Year: 2021 **Vol.: 99** **Fasc.: 3-4**

Title: Four-generated direct powers of partition lattices and authentication

Author(s): Gábor Czédli

For an integer $n \geq 5$, H. Strietz (1975) and L. Zádori (1986) proved that the lattice $\mathrm{Part}(n)$ of all partitions of $\{1, 2, \dots, n\}$ is four-generated. Developing L. Zádori's particularly elegant construction further, we prove that even the k-th direct power $\mathrm{Part}(n)^k$ of $\mathrm{Part}(n)$ is four-generated for many but only finitely many exponents k. E.g., $\mathrm{Part}(100)^k$ is four-generated for every $k \leq 3 \cdot 10^{89}$, and it has a four-element generating set that is not an antichain for every $k \leq 1.4 \cdot 10^{34}$. In connection with these results, we outline a protocol how to use these lattices in authentication and secret key cryptography.

Address:
Gábor Czédli
Bolyai Institute
University of Szeged
Aradi vértanúk tere 1
H-6720 Szeged
Hungary