Linear Recurrence Relations and Cryptography

Mohamad Rushdan Md Said

Abstract

The Fibonacci numbers are one of the most well-known recurrence sequences, predate Leonardo Fibonacci's 1202 discovery by more than a millennium, having arisen around 200 BC. In the late 1800s and early 1900s, investigations into the foundations of mathematics led to the formal definition of so-called recursive functions. Linear recurrence sequences permeate a vast number of areas of mathematics and computer science. They have been studied extensively since the time of Lucas. With the advent of modern cryptography, modern theory of linear recurrence sequences and their generalizations found their way towards some real applications. We will begin with a discussion of polynomials and their properties and use the ideas to investigate the corresponding linear recurrence sequences. One sequence that is of interest and which figures prominently in many parts of number theory is the Lucas sequence and we will consider this sequence and its extensions in detail. This work is divided into two related topics, covering firstly linear recurrence relations and then its application to public-key cryptosystems. In the first part, we will discuss the general recurrence relations and then generalize the Euler totient function to the Lehmer totient function for second order linear recurrence relations and then to numbers in third order recurrence sequences. The totient function and the generalization of the rule for composition of powers as in the RSA cryptosystems form the crucial ingredients that make it possible to construct higher order cryptosystems analogous to the RSA systems. The second part of the work is the application of linear recurrence relations to other aspects of public-key cryptography.