Algebra 6.178

Michael Vaughan-Lee

June 2013

Algebra 6.178 has four paramaters x, y, z, t taking all integer values, subject to $A = \begin{pmatrix} t & x \\ y & z \end{pmatrix}$ being non-singular modulo p. Two such parameter matrices A and B define isomorphic algebras if and only if

$$B = \frac{1}{\det P} PAP^{-1} \bmod p$$

for some matrix P of the form

$$\begin{pmatrix} \alpha & \beta \\ \omega\beta & \alpha \end{pmatrix} \text{ or } \begin{pmatrix} \alpha & \beta \\ -\omega\beta & -\alpha \end{pmatrix} \tag{1}$$

which is non-singular modulo p. (Here, as elsewhere, ω is a primitive element modulo p.) So we need to compute the orbits of $\mathrm{GL}(2, p)$ under the action of the subroup of $\mathrm{GL}(2, p)$ consisting of matrices of the form (1). The set of all matrices P of this form is a group G of order $2(p^2-1)$. The number of orbits is $p^2+(p+1)/2-\gcd(p-1, 4)/2$.

We show that every orbit contains a matrix $\begin{pmatrix} 0 & x \\ y & z \end{pmatrix}$ or $\begin{pmatrix} 1 & x \\ y & z \end{pmatrix}$.

Let $A = \begin{pmatrix} t & x \\ y & z \end{pmatrix}$.

If $P = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$ then $\frac{1}{\det P} PAP^{-1} = \begin{pmatrix} \frac{t}{\alpha^2} & \frac{x}{\alpha^2} \\ \frac{y}{\alpha^2} & \frac{z}{\alpha^2} \end{pmatrix}$. This implies that we can take $t = 0$ or 1 provided t is a square.

If $P = \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix}$ then $\frac{1}{\det P} PAP^{-1} = \begin{pmatrix} -\frac{t}{\alpha^2} & \frac{x}{\alpha^2} \\ \frac{y}{\alpha^2} & -\frac{z}{\alpha^2} \end{pmatrix}$, which means that you can take $t = 0$ or 1 unless -1 is a square, i.e. unless $p = 1 \bmod 4$.

If $P = \begin{pmatrix} 0 & \beta \\ \omega\beta & 0 \end{pmatrix}$ then $\frac{1}{\det P} PAP^{-1} = \begin{pmatrix} -\frac{z}{\beta^2\omega} & -\frac{y}{\beta^2\omega^2} \\ -\frac{x}{\beta^2} & -\frac{t}{\beta^2\omega} \end{pmatrix}$, so in the case $p = 1 \bmod 4$ you can take $t = 0$ or 1 provided t is a square or z is not a square.

More generally, if $P = \begin{pmatrix} \alpha & \beta \\ \omega\beta & \alpha \end{pmatrix}$ then

$$\begin{aligned} & \frac{1}{\det P} PAP^{-1} \\ = \; & \frac{1}{\left(\alpha^2-\beta^2\omega\right)^2} \begin{pmatrix} t\alpha^2 + y\alpha\beta - x\alpha\beta\omega - z\beta^2\omega & x\alpha^2 - y\beta^2 - t\alpha\beta + z\alpha\beta \\ y\alpha^2 - x\beta^2\omega^2 + t\alpha\beta\omega - z\alpha\beta\omega & z\alpha^2 - y\alpha\beta - t\beta^2\omega + x\alpha\beta\omega \end{pmatrix}. \end{aligned}$$

So to show that we can take $t = 0$ or 1 even in the case $p = 1 \bmod 4$, we need to show that whatever the values of t, x, y, z we can always find α, β (not both zero) such that

$$t\alpha^2 + y\alpha\beta - x\alpha\beta\omega - z\beta^2\omega$$

is a square. Clearly this is possible if t is a square, or if z is not a square. So let $p = 1 \bmod 4$, and assume that t is not a square and that z is a square. We show that we can always find some value of α for which

$$t\alpha^2 + y\alpha - x\alpha\omega - z\omega$$

is a square. (Since z is a square, this value of α cannot be zero.) Completing the square, we have

$$t\alpha^2 + y\alpha - x\alpha\omega - z\omega = t(\alpha + \frac{y - x\omega}{2t})^2 - \frac{(y - x\omega)^2}{4t} - z\omega.$$

Setting $\frac{(y-x\omega)^2}{4t} + z\omega$ equal to λ, we see that finding α such that $t\alpha^2 + y\alpha - x\alpha\omega - z\omega$ is a square is equivalent to finding α such that

$$t\alpha^2 - \lambda$$

is a square. If λ is a square then (since $p = 1 \bmod 4$) we see that $t\alpha^2 - \lambda$ is a square when $\alpha = 0$. On the other hand if λ is not a square then (since t is not a square) we can find α such that $t\alpha^2 - \lambda = 0$.

So we can assume that $t = 0$ or 1, This means that we can find representatives for the $p^2 + (p+1)/2 - \gcd(p-1, 4)/2$ orbits in work of order p^5. Not brilliant — it would be nice to do better.