ELEMENTS OF ODD ORDER IN $\mathbf{PSL(2,p)}$

DENIS XAVIER CHARLES

Abstract. We investigate the number of odd order elements in the group $\mathrm{PSL}(2,p)$, where p is a prime. We give a lower bound for this number that is better than the Frobenius bound. We also give a characterization of some of the odd order elements in the group.

1. Introduction

Let p be a prime, $\mathrm{GL}(2,p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z}/p\mathbb{Z},\ ad-bc \neq 0 \right\}$ is the *general linear group* (of dimension 2) over $\mathbb{Z}/p\mathbb{Z}$. The center of this group $Z(\mathrm{GL}(2,p))$ is the set of scalar matrices $\begin{pmatrix} f & 0 \\ 0 & f \end{pmatrix}$, $f \neq 0$. The group $\mathrm{GL}(2,p)/Z(\mathrm{GL}(2,p))$ is the *projective general linear group* denoted $\mathrm{PGL}(2,p)$. The *special linear group* $\mathrm{SL}(2,p)$ is the subgroup $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,p) \;\middle|\; ad-bc = 1 \right\}$. The image of this subgroup onto $\mathrm{PGL}(2,p)$ is the *projective special linear group* denoted $\mathrm{PSL}(2,p)$. The group $\mathrm{PSL}(2,p)$ will be the focus of our study.

2. Structure of $\mathrm{PSL}(2,p)$

We summarize the known facts about the structure of the special and projective linear groups. The group $\mathrm{PGL}(2,p)$ can also be thought of as the group of fractional linear transformations on the projective line $\{w \mid w \in \mathbb{Z}/p\mathbb{Z}\} \cup \{\infty\}$ given by $\alpha(z) = \frac{az+b}{cz+d}$, $ad-bc \neq 0$. Elements in $\mathrm{PGL}(2,p)$ differing by a scalar multiple are equivalent. Hence $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is equivalent to a matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with $\alpha\delta - \beta\gamma = 1$ iff $M = \begin{pmatrix} f & 0 \\ 0 & f \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ or $\det(M)$ is a square in $\mathbb{Z}/p\mathbb{Z}$.

Theorem 2.1. *Let $p > 2$ be a prime. Then*
(1) $|\mathrm{GL}(2,p)| = (p^2-1)(p^2-p)$;
(2) $|\mathrm{PGL}(2,p)| = (p^2-1)p$;
(3) $|\mathrm{SL}(2,p)| = (p^2-1)p$;
(4) $|\mathrm{PSL}(2,p)| = \frac{1}{2}(p^2-1)p$.

Proof : The group $\mathrm{GL}(2,p)$ is just the 2×2 non-singular matrices over the field $\mathrm{GF}(p)$. We can select the first column vector to be any non-zero vector and so we have p^2-1 choices. The span of the first row excludes p vectors and the second column vector can thus be selected in p^2-p ways. Hence $|\mathrm{GL}(2,p)| = (p^2-1)(p^2-p)$. Since the homomorphism from $\mathrm{GL}(2,p)$ to $\mathrm{PGL}(2,p)$ has kernel of order $p-1$ we have $|\mathrm{PGL}(2,p)| = (p^2-1)p$. Now consider the homomorphism $M \to \det M$ from $\mathrm{GL}(2,p)$ to $\mathrm{GF}(p)$. If $ad-bc = \eta$, then $\eta^{-1}\xi(ad-bc) = \xi$, thus each value of the determinant occurs equally often. Hence $\mathrm{SL}(2,p)$ had index $p-1$ in $\mathrm{GL}(2,p)$ and so $|\mathrm{SL}(2,p)| = (p^2-1)p$. Finally, since $|Z(\mathrm{SL}(2,p))| = 2$ for odd prime p, the last claim follows.
□

Understanding the structure of the group $\mathrm{SL}(2,p)$ is essential in our understanding of $\mathrm{PSL}(2,p)$. The following theorem shows that the Sylow-p subgroups of the special linear group are cyclic.

Theorem 2.2. *The group* $\mathrm{SL}(2,p)$ *contains cyclic subgroups of order* $p-1$ *and* $p+1$.

