ON A CLASS OF TRANSITIVE PERMUTATION GROUPS OF PRIME DEGREE $p = 4n + 1$

BY

DAVID CHILLAG

ABSTRACT

Suppose G is a nonsolvable transitive permutation group of prime degree p, such that $|N_G(P)| = p(p-1)$ for some Sylow p-subgroup P of G. Let q be a generator of the subgroup of $N_G(P)$, fixing one letter (it is easy to show that this subgroup is cyclic). Assume that G contains an element j such that $j^{-1}qj = q^{(p+1)/2}$. We shall prove that for almost all primes p of the form $p = 4n+1$, a group that satisfies the above conditions must be the symmetric group on a set with p elements.

Introduction

Let p be an odd prime. Let $GF(p)$ be the field with p elements.

DEFINITIONS. Let $x \in GF(p)$. We shall say that $s(x) = +$ *if x is a quadratic residue modulo p, $s(x) = -$ if x is a quadratic nonresidue modulo p and $s(0) =$* $+$. We also define:

$$s(x_1, x_2, \dots, x_n) = (s(x_1), s(x_2), \dots, s(x_n)),$$

where $x_i \in GF(p)$, $i = 1, 2, \cdots, n$.

Let A_k *be the number of different x's in $GF(p)$ such that*:

$$s(x, x+1, \cdots, x+k, x+k+1) = (-, +, \cdots, +, -) \, (*) \; k = 0, 1, 2, \cdots$$

We shall say that $x \in A_k$ if $x \in GF(p)$ and x satisfies (*).

A prime p is called an A-prime if p is of the form $p = 4n+1$ and there exists $k \neq 0, 1, 2, 3, 5, 11$ such that $A_k \neq 0$.

EXAMPLES.

i) By a theorem of A. Brauer [2], there exists N such that every prime p of the form $p = 4n+1$, $p > N$, is an A-prime.

ii) If $p = 24n+1$ then p is an A-prime as $s(-6, -5, -4, -3, -2, -1, 0, 1,$

Received July 19, 1972

2, 3, 4, 5, 6) = (+ * + + + + + + + + + * +), so either $A_9 \neq 0$ or $A_k \neq 0$ for some $k \geqq 13$,

iii) If $p = 840n + m$, $m = 29, 149, 221, 389, 701, 821$, then $3 \in A_4 \neq 0$ and p is an A-prime.

iv) As in examples (ii) and (iii), we can use quadratic reciprocity and indices tables to construct sequences of A-primes and to check whether a prime is an A-prime or not.

NOTATION. The stabilizer of $i_1, i_2, \cdots, i_n$ in a group H is denoted by $H_{i_1 i_2 \cdots i_n}$. The centralizer and normalizer of a subgroup H of G will be denoted by $C_G(H)$ and $N_G(H)$ respectively. We denote by S_p and AL_p the symmetric and the alternating groups of degree p, respectively.

DEFINITIONS G will be said to *satisfy* (p^*) *if* G *is a nonsolvable transitive permutation group of degree* p *such that* $|N_G(P)| = p(p-1)$ *for some Sylow* p*-subgroup* P *of* G.

We shall prove that $(N_G(P))$ is a cyclic group. Denote by q a generator of $(N_G(P))_\alpha$. G will be said to *satisfy* (p^{**}) *if* G *satisfies* (p^*) *and there exists an element* $j \in G$ *such that* $j^{-1}qj = q^{(p+1)/2}$.

By [4, p. 618, 2.17(a)] we see that if G satisfies (p^*), then G is triply-transitive. We shall prove;

THEOREM 1. *If* p *is an* A*-prime and* G *satisfies* (p^{**}) *then* G *coincides with* S_p.

Theorem 1 and the above result of Brauer [2] yield the following:

COROLLARY 1. *There exists* N *such that if* $p = 4n + 1$ *is a prime greater than* N *and* G *satisfies* (p^{**}), *then* G *coincides with* S_p.

Theorem 1 and examples (ii) and (iii) yield:

COROLLARY 2. *If* p *is a prime of the form* $p = 24n + 1$ *and* G *satisfies* (p^{**}), *then* G *coincides with* S_p.

