Journal of Number Theory 160 (2016) 536–565

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the number of N-free elements with prescribed trace ☆

Aleksandr Tuxanidy, Qiang Wang *

School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada

ARTICLE INFO

Article history:
Received 23 September 2014
Received in revised form 2 September 2015
Accepted 2 September 2015
Available online 2 November 2015
Communicated by D. Wan

MSC:
11T06
11T24

Keywords:
N-free
Character
Gaussian sum
Gaussian period
Semi-primitive
Primitive
Irreducible polynomial
Trace
Mersenne prime
Uniform
Prescribed coefficient
Finite fields

ABSTRACT

In this paper we derive a formula for the number of N-free elements over a finite field $\mathbb{F}_q$ with prescribed trace, in particular trace zero, in terms of Gaussian periods. As a consequence, we derive several explicit formulae in special cases. In addition we show that if all the prime factors of $q-1$ divide m, then the number of primitive elements in $\mathbb{F}_{q^m}$, with prescribed non-zero trace, is uniformly distributed. Finally we explore the related number, $P_{q,m,N}(c)$, of elements in $\mathbb{F}_{q^m}$ with multiplicative order N and having trace $c \in \mathbb{F}_q$.

☆ Research of the authors is partially supported by OGS and NSERC (RGPIN 312588-2012), respectively, of Canada.

* Corresponding author.
E-mail addresses: AleksandrTuxanidyTor@cmail.carleton.ca (A. Tuxanidy), wang@math.carleton.ca (Q. Wang).

http://dx.doi.org/10.1016/j.jnt.2015.09.008
0022-314X/

1. Introduction

Let q be the power of a prime number p and let $\mathbb{F}_q$ be a finite field with q elements. In 1992, Hansen and Mullen [10] conjectured that, except for very few exceptions, there exist irreducible and primitive polynomials of degree m over $\mathbb{F}_q$ with any prescribed coefficient respectively. This led to a great deal of work in the area, and both of these conjectures have since been resolved in the affirmative (see [18,9] for irreducible polynomials, as well as see the survey in [5] and [7] for primitives).

Particular interest has also been placed in deriving explicit formulas for the exact number of irreducible polynomials of degree m over $\mathbb{F}_q$ with one or more prescribed coefficients (see for example [3,11–13,19] and the survey [5] or Section 3.5 by S.D. Cohen in the Handbook of Finite Fields [16]). Here it is worth mentioning the following beautiful formula due to Carlitz [3] describing the number of monic irreducible polynomials of degree m with a prescribed trace coefficient (the coefficient of x^{m-1}). Let $I_{q,m}(c)$ denote the number of monic irreducible polynomials of degree m over $\mathbb{F}_q$ with trace c. Let μ be the Möbius function.

Theorem 1.1 *(Carlitz, 1952). Let q be a power of a prime p and let $m \in \mathbb{N}$. Then for any non-zero element $c \in \mathbb{F}_q \setminus \{0\}$, the number of monic irreducible polynomials of degree m over $\mathbb{F}_q$ and with trace c is given by*

$$I_{q,m}(c \neq 0) = \frac{1}{qm} \sum_{\substack{d|m \\ p\nmid d}} \mu(d) q^{m/d} = \frac{I_{q,m} - I_{q,m}(0)}{q-1},$$

where

$$I_{q,m} = \frac{1}{m} \sum_{d|m} \mu(d) q^{m/d}$$

is the number of irreducible polynomials of degree m over $\mathbb{F}_q$.

Note that

$$I_{q,m}(c) = \frac{I_{q,m} - I_{q,m}(0)}{q-1}, \tag{1}$$

is a constant for any $c \in \mathbb{F}_q^*$, and so $I_{q,m}(c)$ is said to be *uniformly distributed* for $c \in \mathbb{F}_q^*$. One of the results of this paper concerns an analogy to (1) for primitive polynomials in some special cases. We will return to this concept later.

A monic irreducible polynomial of degree m over $\mathbb{F}_q$ is called *primitive* if it has a primitive element of $\mathbb{F}_{q^m}$ as one of its roots. There is a correspondence between the primitive elements in $\mathbb{F}_{q^m}$ and the primitive polynomials of degree m over $\mathbb{F}_q$. In fact the number of primitive elements in $\mathbb{F}_{q^m}$ is m times the number of primitive polynomials of degree m over $\mathbb{F}_q$. Most of the work on primitive polynomials with prescribed coefficients focus