Finite Fields and Their Applications 48 (2017) 420–429

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the irreducibility of Fibonacci and Lucas polynomials over finite fields

Hidetaka Kitayama [a,1], Daisuke Shiomi [b,*]

[a] Department of Mathematics, Faculty of Education, Wakayama University, Wakayama, Japan
[b] Department of Mathematical Sciences, Faculty of Science, Yamagata University, Yamagata, Japan

ARTICLE INFO

Article history:
Received 16 October 2016
Received in revised form 31 August 2017
Accepted 2 September 2017
Available online 15 September 2017
Communicated by D. Panario

MSC:
primary 11B39, 11T55

Keywords:
Fibonacci polynomials
Lucas polynomials
Polynomial rings over finite fields

ABSTRACT

In this paper, we give the necessary and sufficient condition that Fibonacci and Lucas polynomials are irreducible in $\mathbb{F}_q[T]$. As applications of our results, under the GRH, we prove that there are infinitely many irreducible Fibonacci and Lucas polynomials in $\mathbb{F}_q[T]$ for some q.
© 2017 Elsevier Inc. All rights reserved.

1. Introduction

Fibonacci numbers F_n and Lucas numbers L_n are defined recursively by

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \quad (n \geq 2),$$

* Corresponding author.
E-mail addresses: hkitayam@center.wakayama-u.ac.jp (H. Kitayama), shiomi@sci.kj.yamagata-u.ac.jp (D. Shiomi).
[1] The first author is supported by JSPS KAKENHI Grant Numbers JP15K17511, JP25247001.

http://dx.doi.org/10.1016/j.ffa.2017.09.003
1071-5797/© 2017 Elsevier Inc. All rights reserved.

$$L_0 = 2,\ L_1 = 1,\ L_n = L_{n-1} + L_{n-2} \quad (n \geq 2).$$

If F_n (resp. L_n) is a prime, then F_n (resp. L_n) is called a Fibonacci prime (resp. a Lucas prime). Many Fibonacci and Lucas primes have been found by several researchers (see [2], [4]), but it is unknown whether there are infinitely many Fibonacci and Lucas primes.

As an analogue of this problem, several authors have studied the irreducibility of Fibonacci polynomials $F_n(T)$ and Lucas polynomials $L_n(T)$, which are defined recursively by

$$F_0(T) = 0,\ F_1(T) = 1,\ \ F_n(T) = TF_{n-1}(T) + F_{n-2}(T) \quad (n \geq 2),$$
$$L_0(T) = 2,\ L_1(T) = T,\ L_n(T) = TL_{n-1}(T) + L_{n-2}(T) \quad (n \geq 2).$$

Notice that $F_n(1) = F_n$ and $L_n(1) = L_n$. Webb and Parberry [9] showed that $F_n(T)$ is irreducible over $\mathbb{Q}$ if and only if n is a prime. Bergum and Hoggatt [1] showed that $L_n(T)$ is irreducible over $\mathbb{Q}$ if and only if $n = 2^m (m \geq 0)$, and $L_n(T)/T$ (n odd) is irreducible over $\mathbb{Q}$ if and only if n is a prime.

In this paper, we consider the irreducibility of Fibonacci and Lucas polynomials in $\mathbb{F}_q[T]$, where $\mathbb{F}_q$ is the finite field with q elements. By using algebraic number theory, we give the necessary and sufficient condition that $F_n(T)$, $L_n(T)$ and $L_n(T)/T$ (n odd) are irreducible in $\mathbb{F}_q[T]$ (see Theorems 3.1–3.3, 3.5–3.8). As applications of these results, under the GRH, we show that there are infinitely many irreducible Fibonacci and Lucas polynomials in $\mathbb{F}_q[T]$ for some q.

2. Preparation

We review some properties of Fibonacci and Lucas polynomials over $\mathbb{Q}$. For details, see [5] and references therein.

Proposition 2.1. *For $n \geq 2$, we have*

$$F_n(T) = \prod_{k=1}^{n-1} \left(T - 2i \cos\left(\frac{k\pi}{n}\right)\right).$$

Proof. See [5, p. 478]. □

Define $F_n^*(T)$ by

$$F_n^*(T) = \begin{cases} 1 & \text{if } n = 1, \\ \displaystyle\prod_{\substack{k=1 \\ (k,n)=1}}^{n-1} \left(T - 2i \cos\left(\frac{k\pi}{n}\right)\right) & \text{if } n \geq 2. \end{cases}$$

Download English Version:

https://daneshyari.com/en/article/5771572

Download Persian Version:

https://daneshyari.com/article/5771572

Daneshyari.com