COROLLARY 3. *If* p *is a prime of the form* $p = 840n + m$, $m = 29, 149, 221, 389, 701, 821$ *and* G *satisfies* (p^{**}), *then* G *coincides with* S_p.

In the last section we shall see that in some classes of primes, the definition of an A-prime can be generalized and Theorem 1 still holds.

This paper is partly based on a part of the author's M. Sc. thesis at the University of Tel Aviv. The author wishes to express his appreciation of his advisor, Professor M. Herzog, for his devoted guidance and encouragement.

1. The permutation R and its cycle structure

Let p be a prime of the form $p = 4n + 1$; then, $s(x) = s(-x)$. We shall use the arithmetic rules of quadratic residues freely, We write $h \equiv f$ for $h \equiv f \pmod p$.

LEMMA 1.1. *If $x \in A_k$ then $x \not\equiv -(x + c)$, for every $c < k + 1$.*

PROOF. Suppose $x \equiv -(x+c)$; then $x \equiv (p-c)/2$ if c is odd and $x = p-c/2$ if c is even. If $x \equiv p - c/2$, then $x+c \equiv p+c/2$ and $s(x) = -$ imply that $s(x + c) = s(c/2) = s(-c/2) = s(x) = -$. But $c < k+1$; hence, $x \notin A_k$, a contradiction. If $x \equiv (p - c)/2$ and $s(2) = +$, then $x + c = (p+c)/2$ and $s(x + c) = s(p + c) = s(c) = s(p - c) = s(p - c)/2) = s(x) = -$, which is again a contradiction to $x \in A_k$, since $c < k + 1$. If $x \equiv (p - c)/2$ and $s(2) = -$, then $s(x + c) = -s(p + c) = -s(c) = -s(p - c) = s(p-c)/2) = s(x) = -$, which is a contradiction.

DEFINITION Let R be the function:

$$R : GF(p) \to GF(p), \text{ such that}$$

$$R(x) = \begin{cases} x+1 & \text{if } s(x+1) = + \\ -(x+1) & \text{if } s(x+1) = - \end{cases} \quad \text{for every } x \in GF(p).$$

Clearly, R is a permutation on $GF(p)$. We shall write R.c.s. for: "The cycle structure of R contains $\cdots$".

In order to get information about the cycle structure of R, we shall divide the set of primes of the form $4n + 1$ into four subsets according to the quadratic character of 2 and 3.

Case (*a*). $p = 4n+1$, n is even and $s(3) = -$. Here we have $s(\pm 1) = s(\pm 2) = +$, $s(\pm 3) = -$. Hence $x \not\equiv -(x+k)$, $k = 1, 2, 4, 8, 9$ for every x such that $s(x) = -$. (For example $x \not\equiv -(x + 8)$ because otherwise, $x \equiv p - 4$ which implies $s(x) = +$.)

(a1) If $x \in A_0$ then $R(x) \equiv -(x + 1)$ and $R^2(x) = x$; therefore, R.c.s. the 2-cycle $(x, -(x + 1))$.

(a2) If $x \in A_1$, then $R(x) \equiv x + 1$, $R^2(x) \equiv -(x + 2)$, $R^3(x) \equiv -(x + 1)$, $R^4(x) \equiv x$, and because of $x \not\equiv -(x+k)$, $k = 1, 2$, R.c.s. the 4-cycle $(x, x + 1, -(x + 2), -(x + 1))$.

(a3) If $x \in A_2$, then R.c.s. the 6-cycle $(x, x + 1, x + 2, -(x + 3), -(x + 2), -(x + 1))$, except when $x \equiv -(x + 3)$ which implies $x \equiv (p-3)/2$ which actually satisfies $x \in A_2$ In this case R.c.s. the 3-cycle $(x, x + 1, x + 2)$.

(a4) If $x \in A_3$, then R.c.s. the 8-cycle $(x, x+1, x+2, x+3, -(x+4), -(x+3), -(x+2), -(x+1))$, because $x \not\equiv -(x+4)$ and Lemma 1.1.

(a5) If $x \in A_4$, then R.c.s. the 10-cycle $(x, x+1, x+2, x+3, x+4, -(x+5), -(x+4), -(x+3), -(x+2), -(x+1))$. To show this we need to show only (because of Lemma 1.1) that $x \not\equiv -(x+5)$. Suppose not; then, $x \equiv \frac{1}{2}(p-5)$ and $s(x+1) = s(3) = -$, which contradicts the fact that $x \in A_4$.

