ISRAEL JOURNAL OF MATHEMATICS, Vol. 21, No. 1, 1975

A NOTE ON TRANSITIVE PERMUTATION GROUPS OF PRIME DEGREE

BY

DAVID CHILLAG

ABSTRACT

Let G be a nonsolvable transitive permutation group of prime degree p. Let P be a Sylow-p-subgroup of G and let q be a generator of the subgroup of $N_G(P)$ fixing one point. Assume that $|N_G(P)| = p(p-1)$ and that there exists an element j in G such that $j^{-1}qj = q^{(p+1)/2}$. We shall prove that a group that satisfies the above condition must be the symmetric group on p points, and p is of the form $4n+1$.

Let G be a nonsolvable transitive permutation group of prime degree p on a set Ω. Let P be a Sylow p-subgroup of G, $N_G(P)$ the normalizer of P in G and $Q = (N_G(P))_\alpha$ the subgroup of $N_G(P)$ fixing the point $\alpha \in \Omega$. If $|N_G(P)| = p(p-1)$, then it is known that G is triply transitive and according to a conjecture of N. Ito, G is S_p, the full symmetric group on p elements (see [5], p. 618, 2.17(a) or [7]). We note that Q is cyclic of order $p-1$ ([3] Lemma 2.1) and we prove the following special case of Ito's conjecture:

THEOREM. *Let G be a non-solvable transitive permutation group of prime degree p on a set Ω. Let P be a Sylow p-subgroup of G and let q be a generator of $Q = (N_G(P))_\alpha$ for $\alpha \in \Omega$. Assume that $|N_G(P)| = p(p-1)$ and that G contains an element j such that $j^{-1}qj = q^{(p+1)/2}$. Then G coincides with S_p and p is of the form $4n+1$.*

If x is a positive integer, we note by $\phi(x)$ the number of natural numbers which are relatively prime to x and are smaller than x. The following corollary follows from the above theorem:

COROLLARY. *Let p be a prime of the form $4n+1$ and let G be a nonsolvable transitive permutation group of degree p on a set Ω. Let $\alpha \in \Omega$ and let P be a*

Received October 16, 1974, and in revised form January 15, 1975

Sylow p-subgroup of G. Put $Q = (N_G(P))_\alpha$ and $\phi(p-1) = 2^k m$ where m is odd. Assume that $|N_G(P):P| = p-1$ and that 2^k divides $|N_G(Q):Q|$. Then G coincides with S_p.

Proof of Corollary. Let G_α be the stabilizer of α in G. Then since Q is a semiregular subgroup of G_α and $|Q| = p-1$, we get that Q is regular on $\Omega - \{\alpha\}$. But Q is abelian, so we get that $C_{G_\alpha}(Q) = Q$ ([9] p. 9). The fact that Q fixes exactly one point α implies that $C_G(Q) \subseteq N_G(Q) \subseteq G_\alpha$. Therefore $C_G(Q) = Q$ and $N_G(Q)/Q$ is isomorphic to a subgroup A of Aut(Q). Since Aut(Q) is abelian of order $\phi(p-1)$, the assumption implies that A contains the Sylow 2-subgroup of Aut (Q). Now $p = 4n+1$ implies that $p-1$ and $(p+1)/2$ are relatively prime and consequently the function f mapping every element of Q into its $(p+1)/2$ th power is in Aut (Q). But since $((p+1)/2)^2 \equiv 1$ (mod $p-1$), we get that $f^2 = 1$ so that $f \in A$. Now if jQ is the inverse image of f in $N_G(Q)/Q$, then j is the required element in the theorem, and the corollary follows.

Proof of Theorem. If $p = 4n+3$ then $(p-1, (p+1)/2) \neq 1$ and hence $|q| \neq |q^{(p+1)/2}|$. That contradicts the existence of j. Hence $p = 4n+1$. The rest of the proof is based on Theorem 1 in [3]. We will show that all primes $p = 4n+1$ satisfy the condition of that theorem with few exceptions. Let $GF(p)$ be the field with p elements and let A_k be the number of elements $x \in GF(p)$ such that

$$(1)\quad \left(\frac{x}{p}\right) = \left(\frac{x+k+1}{p}\right) = -1 \quad\text{and}\quad \left(\frac{x+1}{p}\right) = \left(\frac{x+2}{p}\right) = \cdots = \left(\frac{x+k}{p}\right) = 1,$$

where $(*/p)$ is the Legendre symbol. If x satisfies (1), we say that x belongs to A_k or $x \in A_k$. In order to prove the theorem we have to show that there is $k \neq 0, 1, 2, 3, 5, 11$ such that $A_k \neq 0$ and use Theorem 1 in [3]. We note that in [3] we have $(0/p) = +1$.

