(x) \in \widetilde{I}(n,q) : p \mid n/deg(h) \text{ and } tr(h) = \gamma\}$$

and

$$G_3 = \{h(x) \in \widetilde{I}(n,q) : deg(h) < n, p \nmid n/deg(h) \text{ and } tr(h) = \gamma\}.$$

Define

$$g_2(x) = \prod_{h \in G_2} h(x) \qquad \text{and} \qquad g_3(x) = \prod_{h \in G_3} h(x).$$

Then

$$B_{n,\gamma}(x) = g_1(x)g_2(x)g_3(x)$$

Then

$$B_{n,\gamma}(x) = \prod_{\substack{f \in \mathcal{I}_d(q) \\ d|n \\ tr(f)=\gamma}} f(x).$$

Proposition 4.2.7 *Let $D(n) = deg(B_{n,\gamma})$. Then $D(n)$ satisfies the recurrence $D(n) = q^{n-1} + D(n/p)$.*

Proof: Note that $g_2(x)$ is the product of all monic irreducible polynomials which have degree dividing n/p with trace γ. Thus, $deg(g_2) = D(n/p)$. By Lemma 4.2.3, we have $deg(g_3) = deg(g)$. Then we have

$$\begin{aligned} D(n) = deg(B_{n,\gamma}) &= deg(g_1) + deg(g_2) + deg(g_3) \\ &= deg(g_1) + D(n/p) + deg(g) \\ &= deg(q_{n,\gamma}) + D(n/p) \\ &= q^{n-1} + D(n/p). \end{aligned}$$

□

Theorem 4.2.8 *Let $\gamma \in \mathbb{F}_q^*$. Then we have*

$$N_\gamma(n,q) = \frac{1}{n} \sum_{d|n} \mu(n/d) \sum_{i=0}^{k_d} q^{p^{(k_d-i)}m_d - 1},$$

where $d = p^{k_d} m_d$ and $p \nmid m_d$.

Proof:

$$D(n) = deg(B_{n,\gamma}) = \sum_{d|n} dN_\gamma(d,q).$$

By Lemma 4.2.4, we have

$$D(n) = \sum_{i=0}^{k} q^{p^{k-i}m-1},$$

where $n = p^k m$ and $p \nmid m$. By applying the Möbius inversion formula, we get

$$N_\gamma(n,q) = \frac{1}{n}\sum_{d|n}\mu(n/d)\sum_{i=0}^{k_d} q^{p^{(k_d-i)}m_d-1}.$$

□

Corollary 4.2.9 *Let $n = p^k m$ and $p \nmid m$. If $\gamma \in \mathbb{F}_q^*$, then*

$$N_\gamma(n,q) = \frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d}.$$

Proof: Let r be a divisor of n. Then $r = p^j d$, where d is a divisor of m and $0 \le j \le k$. If $j < k-1$, then p^2 divides n/r hence $\mu(n/r) = 0$. Therefore, in Theorem 4.2.8, it suffices to consider divisors of n of the form $p^k d$ or $p^{k-1}d$, where d is a divisor of m. Also note that $\mu(n/p^k d) = \mu(m/d)$ and $\mu(n/p^{k-1}d) = -\mu(m/d)$. So by using these facts, we have

$$\begin{aligned}
\mu(n/p^k d)\sum_{i=0}^{k} q^{p^{k-i}d-1} &= \mu(n/p^k d)\left(q^{p^k d-1} + \sum_{i=1}^{k} q^{p^{k-i}d-1}\right)\\
&= \mu(n/p^k d)\left(q^{p^k d-1} + \sum_{i=0}^{k-1} q^{p^{k-1-i}d-1}\right).
\end{aligned}$$

Thus

$$\begin{aligned}
\mu(n/p^k d)\sum_{i=0}^{k} q^{p^{k-i}d-1} + \mu(n/p^{k-1}d)\sum_{i=0}^{k-1} q^{p^{k-1-i}d-1} &= \mu(n/p^k d)(q^{p^k d-1})\\
&= \mu(m/d)(q^{p^k d-1}).
\end{aligned}$$

By Theorem 4.2.8, we have

$$\begin{aligned}
N_\gamma(n,q) &= \frac{1}{n}\sum_{d|m}\mu(m/d)q^{p^k d-1}\\
&= \frac{1}{nq}\sum_{d|m}\mu(m/d)q^{p^k d}\\
&= \frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d}.
\end{aligned}$$

□

Now we obtain a similar expression for $N_0(n,q)$.

Corollary 4.2.10 *Let $n = p^k m$ and $p \nmid m$. We have*

$$N_0(n,q) = \frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d} - \frac{\epsilon}{n}\sum_{d|m}\mu(d)q^{n/dp}$$

where $\epsilon = 1$ if $k > 0$ and $\epsilon = 0$ if $k = 0$.