(a6) If $x \in A_5$, then R.c.s. the 12-cycle $(x, x+1, \cdots, x+5, -(x+6), -(x+5), \cdots, -(x+1))$, except when $x \equiv -(x+6)$ which implies $x \equiv p-3$ which satisfies $x \in A_5$. In this case R.c.s. the 6-cycle $(x, x+1, \cdots\ x+5)$. (Here we use Lemma 1.1 freely.)

(a7) If $x \in A_6$, then R.c.s. 14-cycle. We need to show only that $x \not\equiv -(x+7)$. Suppose not; then $x = (p-7)/2$ and $s(x+2) = s(3) = -$, which is a contradiction to $x \in A_6$.

(a8-a12) If $x \in A_k$, $k = 7, 8, 9, 10, 11$, then as above we can check that $x \in A_k$ implies $x \not\equiv -(x+k+1)$; hence (by Lemma 1.1), we obtain: R.c.s. the $2(k+1)$-cycle $(x, x+1, \cdots, x+k, -(x+k+1), -(x+k), \cdots, -(x+1))$, $k = 7, 8, 9, 10, 11$.

(a13) If $x \in A_k$, $k > 11$, then R.c.s. α-cycle, $\alpha > 12, \alpha \neq 24$. In this last case the cycle is $(x, x+1, \cdots, x+k, \cdots)$. By Lemma 1.1, $\alpha = 24$ can occur only when $k = 23$ and $x \equiv -(x+24)$, which implies $x = p-12$ and $s(x+9) = s(3) = -$, which contradicts $x \in A_{23}$. Hence $\alpha = 24$ does not occur.

Using the same procedure we consider the remaining cases:

Case (*b*). $p = 4n+1$, n is even and $s(3) = +$.

Case (*c*). $p = 4n+1$, n is odd and $s(3) = \pm$.

The results of the above consideration of the three cases are collected in the following lemma.

LEMMA 1.2. *If* $x \in A_k$ *then*:

A) *If* $k \neq 0, 1, 2, 3, 5, 11$, *then R.c.s.* α*-cycle*, $\alpha \nmid 24$

B) *If* $k = 0, 1, 2, 3, 5, 11$, *then R.c.s. the* α*-cycle*, $\alpha = 2(k+1)$, $(\alpha \mid 24)$:

$$(x, x+1, \cdots, x+k, -(x+k+1), -(x+k) \cdots, -(x+1)),$$

except in the cases:

i) n *is even* $s(3) = -$, $k = 2$, $x \equiv (p-3)/2$

n *is even* $s(3) = -$, $k = 5$, $x \equiv p-3$

ii) n *is odd* $k = 0$, $x \equiv \frac{1}{2}(p-1)$

n *is odd* $k = 3$, $x \equiv p-2.$

In these exceptional cases, $\alpha = k+1 \mid 24$ and the α-cycle is $(x, x+1, \cdots, x+k)$.

The following lemma obviously holds because $s(x) = s(-x)$:

LEMMA 1.3. *If* $x \in A_k$, $k = 0,1,2,3,5,11$, *then*:

A) *If x is not an exceptional case, then there exists exactly one* $y \not\equiv x$, $y \in A_k$ *such that*:

$$(x,x+1,x+2,\cdots,x+k,-(x+k+1),-(x+k),\cdots,-(x+1)) =$$
$$(y,y+1,y+2,\cdots,y+k,-(y+k+1),-(y+k),\cdots,-(y+1)).$$

(*R.c.s. this cycle by Lemma* 1.2 (*B*).)

B) *If x is an exceptional case, then there is no $y \not\equiv x$ in $GF(p)$ such that*

$$(x,x+1,\cdots,x+k) = (y,y+1,\cdots,y+k).$$

(*R.c.s.* $(x,x+1,\cdots,x+k)$, *by Lemma* 1.2 (B).)

PROOF.

A) $y \equiv -(x+k+1)$.

B) This can be checked in each exceptional case. (For example, if $k = 3$, $x \equiv p-2$ and y is such that R.c.s. $(x,x+1,x+2,x+3) = (y,y+1,y+2,y+3)$, then $R(y+3) = y$, so $y = y+4$ or $y \equiv -(y+4)$ (by definition of R); hence, $y \equiv -(y+4)$ and $y \equiv p-2 \equiv x$.)

