Chapter 2
Power Pell Sequences, Some Periodic Relations of These Sequences, and a Cryptographic Application With Power Pell Sequences

Çağla Çelemoğlu
Ondokuz Mayis University, Turkey

Selime Beyza Özçevik
Ondokuz Mayıs University, Turkey

Şenol Eren
Ondokuz Mayıs University, Turkey

ABSTRACT

Here, first of all, the authors investigated power Fibonacci sequence modulo k and formulas for the periods of these sequences, based on the period of the Fibonacci sequence modulo k. And then, the authors described a new power sequence for positive integer modulus. They named these sequences power Pell sequences modulo k. After that the authors determined those positive integer moduli for which this sequence exists and the number of such sequences for a given modulo k. In addition, the authors provide formulas for the periods of these sequences, based on the period of the Pell sequence modulo k, and they studied sequence/subsequence relationships between power Pell sequences. Finally, the authors examined ElGamal cryptosystem which is one of the asymmetric cryptographic systems and ElGamal cryptosystem which is obtained by using some power sequences. And they obtained asymmetric cryptographic applications by using power Pell sequences which the authors described.

DOI: 10.4018/978-1-7998-9012-6.ch002

INTRODUCTION

The Fibonacci sequence, $\{F_n\}_0^\infty$, is a sequence of numbers, beginning with the integer couple 0 and 1, in which the value of any element is computed by taking the summation of the two antecedent numbers. If so, for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$ (Koshy, 2001). The first eight terms of this sequence are $1,1,2,3,5,8,13,21$.

There have been many studies in the literature dealing with the Fibonacci sequences. Some authors obtained generalization of the Fibonacci sequence by changing only the first two terms of the sequence or with minor changes only the recurrence relation, while others obtained generalizations of the Fibonacci sequence by changing both of them. In addition, the Fibonacci sequence $F = 0,1,1,2,3,5,8,\ldots$ has come to the fore for centuries, as it seems there is no end to its many surprising properties. It is seen that the popular number sequence has been found to have important properties when the sequence reduced under a modulus. It is well known, the Fibonacci sequence and the other sequences which is obtained by changing the recurrence relation or the first two terms of Fibonacci sequence under a modulus is periodic. $\pi\left(k\right)$ denote the period of the Fibonacci sequence modulo k, formulas are known for computing $\pi\left(k\right)$ based on the prime factorization of k. But if k is prime number, there is no formula for $\pi\left(k\right)$. On the other hand, some equations are provided. For example, if k is prime number and if $k \equiv \pm 1\left(\bmod 10\right)$, $\pi\left(k\right) \mid k-1$ and if $k \equiv \pm 3\left(\bmod 10\right)$, $\pi\left(k\right) \mid 2\left(k+1\right)$ (Renault, 2013).

In this study, the authors used Pell sequence which is obtained by changing only the recurrence relation of Fibonacci sequence, power Fibonacci sequence modulo k, the relationship of periods of these sequences as material. These structures the authors used in this article are introduced as follows:

Definition 1. The Pell sequence (P_n) is defined recursively by the equation $P_n = 2P_{n-1} + P_{n-2}$ for $n \geq 1$, where $P_0 = 0$ and $P_1 = 1$ (Koshy, 2001).

Definition 2. Let G be a bi-infinite integer sequence providing the recurrence relation $G_n = G_{n-1} + G_{n-2}$. Providing $G \equiv 1,\alpha,\alpha^2,\alpha^3,\ldots\left(\bmod k\right)$ for some modulus k, then G is named a power Fibonacci sequence modulo k (Ide and Renault, 2012).

Example 1. For modulo $k = 29$, the two power Fibonacci sequences are following:

1, 6, 7, 13, 20, 4, 24, 28, 23, 22, 16, 9, 25, 5, 1, 6, 7, … and 1, 24, 25, 20, 16, 7, 23, 1, 24, ...

Connectionist Systems and Signal Processing Techniques Applied to the Parameterization of Stellar Spectra

Diego Ordóñez, Carlos Dafonte, Bernardino Arcayand Minia Manteiga (2010). *Soft Computing Methods for Practical Environment Solutions: Techniques and Studies (pp. 187-203).*

www.irma-international.org/chapter/connectionist-systems-signal-processing-techniques/43152