Algebra 6.62

Michael Vaughan-Lee

June 2013

Algebra 6.62 has two parameters x, y, where x, y are integers with $y \neq 0 \bmod p$. Parameter pairs (x, y) and (z, t) give isomorphic algebras if and only if

$$\begin{pmatrix} 1 & 0 \\ z & t \end{pmatrix} = \begin{pmatrix} \mu & \nu \\ \omega\nu & \mu \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x & y \end{pmatrix} \begin{pmatrix} \mu + \nu x & \nu y \\ \omega\nu y & \mu + \nu x \end{pmatrix}^{-1} \bmod p$$

for some matrix $\begin{pmatrix} \mu & \nu \\ \omega\nu & \mu \end{pmatrix}$ with determinant coprime to p. (Here, as elsewhere, ω is a primitive element modulo p.) So we need to compute representatives for the orbits of non-singular matrices $\begin{pmatrix} 1 & 0 \\ x & y \end{pmatrix} \in \mathrm{GL}(2, p)$ under the action of the group of non-singular matrices $\begin{pmatrix} \mu & \nu \\ \omega\nu & \mu \end{pmatrix} \in \mathrm{GL}(2, p)$ given above. There are p orbits.

It is easy enough to generate the p orbit representatives with a simple loop over all non-singular matrices $\begin{pmatrix} \mu & \nu \\ \omega\nu & \mu \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ x & y \end{pmatrix}$. However this method has complexity p^4 for output of size p, which is not very satisfactory! Can we do better? Multiplying $\begin{pmatrix} \mu & \nu \\ \omega\nu & \mu \end{pmatrix}$ through by a non-zero constant has no effect on the action, so we can assume that $\mu = 0, 1$, and that if $\mu = 0$ then $\nu = 1$. This reduces the complexity to p^3.