zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Elsner, Carsten; Spilker, Jürgen

The Lucas property for linear recurrences of second order. (English) Zbl 1439.11010

Elem. Math. 73, No. 4, 151-160 (2018).

Summary: Die Lucas-Eigenschaft modulo einer Primzahl p stellt eine Verbindung her zwischen allen Funktionswerten $f(n)$ einer Funktion $f:\mathbb{N}\to\mathbb{N}$ und dem Produkt $f(n_0)f(n_1)\cdots f(n_r)$, wobei die $n_0,\dots,n_r$ die Ziffern der p-adischen Entwicklung von n sind, nämlich

$$f(n)\equiv f(n_0)f(n_1)\cdots f(n_r)\pmod p\quad (n\geq 1).$$

Diese Eigenschaft kommt jeder Exponentialfunktion $f(n)=c^n$ mit$c\in\mathbb{N}$ und jeder Primzahl p zu. Erstmalig wurde eine solche Beziehung 1878 von E. Lucas für Binomi-alkoeffizienten aufgestellt. In der vorliegenden Arbeit werden Funktionen g betrachtet, die einer linearen Rekursion zweiter Ordnung mit konstanten Koeffizienten genügen. Sollte eine solche Funktion g die Lucas-Eigenschaft modulo p noch nicht haben, sofolgen die Autoren einer in der Zahlentheorie gängigen Vorgehensweise, indem sie die auf arithmetischen Progressionen beruhenden Teilfolgen $f(n):=g(an+b)$ betrachten und charakterisieren, wann f wieder die Lucas-Eigenschaft modulo p hat. Dies haben in einer kürzlich erschienenen Arbeit bereits *H. Zhong* and *T. Cai* [Int. J. Number Theory 13, No. 6, 1617–1625 (2017; Zbl 1428.11036)] für die Fibonacci-Funktion $F(n)$ getan. So hat etwa $f(n)=F(4n+7)$ die Lucas-Eigenschaft modulo 3. In dieser Arbeit wird gleichzeitig das Konzept der Lucas-Eigenschaft von den Primzahlen auf die Carmichael-Zahlen erweitert, die ja bekanntlich eine bedeutende Rollein der Kryptographie spielen.

MSC:

11A07	Congruences; primitive roots; residue systems
11A25	Arithmetic functions; related numbers; inversion formulas
11B37	Recurrences

Keywords:

Lucas property

Software:

ARIBAS

Full Text: DOI

References:

[1] W. Alford, A. Granville, and C. Pomerance, There are Infinitely Many Carmichael Numbers, Ann. Math. 139 (1994), 703-722. · Zbl 0816.11005

[2] D.F. Bailey, More binomial coefficient congruences, Trinity University, San Antonio, TX 78212, 1992, 121- 125. · Zbl 0758.11001

[3] O. Forster, Algorithmische Zahlentheorie, Vieweg (1996), ISBN: 3-528-06580-X

[4] V.E. Hogatt, Fibonacci and Lucas Numbers, Houghton Mifflin (1969).

[5] E. Lucas, Sur les congruences des nombres eul´eriens et des coefficients diff´erentiels des fonctions trigonom´etriques, suivant un module premier, Bull. Soc. Math. France 6 (1878), 49-54.

[6] R. McIntosh, A generalization of a congruential property of Lucas, Amer. Math. Monthly 99, no. 3 (1992), 231-238. · Zbl 0755.11001

[7] H. Zhong and T. Cai, On the Lucas property of linear recurrent sequences, J. Number Theory 13, no. 6 (2017), 1617-1625. · Zbl 1428.11036