Proof: Firstly, we consider the case when $k = 0$. Since $k = 0$ we have $n = m$. We want to show that

$$N_0(n,q) = \frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d}.$$

Note that the cardinality of $\mathcal{I}_n(q)$ is given by the formula

$$N_n(q) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}.$$

By Corollary 4.2.9, if $\gamma \in \mathbb{F}_q^*$, we have

$$N_\gamma(n,q) = \frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d}.$$

There are $q-1$ non-zero elements in $\mathbb{F}_q$ and for two non-zero elements γ and δ we have $N_\gamma(n,q) = N_\delta(n,q)$ by Lemma 4.2.3. It follows that

$$\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} = (q-1)\frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d} + N_0(n,q).$$

Therefore, we have

$$\begin{aligned} N_0(n,q) &= \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} - (q-1)\frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d} \\ &= \frac{1}{n}\sum_{d|m}\mu(d)q^{n/d} - (q-1)\frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d} \\ &= \frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d}. \end{aligned}$$

Now we consider the case $k > 0$. We want to show that

$$N_0(n,q) = \frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d} - \frac{1}{n}\sum_{d|m}\mu(d)q^{n/dp}.$$

As in the case $k = 0$, we have

$$\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} = (q-1)\frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d} + N_0(n,q).$$

So we get

$$N_0(n,q) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} - (q-1)\frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d}.$$

Then it suffices to show that

$$\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}-(q-1)\frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d}=\frac{1}{nq}\sum_{d|m}\mu(d)q^{n/d}-\frac{1}{n}\sum_{d|m}\mu(d)q^{n/dp}.$$

So it is enough to show that the following equality holds:

$$\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}=\frac{1}{n}\sum_{d|m}\mu(d)q^{n/d}-\frac{1}{n}\sum_{d|m}\mu(d)q^{n/dp}.$$

i.e.,

$$\sum_{d|n}\mu(d)q^{n/d}=\sum_{d|m}\mu(d)(q^{n/d}-q^{n/dp}).$$

We have

$$\begin{aligned}\sum_{d|n}\mu(d)q^{n/d} &= \sum_{d|n}\mu(n/d)q^{d}=\sum_{d|m}\mu(n/p^{k-1}d)q^{p^{k-1}d}+\sum_{d|m}\mu(n/p^{k}d)q^{p^{k}d}\\ &= \sum_{d|m}\mu(m/d)q^{p^{k}d}-\sum_{d|m}\mu(m/d)q^{p^{k-1}d}=\sum_{d|m}\mu(m/d)(q^{p^{k}d}-q^{p^{k-1}d})\\ &= \sum_{d|m}\mu(d)(q^{n/d}-q^{n/dp}).\end{aligned}$$

□

Example 4.2.7 *Let $q=5$ and $n=5.2=10$. In this case $m=2$. By Corollary 4.2.9, we have*

$$\begin{aligned}N_1(10,5)=N_2(10,5)=N_3(10,5)=N_4(10,5) &= \frac{1}{50}\sum_{d|2}\mu(d)5^{10/d}\\ &= \frac{1}{50}(\mu(1)5^{10}+\mu(2)5^{5})\\ &= \frac{1}{50}(5^{10}-5^{5})=195250.\end{aligned}$$

By Corollary 4.2.10, we have

$$N_0(10,5)=\frac{1}{50}\sum_{d|2}\mu(d)5^{10/d}-\frac{1}{10}\sum_{d|2}\mu(d)5^{10/(5d)}=195250-2=195248.$$

Now we compute the number of monic irreducible polynomials of degree 10 over $\mathbb{F}_5$. We have

$$N_{10}(5)=\frac{1}{10}\sum_{d|10}\mu(d)5^{10/d}=976248.$$

Observe that $976248=4.195250+195248$.

Now, we turn our attention to the number of polynomials $f(x) \in \mathcal{I}_n(q)$ with a large number of prescribed coefficients. Ha [13] recently obtained the number of polynomials $f(x) \in \mathcal{I}_n(q)$ with $k = o(n)$ prescribed coefficients for large n. Consider the set $I = \{i_1, \ldots, i_k\}$, $1 \leq i_j \leq n$ and $b_1, \ldots, b_k \in \mathbb{F}_q$. Put

$$\epsilon = \begin{cases} 1 & \text{if } 0 \notin I, \\ 1 + \frac{1}{q-1} & \text{if } 0 \in I, \text{ and } a_n \neq 0 \\ 0 & \text{if } 0 \in I, \text{ and } a_n = 0. \end{cases}$$

Let $N(n, k, q)$ be the number of polynomials $f(x) \in \mathcal{I}_n(q)$, where $f(x)$ is as in (4.1) and $a_{i_j} = b_j$, $1 \leq j \leq k$.

Ha [13] shows that $N(n, k, q) = \epsilon q^{n-k}(1 + o(1))/n$ when $k = o(n)$ and n is large. See [13] for the precise statement.

The collection of results that we briefly described above is far from being complete. However, they point to many non-trivial questions, which are still open.

Bibliography

[1] O. Ahmadi, *On the Distribution of Irreducible Trinomials over $\mathbb{F}_3$*, Finite Fields and Their Applications **13**, 659-664, 2007.

[2] L. Carlitz, *A Theorem of Dickson on Irreducible Polynomials*, Proceedings of the American Mathematical Society **3**, 693-700, 1952.

