Additive Combinatorics
March 30 – April 12, 2006

Growth and generation in $\mathrm{SL}_2(Z/pZ)$

Harald Helfgott
helfgott@dms.umontreal.ca
Département de mathématiques et de statistique
Université de Montréal
C.P. 6128, Succ. Centre-ville
Montréal, Québec H3C 3J7
CANADA

Abstract

We show that every subset of $\mathrm{SL}_2(Z/pZ)$ grows rapidly when it acts on itself by the group operation. It follows readily that, for every set of generators A of $\mathrm{SL}_2(Z/pZ)$, every element of $\mathrm{SL}_2(Z/pZ)$ can be expressed as a product of at most $O\big((\log p)^c\big)$ elements of the union of A and A^{-1}, where c and the implied constant are absolute.