NOTE ON PRIMITIVE PERMUTATION GROUPS AND A DIOPHANTINE EQUATION

J.D. HENSTRIDGE and Cheryl E. PRAEGER

Department of Mathematics, The University of Western Australia, Nedlands, W.A. 6009, Australia

Received 16 December 1977

It is shown that there are no transitive rank 3 extensions of the projective linear groups $H$, $PSL(m, q) \leq H \leq P\Gamma L(m, q)$, for any prime power $q$ and integer $m \geq 3$. In the course of the proof the diophantine equation $5^m + 11 = x^2$, where $m, x$ are positive integers, arose. As such equations can now be solved completely we had the choice of using number theory or geometry to complete the proof.

If a group $G$ has a maximal subgroup $H$, then $G$ acts by right multiplication on the set $\Omega$ of right cosets of $H$ in $G$ as a primitive, but not necessarily faithful, permutation group. As part of the search for new finite simple groups it is of interest to determine all possible groups $G$, and in particular all simple groups, which contain a given group $H$ as a maximal subgroup. This problem is very difficult, but if the permutation representation induced on $\Omega$ has small rank and is faithful it has been solved for certain groups $H$. In this paper we assume that $G$ is faithful on $\Omega$ and that $H$ has an orbit $\Delta$ in $\Omega$ such that $PSL(m, q) \leq H \leq P\Gamma L(m, q)$ in its natural representation on the points or hyperplanes of the projective space, for some $m \geq 3$ and prime power $q$. The case in which $G$ has rank 2 on $\Omega$ was dealt with by H. Zassenhaus [11] and D.R. Hughes [7]. We shall show that there exist no groups $G$ which have rank 3 on $\Omega$. This result is a generalisation of Bannai [2] which has the additional assumptions that $H$ is faithful on $\Delta$ and $q$ is even.

Using a recent result of one of the authors [9] and the powerful restrictions on intersection numbers developed by D.G. Higman [4] we could show that either $q = 3$, $m = 5$, or $q = 5$ and $5^m + 11$ is a perfect square. The former case was eliminated by considering the action of a Sylow 13-subgroup. A very complicated general argument involving geometry and a Sylow $p$-subgroup, where $p$ is a prime greater than 5 dividing $(5^{m-2} - 1)$, could be constructed to eliminate the other case. However the diophantine equation

$$5^m + 11 = x^2$$

where $m, x$ are positive integers interested us, for a computer search for solutions (which involved consideration of the equation modulo various primes), showed that the only solutions for $m < 10^{30}$ are for $m = 1, 2, 5$. Then in a conversation
with David Hunt and Alf van der Poorten we discovered that Gel'fond–Baker inequalities yielded computable bounds on values of \( m \) satisfying such equations. Very recently Hunt and van der Poorten produced a concise proof that the only solutions of (1) are for \( m = 1, 2, 5 \) (see [6]). Thus our proof was greatly simplified.

The formal statement of the result and details of the proof follow.

**Theorem.** Let \( G \) be a primitive simply transitive permutation group on \( \Omega \) and assume that \( G_\alpha, \alpha \in \Omega, \) has an orbit \( \Delta(\alpha) \) in \( \Omega \) such that \( \text{PSL}(m, q) \leq G^{(\alpha)} \leq \text{PGL}(m, q) \) in its representation on the \((q^m - 1)/(q - 1)\) points of the projective space, where \( m \geq 3 \) and \( q \) is a prime power. Then \( G \) has rank at least four on \( \Omega \).

**Proof of the theorem.** Let \( G \) satisfy the assumptions of the theorem and assume that \( G \) has rank 3 on \( \Omega \). Set \( k = (q^m - 1)/(q - 1) = |\Delta(\alpha)| \). Then \( \Gamma(\alpha) = \Omega - (\Delta(\alpha) \cup \{\alpha\}) \) is an orbit of \( G_\alpha \) which by [9] has length \( l = k(k - 1)/\mu \), where \( \mu \) is 1 or 2, or \( \mu = q \) is 3 or 4, or \( \mu = q + 1 \) is 3, 4, or 6. Moreover if \( \mu > 1 \), then \( G_\alpha \) is faithful on \( \Delta(\alpha) \), and if \( \mu = q + 1 \), then \( m \geq 4 \). The case \( \mu = 1 \) is impossible by results of D.G. Higman and M. Aschbacher ([4, Theorem 1], [1] and [5]). Hence \( \mu \) is 2, 3, 4, or 6 and \( G_\alpha \) is faithful on \( \Delta(\alpha) \).