2. Groups containing R

Let G be a permutation group over $\Omega_p = \{\alpha_1,\alpha_2,\cdots,\alpha_p\}$. We take $GF(p)$ as Ω_p in order to facilitate the calculation.

LEMMA 2.1. *If p is an odd prime and G satisfies* (p^*), *then G is* 3-*transitive and* $(N_G(P))_\alpha$ *is a cyclic group of order* $p-1$.

PROOF. G is 3-transitive by [4], p. 618, 2.17(a)]. P is a transitive cyclic group. Therefore $C_G(P) = P$. $N_G(P)$ is a transitive group of prime degree and therefore $(N_G(P))_\alpha$ is *a* maximal subgroup of $N_G(P)$; hence, $N_G(P) = P(N_G(P))_\alpha$. But $P \cap (N_G(P))_\alpha = \langle 1 \rangle$ and consequently

$$\frac{N_G(P)}{C_G(P)} = \frac{N_G(P)}{P} \simeq (N_G(P))_\alpha$$

is a cyclic group since it lies in Aut (P). Obviously $|(N_G(P))_\alpha| = p-1$.

LEMMA 2.2. *If p is a prime, $p > 3$, and G satisfies* (p^{**}), *then G contains the permutation R and q is an odd permutation.*

PROOF. Obviously $G = PG_\alpha$. Write $j = p_1 g_1$, where $p_1 \in P$, $g_1 \in G_\alpha$ and put $p_2 = q^{-1}p_1{}^{-1}qp_1$; then $p_2 \in P$. But $j^{-1}qj \in \langle q \rangle$ implies $j^{-1}qj = g_1^{-1}qp_2g_1 \in \langle q \rangle \subset G_\alpha$ and consequently $p_2 \in G_\alpha \cap P = \langle 1 \rangle$.

Therefore, $q \in C_G(P_1)$ and because of $C_G(P) = P$, we must have $p_1 = 1$. Hence, $j \in G_\alpha$. $N_G(P)$ is clearly a solvable transitive group whence [8, p. 29, 11. 6] implies that $(N_G(P))_{\alpha\beta} = \langle q \rangle_\beta = \langle 1 \rangle$, $\alpha \neq \beta$. But G_α is transitive on $GF(p) - \{\alpha\}$ and $|q| = p - 1$ (Lemma 2.1); therefore, $G_\alpha = \langle q \rangle\, G_{\alpha\beta}$, and we can assume that $j \in G_{\alpha\beta}$. We put $P = \langle \rho \rangle$ and take $(x)\rho$, $(x)q$ and $(x)j$ as analytic forms of ρ, q and j on $GF(p)$ respectively. (In this proof only permutations act from the right side.) We may assume that $(x)\rho \equiv x + 1$. Since P is transitive on $GF(p)$, there exists $h \in P$ such that $(\alpha)h \equiv 0$. Therefore $\langle q^h \rangle = (N_G(P))_0$. Hence, by replacing q by q^h, β by $\beta(h)$, and j by j^h if necessary, we can assume that $0(q) \equiv 0$. Let f be an integer such that $\rho q = q\rho^f$. As $C_G(P) = P$ and $|q| = p - 1$, f is a primitive root modulo p. But $\rho q = q\rho^f$ implies $(x + 1)q \equiv (x)q + f$. As $0(q) \equiv 0$, by induction we obtain $(x)q \equiv fx$. Therefore q is a $(p - 1)$-cycle, hence it is an odd permutation. The relation $jq^2 = q^2 j$, which holds, implies that $(f^2 - 1)\cdot(0)j \equiv 0$. But $p > 3$, hence $(0)j \equiv 0$. Since $\langle q \rangle$ is transitive on $GF(p) - \{0\}$, there exists $t \in \langle q \rangle$ such that $(\beta)t \equiv 1$. Therefore, $((N_G(\langle q \rangle))_{0\beta})^t = (N_G(\langle q \rangle))_{01}$, and by replacing j by j^t if necessary, we can assume $(1)j \equiv 1$. The relation $j^{-1}qj = q^{(p+1)/2}$ and the congruence $f^{(p-1)/2} \equiv -1 \pmod p$ yield: $(fx)j \equiv -f\cdot(x)j$. If $x \in GF(p)$, $x \neq 0$, and $s(x) = +$, then $x \equiv f^r$ for some r, r even and if $s(x) = -$, then $x \equiv f^r$, r odd. Therefore, since $(f^r)j \equiv (-f)^r(1)j = (-1)^r f^r$,

