ICM 1998, Berlin, Aug. 18–27

Abstracts of Short Communications and Posters

Section:

13. Combinatorics

1991 MS Classification: 5, 20, 94

Keedwell, Anthony Donald, University of Surrey, England

Crossed-inverse quasigroups and their use in cryptography.

A *finite quasigroup* $(Q,_0)$ of order n consists of a set Q of symbols on which a binary operation $(_0)$ is defned such that (i) for all pairs of elements $a, b \in Q, a_0b \in Q$; and (ii) for all pairs $a, b \in Q$, there exists unique elements $x, y \in Q$ such that $x_0b = b$ and $a_0y = b$. If, for each $a \in Q$, there ecists an element $a' \in Q$ such that $(a_0b)_0a' = b$ for all $b \in Q$, the quasigroup is said to have the *right crossed-inverse property.* Such a quasigroup also has the left crossed-inverse property and is called a *crossed-inverse quasigroup.*
We show how crossed-inverse quasigroup with long inverse cycles may be constructed and suggest several applications to cryptography.

Reference: R. Artzy, On loops with a special property, Proc. Amer. Math. Soc. 6(1955), 448 - 452.