Journal of Number Theory 152 (2015) 21–37

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Sequences of irreducible polynomials over odd prime fields via elliptic curve endomorphisms

S. Ugolini

Dipartimento di Matematica, Università degli studi di Trento, Via Sommarive 14, I-38050 Povo (Trento), Italy

ARTICLE INFO

Article history:
Received 25 May 2014
Received in revised form 9 September 2014
Accepted 18 December 2014
Available online 7 February 2015
Communicated by David Goss

Keywords:
Irreducible polynomial iterative constructions
Finite fields
Elliptic curves

ABSTRACT

Text. In this paper we present and analyze a construction of irreducible polynomials over odd prime fields via the transforms which take any polynomial $f \in \mathbf{F}_p[x]$ of positive degree n to $\left(\frac{x}{k}\right)^n \cdot f\left(k(x+x^{-1})\right)$, for some specific values of the odd prime p and $k \in \mathbf{F}_p$.

Video. For a video summary of this paper, please visit http://youtu.be/Lmw5m_c-i8s.

1. Introduction

Let f be a polynomial of positive degree n defined over the field $\mathbf{F}_p$ with p elements, for some odd prime p. We set $q = p^n$ and denote by $\mathbf{F}_q$ the finite field with q elements.

For a chosen $k \in \mathbf{F}_p^*$ we define the Q_k-transform of f as

$$f^{Q_k}(x) = \left(\frac{x}{k}\right)^n \cdot f\left(\vartheta_k(x)\right),$$

E-mail address: sugolini@gmail.com.

http://dx.doi.org/10.1016/j.jnt.2014.12.027

where ϑ_k is the map which takes any element $x \in \mathbf{P}^1(\mathbf{F}_q) = \mathbf{F}_q \cup \{\infty\}$ to

$$\vartheta_k(x) = \begin{cases} \infty & \text{if } x = 0 \text{ or } \infty, \\ k \cdot (x + x^{-1}) & \text{otherwise.} \end{cases}$$

The aforementioned Q_k-transforms seem a natural generalization of some specific transforms employed by different authors for the synthesis of irreducible polynomials over finite fields. In [3] Meyn used the so-called Q-transform, which coincides with the Q_1-transform according to the notations of the present paper. Moreover, setting $k = \frac{1}{2}$ we recover the R-transform introduced by Cohen [1] and used more recently by us [5] to construct sequences of irreducible polynomials over odd prime fields.

In this paper we would like to take advantage of the knowledge of the dynamics of the maps ϑ_k for some specific values of k [4] and extend our investigation [5]. In the following we will give a thorough description of the sequences of irreducible polynomials constructed by repeated applications of a Q_k-transform, when k belongs to one of the following sets:

- $C_1 = \left\{\frac{1}{2}, -\frac{1}{2}\right\}$;
- $C_2 = \left\{k \in \mathbf{F}_p : k \text{ is a root of } x^2 + \frac{1}{4}\right\}$, provided that $p \equiv 1 \pmod 4$;
- $C_3 = \left\{k \in \mathbf{F}_p : k \text{ is a root of } x^2 + \frac{1}{2}x + \frac{1}{2}\right\}$, provided that $p \equiv 1, 2$, or $4 \pmod 7$;
- $C_3^- = \left\{k \in \mathbf{F}_p : -k \text{ is a root of } x^2 + \frac{1}{2}x + \frac{1}{2}\right\}$, provided that $p \equiv 1, 2$, or $4 \pmod 7$.

Indeed, the case $k = \frac{1}{2}$ has been analyzed in [5] and we can easily adapt the results of that paper to the case $k = -\frac{1}{2}$ (see the subsequent Remark 2.2). Hence, in this paper we will mainly concentrate on the cases that $k \in C_2 \cup C_3 \cup C_3^-$.

2. Preliminaries

Let p be an odd prime and q a power of p. For a fixed $k \in \mathbf{F}_p^*$, the dynamics of the map ϑ_k over $\mathbf{P}^1(\mathbf{F}_q)$ can be visualized by means of the graph $G^q_{\vartheta_k}$, whose vertices are labeled by the elements of $\mathbf{P}^1(\mathbf{F}_q)$ and where a vertex α is joined to a vertex β if $\beta = \vartheta_k(\alpha)$. As in [4] we say that an element $x \in \mathbf{P}^1(\mathbf{F}_q)$ is ϑ_k-periodic if $\vartheta_k^r(x) = x$ for some positive integer r. We will call the smallest of such integers r the period of x with respect to the map ϑ_k. Nonetheless, if an element $x \in \mathbf{P}^1(\mathbf{F}_q)$ is not ϑ_k-periodic, then it is preperiodic, namely $\vartheta_k^l(x)$ is ϑ_k-periodic for some positive integer l.

In [4] the reader can find more details about the length and the number of the cycles of $G^q_{\vartheta_k}$, when $k \in C_1 \cup C_2 \cup C_3$. For the purposes of the present paper we are just interested in the structure of the reversed binary trees attached to the vertices of a cycle.

The following lemma shows how the maps ϑ_k and ϑ_{-k} are related, for any $k \in \mathbf{F}_p^*$.

Lemma 2.1. *Let $k \in \mathbf{F}_p^*$ and $x \in \mathbf{P}^1(\mathbf{F}_q)$. The following hold:*

(1) $\vartheta_k^{2r}(x) = \vartheta_{-k}^{2r}(x)$ *for any nonnegative integer r;*