Algebra 5.45

Michael Vaughan-Lee

June 2013

Algebra 5.45 has p immediate descendants of order p^6. These p descendants are given by a two parameter family of Lie rings, named 6.427.

The two parameters are x, y, and the pair (x, y) gives the same algebra as (z, t) if and only if $y^2 - \omega x^2 = t^2 - \omega z^2 \bmod p$. (Here, as elsewhere, ω is a primitive element modulo p.) We get the $\frac{p+1}{2}$ distinct squares modulo p with parameters $(x, 0)$ with $0 \leq x \leq \frac{p-1}{2}$. To obtain the non-squares, find a such that $a^2 - \omega$ is not a square modulo p, and take parameters (ay, y) for $0 < y \leq \frac{p-1}{2}$. In the case $p = 1 \bmod 4$, $a = 0$ will do. I don't think the search for a is linear in p for $p = 3 \bmod 4$, but since $a^2 - \omega$ is not a square modulo p for half of the possible values of a, you would have to be unlucky not to find a suitable a quickly.