$$(x)j = \begin{cases} x & \text{if } s(x) = + \\ -x & \text{if } s(x) = -, \end{cases}$$

and ρj is the permutation R as $(x)\rho j \equiv (x + 1)j$. The lemma is proved.

Definition. If $p = 4n + 1$, then p is a sum of two squares, $p = a^2 + b^2$. Suppose b is even; then, $a^2 \equiv 1 \pmod 4$, hence we can choose $a \equiv +\left(\frac{2}{p}\right) \pmod 4$, where $\left(\frac{x}{p}\right)$ is the Legendre symbol. Such an a is called *odd base of p*.

Lemma 2.3. *Let p be a prime of the form $p = 4n + 1$, and let a be the odd base of p. Then*:

$$A_0 = \tfrac{1}{4}(p - 1) \tag{1}$$

$$A_1 = \begin{cases} \dfrac{p - 2a + 1}{8} & \text{if } n \text{ is even} \\[2ex] \dfrac{p - 2a - 7}{8} & \text{if } n \text{ is odd} \end{cases} \tag{2}$$

$$A_2 + \tfrac{1}{2}A_3 \geqq \begin{cases} \dfrac{p+6a-15}{16} & \textit{if } n \textit{ is even} \\ \\ \dfrac{p+6a+9}{16} & \textit{if } n \textit{ is odd}\ . \end{cases} \tag{3}$$

PROOF. We recall that here we have $\left(\frac{0}{p}\right) = +1$, but A_0 and A_1 are unchanged if we either interpret $\left(\frac{0}{p}\right)$ as zero or do not define it at all. We find (1) in [7, p. 97, 8*b*]. We now take $\left(\frac{0}{p}\right)$ as zero, (only for the proof of (2)). Then:

$$A_1 + \frac{1}{2}\left(1 - \left(\frac{2}{p}\right)\right) = \frac{1}{8} \sum_{x \in GF(p)} \left(1 - \left(\frac{x}{p}\right)\right)\left(1 + \left(\frac{x+1}{p}\right)\right)\left(1 - \left(\frac{x+2}{p}\right)\right).$$

By

$$\sum_{x \in GF(p)} \left(\frac{x}{p}\right) = 0,$$

which is trivial and

$$\sum_{x \in GF(p)} \frac{(x(x+c)}{p} = -1, \quad c \not\equiv 0 \pmod{p}$$

which is [7, p. 97 8a], we obtain:

$$A_1 + \frac{1}{2}\left(1 - \left(\frac{2}{p}\right)\right) = \frac{p+1}{8} + \frac{1}{8} \sum_{x \in GF(p)} \left(\frac{x(x+1)(x+2)}{p}\right).$$

Now Jacobastal's formula [3, p. 45 (144)] and the fact that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{if } n \textit{ is even} \\ \\ -1 & \textit{if } n \textit{ is odd} \end{cases}$$

yield (2). (Note that in [3] a, the odd base, is taken as $a \equiv -\left(\frac{2}{p}\right)$ mod 4), and $\left(\frac{0}{p}\right) = 0$ [3, (1) p. vii].)

An element $x \in GF(p)$ satisfies $x \in A_k$, for some k, if and only if $s(x) = -$ and $x \in A_k$ for exactly one k. Therefore, $A_0 + A_1 + A_2 + \cdots$ is the number of quadratic nonresidues modulo p. Hence:

$$A_0 + A_1 + A_2 + \cdots = \tfrac{1}{2}(p-1). \tag{i}$$

To each $x \in A_j$, correspond the following $j+1$ elements of $GF(p)$: $x, x+1, \cdots, x+j$. In this way, there are $(j+1)A_j$ elements corresponding to A_j, $j = 0, 1, 2, \cdots$, and each $y \in GF(p)$ is exactly one of the $(j+1)A_j$ elements corresponding to exactly one A_j. Therefore:

