Finite Fields Appl. 38 (2016) 1–12

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Counting irreducible binomials over finite fields

Randell Heyman, Igor E. Shparlinski *

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

ARTICLE INFO

Article history:
Received 3 April 2015
Received in revised form 27 November 2015
Accepted 1 December 2015
Available online 21 December 2015
Communicated by D. Panario

MSC:
11T06

Keywords:
Irreducible binomials
Finite fields
Primes in arithmetic progressions

ABSTRACT

We consider various counting questions for irreducible binomials of the form $X^t - a$ over finite fields. We use various results from analytic number theory to investigate these questions.

1. Introduction

1.1. Background

It is reasonably easy to obtain an asymptotic formula for the total number of irreducible polynomials over the finite field $\mathbb{F}_q$ of q elements, see [10, Theorem 3.25].

* Corresponding author.
E-mail addresses: randell@unsw.edu.au (R. Heyman), igor.shparlinski@unsw.edu.au (I.E. Shparlinski).

http://dx.doi.org/10.1016/j.ffa.2015.12.001
1071-5797/

Studying irreducible polynomials with some prescribed coefficients is much more difficult, yet remarkable progress has also been achieved in this direction, see [4,8,14] and references therein.

Here we consider a special case of this problem and investigate some counting questions concerning irreducible binomials over the finite field $\mathbb{F}_q$ of q elements. More precisely, for an integer t and a prime power q, let $N_t(q)$ be the number of irreducible binomials over $\mathbb{F}_q$ of the form $X^t - a \in \mathbb{F}_q[X]$.

We use a well known characterisation of irreducible binomials $X^t - a$ over $\mathbb{F}_q$ of q elements to count the total number of such binomials on average over q or t. In fact, we consider several natural regimes, for example, when t is fixed and q varies or when both vary in certain ranges $t \le T$ and $q \le Q$. There has always been very active interest in binomials, see [10, Notes to Chapter 3] for a survey of classical results. Furthermore, irreducible binomials have been used in [15] as building blocks for constructing other irreducible polynomials over finite fields, and in [3] for characterising the irreducible factors of $x^n - 1$ (see also [1,11] and references therein for more recent applications). However, the natural question of investigating the behaviour of $N_t(q)$ has never been addressed in the literature.

Our methods rely on several classical and modern results of analytic number theory; in particular the distribution of primes in arithmetic progressions.

1.2. Notation

As usual, let $\omega(s)$, $\pi(s)$, $\varphi(s)$, $\Lambda(s)$ and $\zeta(s)$ denote the number of distinct prime factors of s, the number of prime numbers less than or equal to s, the Euler totient function, the von Mangoldt function and the Riemann-zeta function evaluated at s respectively.

For positive integers Q and s we denote the number of primes $p \le Q$ in the arithmetic progression $p \equiv a \pmod s$ by

$$\pi(Q; s, a) = \sum_{\substack{p \le Q \\ p \equiv a \pmod s}} 1.$$

We also denote

$$\psi(Q; s, a) = \sum_{\substack{p \le Q \\ p \equiv a \pmod s}} \Lambda(p).$$

The letter p always denotes a prime number whilst the letter q always denotes a prime power.

We recall that the notation $f(x) = O(g(x))$ or $f(x) \ll g(x)$ is equivalent to the assertion that there exists a constant $c > 0$ (which may depend on the real parameter