THE LUCAS PROPERTY FOR LINEAR RECURRENCES OF SECOND ORDER

Carsten Elsner and Jürgen Spilker

Elemente der Mathematik 73 (2018), 151 - 160

Every exponential function $f(n) = k^n$ with a fixed integer k has the so-called Lucas property modulo a prime number p, which is expressed by the congruence

$$f(n) \equiv \prod_{0 \le i \le r} f(n_i) \pmod{p}.$$

Here the integers n_i are the coefficients of the p-adic representation of n. E. Lucas and later authors applied this concept to binomial coefficients. Recently, H. Zhong and T. Cai proved a necessary and sufficient condition for the Lucas property modulo p involving the sequences $F(an+b)$, where $F(n)$ is the Fibonacci sequence and a, b are two fixed positive integers. In this note two necessary and sufficient conditions for the Lucas property modulo p are proven, which are applicable to all functions $f(n) = g(an+b)$, when $g(n)$ satisfies a linear recurrence formula of order two. This generalizes the result of H. Zhong and T. Cai. We extend our result to Carmichael numbers p. An application to the difference of exponential functions is presented.

2010 MS Classification numbers: 11A07, 11B37, 11B50
Key Words: Lucas property, linear recurrences