Lemma. *If $p > 10000$ then $A_4 \neq 0$.*

Proof. In this lemma we take $(0/p) = 0$, so that we can use [4]. By doing that A_4 remains unchanged, since $p = 4n+1$ implies $(x/p) = (-x/p)$. Let $x \in GF(p)$ and define

$$M(x) = \left(1 - \left(\frac{x}{p}\right)\right)\left(1 + \left(\frac{x+1}{p}\right)\right)\left(1 + \left(\frac{x+2}{p}\right)\right)\left(1 + \left(\frac{x+3}{p}\right)\right)\cdot$$

$$\cdot\left(1 + \left(\frac{x+4}{p}\right)\right)\left(1 - \left(\frac{x+5}{p}\right)\right).$$

Clearly $x \in A_4$ if and only if $M(x) = 64$. Also if $x \leqq p-6$ then $x \notin A_4$ if and only if $M(x) = 0$. Therefore $64A_4 = \Sigma_{x=1}^{p-6} M(x)$. Now since $M(x) \leqq 32$ for $x > p-6$ and $M(p-1) = 0$, we obtain:

$$\left| 64A_4 - \sum_{x=1}^{p} M(x) \right| \leqq \sum_{x=p-5}^{p} |M(x)| \leqq 5 \cdot 32. \tag{2}$$

We next write $M(x) = 1 + \Sigma_{i=1}^{6} M_i(x)$, where $M_i(x)$ is the sum of $\binom{6}{i}$ terms of the form

$$\left(\frac{(x+u_1)(x+u_2)\cdots(x+u_i)}{p} \right).$$

By Lemma 1 and the end of the proof of Lemma 2 in [4], pp. 36–38, we get that $|\Sigma_{x=1}^{p} M_i(x)|$ is not bigger than $\binom{6}{i}(i-1)\sqrt{p}$ if i is odd and is not bigger than $\binom{6}{i}[1+(i-2)\sqrt{p}]$, if i is even. Therefore

$$\left| \sum_{x=1}^{p} M(x) - p \right| \leqq \binom{6}{2} + \binom{6}{3} 2\sqrt{p} + \binom{6}{4}(2\sqrt{p}+1) + \binom{6}{5} 4\sqrt{p} + (1 + 4\sqrt{p}).$$

Hence

$$\left| \sum_{x=1}^{p} M(x) - p \right| \leqq 98\sqrt{p} + 31. \tag{3}$$

We combined $64A_4 \geqq \Sigma_{x=1}^{p} M(x) - 5\cdot 32$ of (2) with $\Sigma_{x=1}^{p} M(x) \geqq p - 98\sqrt{p} - 31$ of (3) to get $64A_4 \geqq p - 98\sqrt{p} - 31 - 5\cdot 32$. But $p > 10000$, so $64A_4 > 0$. The lemma is proved.

Using a computer program written by Professor George Purdy at the University of Illinois, Urbana, we find that $A_4 \neq 0$ for all primes $p = 4n+1$, $0 < p < 10000$, except for the primes: $5, 13, 17, 41, 53, 61, 101, 109, 197$. The theorem holds for $p = 5, 17$ by [6], since q is an odd permutation ([3], Lemma 2.2). The case $p = 41$ is proved in [3] (Theorem 3). If $p = 101$ then $18 \in A_7$ and if $p = 197$ then $58 \in A_7$ (see [1]), hence $A_7 \neq 0$ and by [3] we are done. Since q is an odd permutation [7] (Corollary 1) proves the cases $p = 109, 61$, and since G is triply transitive [8] proves the theorem for $p = 53$. If $p = 13$, then by Lemma 2.2 in [3] we see that G contains a permutation R that has the following cycle structure: $(0,1,11,12)(6)(5,7)(2,3,4,8,9,10)$. Hence $1 \neq R^6 = (0,1,11,12)^6$ and the minimal degree μ of G is smaller than or equal to 4. But if G doesn't contain the alternating group, we get from [2] (p. 185 I) that $\mu \geqq 13/3 > 4$. Hence G coincides with S_{13}.

ACKNOWLEDGMENT

I wish to thank Professor George Purdy for the computer program.
The computer program is available from the author.

REFERENCES

1. R. V. Andree, *A Table of Indices and Power residues for all Primes and Prime Powers Below 2000*, W. Norton and Company, Inc., New York, 1962.

2. A. Bochert, *Über die Klasse der transitiven Substitutionengruppen*, Math. Ann. **40** (1892), 176–193.

3. D. Chillag, *On a class of transitive permutation groups of prime degree* $p = 4n + 1$, Israel J. Math. **15** (1973), 78–91.

4. S. Chowla, *The Riemann Hypothesis and Hilbert's Tenth Problem*, Blackie and Son Ltd., London and Glasgow, 1965.

5. B. Huppert, *Endliche Gruppen*, Springer-Verlag, Berlin–Heidelberg–New York, 1967.

6. N. Ito, *On transitive permutation groups of Fermat prime degree*, Proc. Int. Conf. Theory of Groups, Aust. Natl. Univ. Canberra, 1965, 191–202.

7. P. M. Neumann, *Transitive permutation groups of prime degree*, J. London Math. Soc. (2) **5** (1972), 202–208.

8. J. Saxl, *On triply transitive groups of odd degree*, J. London Math. Soc. (2), **7** (1973), 159–167.

9. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York and London.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS, U.S.A.