

## Four-generated direct powers of partition lattices and authentication

By GÁBOR CZÉDLI (Szeged)

**Abstract.** For an integer  $n \geq 5$ , H. Strietz (1975) and L. Zádori (1986) proved that the lattice  $\text{Part } n$  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  $\text{Part } n^k$  of  $\text{Part } n$  is four-generated for many but only finitely many exponents  $k$ . E.g.,  $\text{Part } 100^k$  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.

GÁBOR CZÉDLI  
BOLYAI INSTITUTE  
UNIVERSITY OF SZEGED  
ARADI VÉRTANÚK TERE 1  
H-6720 SZEGED  
HUNGARY

---

*Mathematics Subject Classification:* 06C10.

*Key words and phrases:* partition lattice, equivalence lattice, four-generated lattice, Stirling number of the second kind, Bell number, secret key, authentication scheme, cryptography, crypto-system, commitment, semimodular lattice.