Proof : Consider the matrices $\begin{pmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{pmatrix}$, where $\lambda \neq 0$. These matrices form a subgroup of $\mathrm{SL}(2,p)$ which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\star}$, and hence is cyclic of order $p-1$.

To prove the second assertion we consider the matrices of $\mathrm{GL}(2,p)$ as defining linear transformations on a vector space V of dimension 2 over $\mathrm{GF}(p)$. Such a vector space is a degree 2 algebraic extension of $\mathrm{GF}(p)$ and hence $V \cong \mathrm{GF}(p^2)$. We know that the multiplicative group of $\mathrm{GF}(p^2)$ is cyclic and so left multiplication by the generator of this group is a linear transformation of order p^2-1. Thus $\mathrm{GL}(2,p)$ contains a cyclic group C of order p^2-1. Now consider the homomorphism $M \to \det M$ of C onto the multiplicative group of $\mathrm{GF}(p)$ whose order is $p-1$. The kernel of this homomorphism is cyclic and has order a multiple of $p+1$ and thus has a cyclic subgroup of order $p+1$. □

3. Odd order elements in $\mathrm{PSL}(2,p)$

It is clear from the results of the previous section that there are at least $\frac{p(p-1)}{2}$ elements of odd order. The following theorem gives a non-trivial lower bound on the number of odd order elements. We adopt the notation of [Gor68].

Theorem 3.1 (Frobenius). *Let* m *be a divisor of the order of a finite group* G. *Then the number of solutions of the equation* $g^m = 1$ *in* G *is a multiple of* m.

Corollary 3.2. *Let* $n = p(p^2-1)/2$, *and let* $\nu_2(n)$ *be the largest power of 2 that divides* n. *Then there are at least*

$$\frac{n}{2^{\nu_2(n)}}$$

elements of odd order in $\mathrm{PSL}(2,p)$.

For the rest of this section we will consider $\mathrm{PSL}(2,p)$ as the group of actions on the projective line $\mathcal{L}$. The following results will prove useful.

Theorem 3.3. $\mathrm{PSL}(2,p)$ *is doubly transitive on* $\mathcal{L}$ *and only the identity fixes three points.*

A group which has the property given above is called a *Zassenhaus* group. We will make use of the following facts about Zassenhaus groups.

Theorem 3.4. *Let* G *be a Zassenhaus group acting on* $n+1$ *letters (called the degree) and let* N *be the subgroup fixing a letter. Then we have*

(1) N *is a Frobenius group with kernel* K *of order* n *and complement* H.
(2) K *is a Hall subgroup of* G, K *is disjoint from its conjugates, and* $N = N_G(K)$.
(3) H *is a subgroup of* G *fixing two letters,* H *is disjoint from its conjugates in* G, *and* $|N_G(H) : H| = 2$.
(4) $|G| = en(n+1)$, *where* $e = |H|$ *and* e *divides* $n-1$.

As a consequence we have that $\mathrm{PSL}(2,p)$ is a Zassenhaus group of degree $p+1$, on the points $\{\infty, 0, 1, \cdots, p-1\}$. $|K| = p$, $|H| = \frac{p-1}{2}$. Further $|N_G(H)| = p-1$.

Theorem 3.5. *Let* ν *be the largest power of 2 that divides* $p-1$. *Then there are at least*

$$\frac{(p^2-1)}{2}\left(\frac{p-1}{2^{\nu}}+2\right)+\frac{p-1}{2^{\nu}}$$

elements of odd order in $\mathrm{PSL}(2,p)$.

