Zubkov, A. M.; **Tarakanov, V. E.**

Cycle structure of power mappings in a residue class ring. (English. Russian original)

Zbl 1398.94089

Discrete Math. Appl. 23, No. 3-4, 273-298 (2013); translation from Diskretn. Mat. 25, No. 2, 39-62 (2013).

From the introduction: In this paper we describe constructively the structure of the set of cycles for mappings $x \mapsto x^d \pmod N$ with arbitrary vaues of d and N. in §§1–2 the combinatorially-algebraic approach to the description of these cycle structures is suggested. It allows to reduce a problem to the two following ones:

a) the description of cycle structures of power mappings of arbitrary primary cyclic groups and

b) the description of cycle structure power mapping on the direct product of cyclic groups via cycle structure of factors.

The cyclic structures of the mapping $f^{(d)}\colon x \to x^d$ for the primary cyclic groups of an odd order are described in §3, and, fopr groups of an even order in §4. At last, in §5 using the composition operation of cycle structures introduced in §2 and the results of §§3–4, we describe the cycle structures for mappings $f^{(d)}$ on the sets $\mathbb{Z}_N^*$ of invertible elements of a ring $\mathbb{Z}_N$ of residue classes modulo N for any d, $N \geq 2$.

MSC:

94A55 Shift register sequences and sequences over finite alphabets in information and communication theory

11T71 Algebraic coding theory; cryptography (number-theoretic aspects)

05A15 Exact enumeration problems, generating functions

Full Text: DOI