[3] S. D. Cohen, *Explicit Theorems on Generator Polynomials*, Finite Fields and Their Applications **11**, 337-357, 2005.

[4] S. D. Cohen, *Primitive Elements and Polynomials with Arbitrary Trace*, Discrete Math. **83**, 1-7, 1990.

[5] S. D. Cohen, *The Distribution of Polynomials over Finite Fields*, Acta Arith. **17**, 255-271, 1970.

[6] S. D. Cohen, D. Mills, *Primitive Polynomials with First and Second Coefficients Prescribed*, Finite Fields and Their Applications **9**, 334-350, 2003.

[7] S. D. Cohen, M. Presern, *Primitive Polynomials with Prescribed Second Coefficient*, Glasg. Math. J. **48**, 281-307, 2006.

[8] S. D. Cohen, M. Presern, *The Hansen-Mullen Primitivity Conjecture: Completion of Proof*, in: Number Theory and Polynomials, in: London Math. Soc. Lecture Note Ser., vol. 352, Cambridge University Press, Cambridge, 89-120, 2008.

[9] S. Gao, J. Howell, D. Panario, *Irreducible Polynomials of Given Forms*, Contemp. Math **225**, 43-53, 1999.

[10] T. Garefalakis, *Irreducible Polynomials with Consecutive Zero Coefficients*, Finite Fields and Their Applications **14**, 201-208, 2008.

[11] T. Garefalakis, G. Kapetanakis, *On the Hansen-Mullen Conjecture for Self-reciprocal Irreducible Polynomials*, Finite Fields and Their Applications **18**, 832-841, 2012.

[12] T. Garefalakis, G. Kapetanakis, *A Note on the Hansen-Mullen Conjecture for Self-reciprocal Irreducible Polynomials*, Finite Fields and Their Applications **35**, 61-63, 2015.

[13] J. Ha, *Irreducible Polynomials with Several Prescribed Coefficients*, http://arxiv.org/abs/1601.06867.

[14] K. H. Ham, G. L. Mullen, *Distribution of Irreducible Polynomials of Small Degrees over Finite Fields*, Math. Comp. **67**, 337-341, 1998.

[15] W. B. Han, *Coefficients of Primitive Polynomials over Finite Fields*, Math. Comp. **65**, 331-340, 1996.

[16] R. Heyman, I. E. Shparlinski, *Counting Irreducible Binomials over Finite Fields*, Finite Fields and Their Applications **38**, 1-12, 2016.

[17] D. Jungnickel, S. A. Vanstone, *On Primitive Polynomials over Finite Fields*, J. Algebra **124**, 337-353, 1989.

[18] R. Kim, W. Koepf, *Divisibility of Trinomials by Irreducible Polynomials over* $\mathbb{F}_2$, International Journal of Algebra, Vol.3, No.4, 189-197, 2009.

[19] B. O. Koma, D. Panario, Q. Wang, *The Number of Irreducible Polynomials of Degree n over $\mathbb{F}_q$ with Given Trace And Constant Terms*, Discrete Mathematics **310**, 1282-1292, 2010.

[20] E. N. Kuz'min, *On A Class of Irreducible Polynomials over A Finite Field*, Doklady Akademii Nauk SSSR **313**, No.3, 552-555, 1990 (in Russian); English translation in Soviet Math. Dokl. **42**, No.1, 45-48, 1991.

[21] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[22] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone and T. Yaghoobian, *Applications of Finite Fields*, Kluwer, 1993.

[23] G. L. Mullen, D. Panario, *Handbook of Finite Fields*, CRC Press, 2013.

[24] D. Panario, G. Tzanakis, *A Generalization of the Hansen-Mullen Conjecture on Irreducible Polynomials over Finite Fields*, Finite Fields and Their Applications **18**, 303-315, 2012.

[25] L. Redei, *A Short Proof of A Theorem of St. Schwarz Concerning Finite Fields*, Casopis pro pestovani matematiky a fysiky, Vol.75, 211-212, 1950.

[26] I. E. Shparlinski, *Finite Fields: Theory and Computation*, Springer, 1999.

[27] St. Schwarz, *On the Reducibility of Binomial Congruences and on the Bound of the Least Integer Belonging to A Given Exponent mod p*, Casopis pro pestovani matematiky a fysiky, Vol.74, 1-16, 1949.

[28] A. Tuxanidy, Q. Wang, *A New Proof of the Hansen-Mullen Irreducibility Conjecture*, http://arxiv.org/abs/1604.04023v1.

[29] D. Wan, *Generators and Irreducible Polynomials over Finite Fields*, Math. Comp. **66**, 1195-1212, 1997.

[30] J. L. Yucas, *Irreducible Polynomials over Finite Fields with Prescribed Trace/Prescribed Constant Term*, Finite Fields and Their Applications **12**, 211-221, 2006.

[31] J. L. Yucas, G. L. Mullen, *Self-reciprocal Irreducible Polynomials over Finite Fields*, Des. Codes Cryptogr. **33**, 275-281, 2004.