Proof : Working out the proof of the previous theorem in the case of $\mathrm{PSL}(2,p)$ we get the following facts. H is the cyclic group of order $\frac{p-1}{2}$ — the image of the cyclic group of order $p-1$ in $\mathrm{SL}(2,p)$. The normalizer of this group can be explicitly computed and it is: $\left\{\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{pmatrix}, \begin{pmatrix}0 & -\alpha^{-1}\\ \alpha & 0\end{pmatrix} \;\middle|\; \alpha \neq 0\right\}$. Let us see when two conjugates of H are the same. Now $aHa^{-1} = bHb^{-1}$ iff $a^{-1}b \in N_G(H)$. It is clear that none of the p-Sylow

group elements can be in the normalizer and it turns out that we can partition the $p+1$ p-Sylow groups into classes of two groups such that pairwise products from these classes cannot also be in the normalizer. Let $S_1, \cdots S_{(p+1)/2}$, be representative groups of these classes. Also let m be the number of odd order elements in H ($m = \frac{p-1}{2^\nu}$ since it is a cyclic group). Conjugating by elements in $\cup_i S_i$ yields distinct conjugates of H. Thus this gives us a total of $\frac{(p^2-1)}{2}m + m$ elements of odd order. Since the p-Sylow subgroups (of which there are $p+1$) are disjoint they give an additional $p^2 - 1$ elements of odd order we arrive at the claimed estimate.
□

4. On the solutions of $g^m = I$ in $SL(2,p)$

In what follows we will characterize the elements in $SL(2,p)$ which satisfy equations of the type $g^m = I$.

Theorem 4.1. *Let* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,p)$, *and* $\tau = \mathrm{Tr}(M) = a + d$. *Then*

$$M^n = \begin{pmatrix} a\chi_n - \chi_{n-1} & b\chi_n \\ c\chi_n & d\chi_n - \chi_{n-1} \end{pmatrix}$$

for $n \geq 1$, *where* $\chi_0 = 0$, $\chi_1 = 1$ *and*

$$\chi_n = \tau\chi_{n-1} - \chi_{n-2}, \text{ for } n > 1.$$

Proof : The proof is by induction on n. The result is true for $n = 1$. Assume for the result for n, as the induction hypothesis. Now

$$\begin{aligned}
M^{n+1} &= M^n M \\
&= \begin{pmatrix} a\chi_n - \chi_{n-1} & b\chi_n \\ c\chi_n & d\chi_n - \chi_{n-1} \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
&= \begin{pmatrix} a^2\chi_n - a\chi_{n-1} + bc\chi_n & ab\chi_n - b\chi_{n-1} + bd\chi_n \\ ac\chi_n + cd\chi_n - c\chi_{n-1} & bc\chi_n + d^2\chi_n - d\chi_{n-1} \end{pmatrix} \\
&= \begin{pmatrix} a^2\chi_n - a\chi_{n-1} + (ad-1)\chi_n & b(\chi_n(a+d) - \chi_{n-1}) \\ c(\chi_n(a+d) - \chi_{n-1}) & (ad-1)\chi_n + d^2\chi_n - d\chi_{n-1} \end{pmatrix} \\
&= \begin{pmatrix} a((a+d)\chi_n - \chi_{n-1}) - \chi_n & b(\chi_n\tau - \chi_{n-1}) \\ c(\chi_n\tau - \chi_{n-1}) & d((a+d)\chi_n - \chi_{n-1}) - \chi_n) \end{pmatrix} \\
&= \begin{pmatrix} a\chi_{n+1} - \chi_n & b\chi_{n+1} \\ c\chi_{n+1} & d\chi_{n+1} - \chi_n \end{pmatrix}.
\end{aligned}$$

This proves the inductive step. □

Corollary 4.2. *Let* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *Then* $M^3 = I$ *iff* $\mathrm{Tr}(M) = -1$.

Proof : Let $\tau = a + d$. Then by the above theorem $M^3 = \begin{pmatrix} a(\tau^2-1) - \tau & b(\tau^2-1) \\ c(\tau^2-1) & d(\tau^2-1) - \tau \end{pmatrix}$. If $\tau = -1$ clearly $M^3 = I$. Now if one of b, c is not zero then we are done. Suppose $b = c = 0$, then $ad - bc = 1$ gives $d = a^{-1}$. Thus $a(\tau^2 - 1) - \tau = d(\tau^2 - 1) - \tau$ which implies $(\tau^2 - 1)(a - d) = 0$, if $a \neq 1, a^{-1} = d \neq a$ and so $(\tau^2 - 1) = 0$, this then implies $\tau = -1$. □

Corollary 4.3. *Let* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *Then* $M^p = I$, *iff* $\mathrm{Tr}(M) = 2$.

