Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Prescribing coefficients of invariant irreducible polynomials

Giorgos Kapetanakis

Faculty of Engineering and Natural Sciences, Sabancı Üniversitesi, Ortha Mahalle, Tuzla 34956, Istanbul, Turkey

ARTICLE INFO

Article history:
Received 28 March 2017
Received in revised form 24 May 2017
Accepted 25 May 2017
Available online xxxx
Communicated by D. Wan

MSC:
11T06
11T23

Keywords:
Hansen–Mullen conjecture
Finite fields
Character sums

ABSTRACT

Let $\mathbb{F}_q$ be the finite field of q elements. We define an action of $\mathrm{PGL}(2,q)$ on $\mathbb{F}_q[X]$ and study the distribution of the irreducible polynomials that remain invariant under this action for lower-triangular matrices. As a result, we describe the possible values of the coefficients of such polynomials and prove that, with a small finite number of possible exceptions, there exist polynomials of given degree with prescribed high-degree coefficients.

1. Introduction

Let q be a power of the prime number p. By $\mathbb{F}_q$ we denote the finite field of q elements. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,q)$ and $F \in \mathbb{F}_q[X]$. Following previous works [10,22,24], define

$$A \circ F = (bX+d)^{\deg(F)} F\left(\frac{aX+c}{bX+d}\right). \tag{1}$$

E-mail address: gnkapet@sabanciuniv.edu.

http://dx.doi.org/10.1016/j.jnt.2017.05.003

It is clear that the above defines an action of $\mathrm{GL}(2, q)$ on $\mathbb{F}_q[X]$.

Recall the usual equivalence relation in $\mathrm{GL}(2, q)$, namely for $A, B \in \mathrm{GL}(2, q)$,

$$A \sim B :\iff \exists\, C \in \mathrm{GL}(2, q) \text{ such that } A = C^{-1}BC.$$

Further, define the following equivalence relations for $A, B \in \mathrm{GL}(2, q)$ and $F, G \in \mathbb{F}_q[X]$.

$$A \sim_q B :\iff A = \lambda B, \text{ for some } \lambda \in \mathbb{F}_q^* \text{ and}$$
$$F \sim_q G :\iff F = \lambda G, \text{ for some } \lambda \in \mathbb{F}_q^*$$

It follows that, for $F \in \mathbb{F}_q[X]$ the equivalence class $[F] := \{G \in \mathbb{F}_q[X] \mid G \sim_q F\}$ consists of polynomials of the same degree with F that are all either irreducible or reducible and every such class contains exactly one monic polynomial. Further, the action defined in (1) also induces an action of $\mathrm{PGL}(2, q) = \mathrm{GL}(2, q)/ \sim_q$ on $\mathbb{F}_q[X]/ \sim_q$, see [24]. For $A \in \mathrm{GL}(2, q)$ and $n \in \mathbb{N}$, we define

$$\mathbb{I}_n^A := \{P \in \mathbb{I}_n \mid [A \circ P] = [P]\},$$

where $\mathbb{I}_n$ stands for the set of monic irreducible polynomials of degree n over $\mathbb{F}_q$. Recently, the estimation of the cardinality of $\mathbb{I}_n^A$ has gained attention [10,22,24]. In a similar manner, we introduce a natural notation abuse for $[A], [B] \in \mathrm{PGL}(2, q)$, i.e.

$$[A] \sim [B] :\iff \exists\, [C] \in \mathrm{PGL}(2, q) \text{ such that } [A] = [C^{-1}BC].$$

We note that throughout this paper, we will denote polynomials with capital Latin letters and their coefficients with their corresponding lowercase ones with appropriate indices. In particular, if $F \in \mathbb{F}_q[X]$ is of degree n, then $F(X) = \sum_{i=0}^{n} f_i X^i$, in other words, f_i will stand for the i-th coefficient of F. Two well-known results in the study of the distribution of polynomials over $\mathbb{F}_q$ are the following.

Theorem 1.1 *(Hansen–Mullen irreducibility conjecture). Let $a \in \mathbb{F}_q$, $n \geq 2$ and fix $0 \leq j < n$. There exists an irreducible polynomial $P(X) = X^n + \sum_{k=0}^{n-1} p_k X^k \in \mathbb{F}_q[X]$ with $p_j = a$, except when*

1. *$j = a = 0$ or*
2. *q is even, $n = 2$, $j = 1$, and $a = 0$.*

Theorem 1.2 *(Hansen–Mullen primitivity conjecture). Let $a \in \mathbb{F}_q$, $n \geq 2$ and fix $0 \leq j < n$. There exists a primitive polynomial $P(X) = X^n + \sum_{k=0}^{n-1} p_k X^k \in \mathbb{F}_q[X]$ with $p_j = a$, unless one of the following holds.*

1. *$j = 0$ and $(-1)^n a$ is non-primitive.*
2. *$n = 2$, $j = 1$ and $a = 0$.*
3. *$(q, n, j, a) = (4, 3, 2, 0), (4, 3, 1, 0)$ or $(2, 4, 2, 1)$.*