

On the solution of $J_\alpha^x = J_\beta^y$ and reduced linear modular systems

Edusmildo Orozco, University of Puerto Rico at Rio Piedras

A reduced linear modular system (RLMS) is a finite dynamical system over a finite field and, in previous works, it has been shown that the structure of the associated functional graph resembles the cyclic structure of a linear modular system. Let J_α be a Jordan block over a finite field. We consider the equation $J_\alpha^x = J_\beta^y$ in the unknowns x and y and discuss solutions when $\alpha\beta^{-1}$ is an integer and its connection with Lucas' theorem and the Chinese remainder theorem. This problem is related to the structure of certain RLMSs which in turn play an important role in the efficient computation of symmetric prime edge-length multidimensional fast Fourier transforms.

Keywords: reduced linear modular system, finite field, symmetric prime edge-length FFT