Finite Fields and Their Applications 50 (2018) 35–65

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

The arithmetic of consecutive polynomial sequences over finite fields

Domingo Gómez-Pérez [a], Alina Ostafe [b], Min Sha [b,*]

[a] *Department of Mathematics, Statistics and Computer Science, University of Cantabria, Santander 39005, Spain*
[b] *School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia*

A R T I C L E   I N F O

Article history:
Received 30 January 2017
Received in revised form 15 October 2017
Accepted 6 November 2017
Available online xxxx
Communicated by D. Panario

MSC:
primary 11T06, 11B50
secondary 11T24

Keywords:
Consecutive polynomial sequence
Consecutive irreducible sequence
Character sum

A B S T R A C T

Motivated by a question of van der Poorten about the existence of an infinite chain of prime numbers (with respect to some base), in this paper we advance the study of sequences of consecutive polynomials whose coefficients are chosen consecutively from a sequence in a finite field of odd prime characteristic. We study the arithmetic of such sequences, including bounds for the largest degree of irreducible factors, the number of irreducible factors, as well as for the number of such sequences of fixed length in which all the polynomials are irreducible.

* Corresponding author.
E-mail addresses: domingo.gomez@unican.es (D. Gómez-Pérez), alina.ostafe@unsw.edu.au (A. Ostafe), shamin2010@gmail.com (M. Sha).

https://doi.org/10.1016/j.ffa.2017.11.002

1. Introduction

1.1. Motivation

In [23], van der Poorten observed that the numbers

$$19, 197, 1979, 19793, 197933, 1979339, 19793393, 197933933, 1979339339$$

are all prime numbers and raised a question that whether there is such an infinite chain of prime numbers (with respect to some base b). One related question is whether there exists the largest truncatable prime in a given base b (such a prime can yield a sequence of primes when digits are removed away from the right). Note that the above integer 1979339339 is not a truncatable prime. The authors in [1] have given heuristic arguments for the length of the largest truncatable prime in base b (roughly, the length is $be/\log b$, where e is the base of the natural logarithm) and computed the largest truncatable primes in base b for $3 \leqslant b \leqslant 15$. Both questions might be very hard.

Mullen and Shparlinski [21, Problem 31] asked an analogous question about polynomials over finite fields. More precisely, let p be an odd prime number and $q = p^s$ for some positive integer s. We denote by $\mathbb{F}_q$ the finite field of q elements, and use $\mathbb{F}_q[X]$ to denote the ring of polynomials with coefficients in $\mathbb{F}_q$.

For a (finite or infinite) sequence $\{u_n\}_{n\geqslant 0}$, of non-zero elements in $\mathbb{F}_q$, we define a *consecutive polynomial sequence* $\{f_n\}_{n\geqslant 1}$, associated to the sequence $\{u_n\}$, in $\mathbb{F}_q[X]$ as follows:

$$f_n = u_n X^n + \ldots + u_1 X + u_0, \; n \geqslant 1. \tag{1.1}$$

If all the polynomials f_n, $n \geqslant 1$, are irreducible, then the sequence $\{f_n\}$ is called a *consecutive irreducible polynomial sequence*, and $\{u_n\}$ is called a *consecutive irreducible sequence*.

Given a sequence $\{u_n\}$, let $L(\{u_n\})$ be either ∞ if $\{u_n\}$ is infinite, or a non-negative integer such that $L(\{u_n\}) + 1$ is the length of $\{u_n\}$. That is, $L(\{u_n\})$ is the length of the associated polynomial sequence $\{f_n\}$.

Mullen and Shparlinski [21, Problem 31] asked for lower and upper bounds for the maximum length $L(q) = \max\{L(\{u_n\})\}$ (possibly infinite), where $\{u_n\}$ runs through all consecutive irreducible sequences over $\mathbb{F}_q$. The only known result is a lower bound due to Chow and Cohen [4, Theorem 1.2],

$$L(q) > \frac{\log q}{2 \log\log q}, \tag{1.2}$$

whenever $q \neq 3$; they also observed that for $q = 3$, $L(3) = 3$.

The work on irreducible polynomials with prescribed coefficients might reflect that such an upper bound of $L(q)$ indeed exists. Twenty years ago, Hansen and Mullen [13,