Proof : An element of order p defines a Sylow subgroup, which is just a conjugate subgroup of the elements of the form $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$, these elements and their conjugates all have trace 2. Now for the other direction. If $\tau = 2$, then by induction $\chi_n = n$, thus $M^p = \begin{pmatrix} -(-1) & 0 \\ 0 & -(-1) \end{pmatrix}$. □

Next we characterize the solutions of the equation $g^{p-1} = I$.

Theorem 4.4. *Let* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\tau = a + d$. *Then* $M^{p-1} = I$ *iff* $\tau = \alpha + \alpha^{-1}$, $\alpha \neq 1$.

Proof : The solutions to $g^{p-1} = I$ consist of conjugates of the cyclic subgroup of order $p - 1$ exhibited earlier. All these conjugates have trace of the form claimed by the theorem. Now suppose M is a matrix with trace $\tau = \alpha + \alpha^{-1}$. We first prove the following claim.
Claim: If $\tau = \alpha + \alpha^{-1}$ then $\chi_n = \alpha^{n-1} + \alpha^{-(n-1)} + \chi_{n-2}$ for $n \geq 2$.
Proof of claim: $\chi_2 = \tau = \alpha + \alpha^{-1} + 0 = \alpha + \alpha^{-1} + \chi_0$. Now

$$\begin{aligned}
\chi_{n+1} &= \tau\chi_n - \chi_{n-1} \\
&= \tau(\alpha^{n-1} + \alpha^{-(n-1)} + \chi_{n-2}) - \chi_{n-1} \\
&= \tau(\alpha^{n-1} + \alpha^{-(n-1)}) + \tau\chi_{n-2} - \chi_{n-1} \\
&= \alpha^n + \alpha^{-n} + \alpha^{n-2} + \alpha^{-(n-2)} + \tau\chi_{n-2} - \chi_{n-1} \\
&= \alpha^n + \alpha^{-n} + \tau\chi_{n-2} - \chi_{n-3} \\
&= \alpha^n + \alpha^{-n} + \chi_{n-1},
\end{aligned}$$

since $\chi_{n-1} = \alpha^{n-2} + \alpha^{-(n-2)} + \chi_{n-3}$.
This proves the claim.

Now if $n = 2m$, we have

$$\begin{aligned}
\chi_n &= \alpha^{n-1} + \alpha^{n-3} + \cdots + \alpha^3 + \alpha \\
&\quad + \alpha^{-(n-1)} + \alpha^{-(n-3)} + \cdots + \alpha^{-1} \\
&= \alpha\left(\frac{(\alpha^2)^m - 1}{\alpha^2 - 1}\right) + \alpha^{-1}\left(\frac{(\alpha^{-2})^m - 1}{\alpha^{-2} - 1}\right).
\end{aligned}$$

Since $\alpha^{p-1} = \alpha^{-(p-1)} = 1$, we have $\chi_{p-1} = 0$. Now suppose $n = 2m + 1$, then

$$\begin{aligned}
\chi_n &= \alpha^{2m} + \alpha^{2(m-1)} + \cdots + \alpha^4 + \alpha^2 + \\
&\quad + \alpha^{-2m} + \alpha^{-2(m-1)} + \cdots + \alpha^{-4} + \alpha^{-2} + 1 \\
&= 1 + \alpha^2\left(\frac{(\alpha^2)^m - 1}{\alpha^2 - 1}\right) + \alpha^{-2}\left(\frac{(\alpha^{-2})^m - 1}{\alpha^{-2} - 1}\right).
\end{aligned}$$

Thus

$$\begin{aligned}
\chi_{p-2} &= 1 + \frac{\alpha^{p-1} - \alpha^2}{\alpha^2 - 1} + \frac{\alpha^{-(p-1)} - \alpha^{-2}}{\alpha^{-2} - 1} \\
&= 1 - 1 - 1 \\
&= -1.
\end{aligned}$$

Thus $M^{p-1} = I$. □

References

[Gor68] Gorenstein, Daniel. *Finite Groups*, Harper & Row publishers, 1968.