Algebra 6.427

Michael Vaughan-Lee

June 2013

Algebra 6.427 is a family of p algebras of order p^6 which are immediate descendants of algebra 5.45. This family has $p+1$ descendants of order p^7 given by a two parameter family with parameters x, y, with the isomorphism type depending on the value of $y^2 - \omega x^2$ (Here, as elsewhere, ω is a primitive element modulo p.)

This is essentially the same as in the descendants of 5.45. First we need representative pairs (x, y) giving the $(p-1)$ *non-zero* values of $y^2 - \omega x^2$. We get the $\frac{p-1}{2}$ distinct non-zero squares modulo p with parameters $(x, 0)$ with $0 < x \leq \frac{p-1}{2}$. 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. We also need to find a single pair (x, y) with $y^2 - \omega x^2 = \omega$, and we can find such a pair by evaluating $y^2 - \omega(ay)^2$ for $0 < y \leq \frac{p-1}{2}$.