We now consider the Higman parameters of \( G \) (see [4]). If \( \beta \in \Delta(\alpha) \), then by [5, (2.6)] \( \lambda = |\Delta(\alpha) \cap \Delta(\beta)| = 0 \). Also if \( \gamma \in \Gamma(\alpha) \), then \( |\Delta(\alpha) \cap \Delta(\gamma)| = \mu \), where \( l = k(k - 1)/\mu \) (see [3]). By [4, Lemma 7] \( d = 4k + \mu(\mu - 4) \) is a square and \( d^2 \) divides \( e = k(k + \mu - 3) \). Examination of these conditions shows:

**Lemma.** Either (a) \( q = 3, m = 5, \mu = 4, \) and \( n = 3752 = 2^3 \cdot 7 \cdot 67 \), or
(b) \( q = 5, \mu = 1 + k + k(k - 1), \) and \( 5m + 11 \) is a square.

**Proof.** Suppose first that \( \mu = 2 \). Then \( d = 4q(q^m - 1)/(q - 1) \) is a square and hence both \( q \) and \( (q^m - 1)/(q - 1) \) are squares. By [8], (or see Math. Reviews Vol. 8, 315), it follows that \( m = 3 \). Hence \( q + 1 = y^2 \) for some integer \( y \) and so \( q = (y + 1)(y - 1) \) which can never be both a square and a prime power, contradiction. If \( \mu = 3 \), then \( d = 4k - 3 \) divides \( e^2 = k^4 \). Since \( k \geq 7 \) it follows that \( k = 21 \). However if \( \mu = 3 \), then \( q = 2 \) or 3 and \( k \) is not 21 for any \( m \). If \( \mu = 4 \), then \( d = 4k \) and hence \( k = (q^m - 1)/(q - 1) \) is a square. By [8] \((m, q)\) is either \((4, 7)\) or \((5, 3)\). Since \( \mu \) is \( q \) or \( q + 1 \) we must have \( m = 5, q = 3, \) and part (a) is true.

Finally let \( \mu = 6 \). Then \( q = 5 \) and \( m \geq 4 \). Also \( d = 4(k + 3) = 5m + 11 \) is a square. (The divisibility condition yields slightly more information in this case but it is not required.) Finally we show that neither possibility can arise.

In case (a) of the lemma we have \( \text{PSL}(5, 3) \leq G_\alpha \leq \text{PGL}(5, 3) \), and \( |G : G_\alpha| = 2^3 \cdot 7 \cdot 67 \). Moreover \( G_\alpha^{(\alpha)} \) is the action on points and \( G_\alpha^{(\alpha)} \) the action on lines of the projective space. A fairly easy geometrical argument shows that a Sylow \( 13 \)-subgroup of \( \text{PSL}(5, 3) \) fixes exactly 4 points and 1 line of the projective space. Hence a Sylow \( 13 \)-subgroup \( P \) of \( G_\alpha \) fixes 4 points of \( \Delta(\alpha) \), 1 point of \( \Gamma(\alpha) \), and
hence 6 points of $\Omega$. By [10, 3.7] the normaliser $N$ of $P$ in $G$ is transitive on the fixed points of $P$ in $\Omega$ and so $|N : N \cap G_\alpha| = 6$. As $P$ is a Sylow 13-subgroup of both $G$ and $G_\alpha$ it follows from Sylow's theorem that $|G_\alpha : N \cap G_\alpha| = 1 \pmod{13}$ and $|G : N| = 1 \pmod{13}$. Thus mod 13, $6 | G : N | = 6 | G : N \cap G_\alpha| = n |G_\alpha : N \cap G_\alpha| = n$, a contradiction.

In case (b) of the lemma we must have $m = 5$ by [6], since $m \geq 3$. Moreover we have $\text{PSL}(5, 5) \leq G_\alpha \leq \text{PGL}(5, 5)$, and $G^{\Delta(\alpha)}$ is the action on points and $G^{\Gamma(\alpha)}$ is the action on lines of the projective space. Again an easy geometrical argument shows that a Sylow 31-subgroup of $\text{PSL}(5, 5)$ fixes 6 points and 1 line of the projective space. Hence a Sylow 31-subgroup $P$ of $G_\alpha$ fixes exactly 8 points of $\Omega$. This yields a contradiction just as in the previous case. The proof of the theorem is complete.

References:

[2] E. Bannai, Primitive extensions of rank 3 of the finite projective special linear groups $\text{PSL}(n, q)$, $q = 2^t$, Osaka J. Math. 9 (1972) 57–73.