$$A_0 + 2A_1 + 3A_2 + \cdots = p. \tag{ii}$$

But $A_0 = \frac{1}{4}(p-1)$; therefore, (i) yields:

$$A_1 + A_2 + A_3 + \cdots = \tfrac{1}{4}(p-1). \tag{iii}$$

Subtracting (i) from (ii) yields:

$$A_1 + 2A_2 + 3A_3 + \cdots = \tfrac{1}{2}(p+1). \tag{iv}$$

Subtracting (iii) from (iv) yields:

$$A_2 + 2A_3 + 3A_4 + \cdots = \tfrac{1}{4}(p+3). \tag{v}$$

Subtracting (iii) from (v) yields:

$$1 + A_1 = A_3 + 2A_4 + 3A_5 + \cdots. \tag{vi}$$

Substituting A_1 into (iii) yields:

$$A_2 + A_3 + A_4 + \cdots = \begin{cases} \dfrac{p+2a-3}{8} & \text{if } n \text{ is even} \\[2ex] \dfrac{p+2a+5}{8} & \text{if } n \text{ is odd.} \end{cases} \tag{4}$$

Substituting A_1 into (vi) yields:

$$A_3 + 2A_4 + 3A_5 + \cdots = \begin{cases} \dfrac{p-2a+9}{8} & \text{if } n \text{ is even} \\[2ex] \dfrac{p-2a+1}{8} & \text{if } n \text{ is odd.} \end{cases} \tag{5}$$

Subtracting (4) from (5) (in both cases) yields:

$$A_4 + 2A_5 + 3A_6 + \cdots \equiv \begin{cases} \dfrac{3-a}{2} + A_2 & \text{if } n \text{ is even} \\[2ex] \dfrac{-a-1}{2} + A_2 & \text{if } n \text{ is odd.} \end{cases} \tag{6}$$

Adding the right side of (6) to the left side of (4) yields:

$$2A_2 + A_3 + \frac{3-a}{2} = \frac{p+2a-3}{8} + A_5 + 2A_6 + \cdots \text{ if } n \text{ is even}$$

$$2A_2 + A_3 + \frac{-1-a}{2} = \frac{p+2a+5}{8} + A_5 + 2A_6 + \cdots \text{ if } n \text{ is odd.}$$

Therefore, ($A_k \geqq 0$), we get:

$$\frac{3-a}{2} + 2A_2 + A_3 \geqq \frac{p+2a-3}{8} \text{ if } n \text{ is even}$$

$$\frac{-a-1}{2} + 2A_2 + A_3 \geqq \frac{p+2a+5}{8} \text{ if } n \text{ is odd,}$$

and (3) follows.

PROOF OF THEOREM 1. By Lemmas 2.1 and 2.2, G is 3-transitive, $R \in G$ and q is an odd permutation. By Lemma 1.2 (A) and the fact that p is an A-prime, we get that $R^{24} \neq 1$. Let μ be the minimal degree of G. In order to prove the theorem, it is sufficient to show that degree $R^{24} < (p+1)/3$, since then $\mu < (p+1)/3$ or $3\mu < p+1$, which implies $3\mu \leqq p$ hence $3\mu < p$.

Therefore, by the theorem of Bochert [1, p. 185], G contains AL_p. But $q \in G$ is an odd permutation, hence $G = S_p$. We have to prove only that degree $R^{24} < (p+1)/3$. By Lemmas 1.2 (B) and 1.3 of Section 1, we obtain that R^{24} leaves at least θ symbols of $GF(p)$ fixed, where

$$\theta = \begin{cases} \dfrac{2A_0}{2} + \dfrac{4A_1}{2} + \dfrac{6(A_2-1)}{2} + 3 + \dfrac{8A_3}{2} & \text{(in Case (a), Section 1)} \\[2ex] \dfrac{2A_0}{2} + \dfrac{4A_1}{2} + \dfrac{6A_2}{2} + \dfrac{8A_3}{2} & \text{(in Case (b), Section 1)} \\[2ex] \dfrac{2(A_0-1)}{2} + 1 + \dfrac{4A_1}{2} + \dfrac{6A_2}{2} + \dfrac{8(A_3-1)}{2} + 4 & \text{(in Case (c), Section 1).} \end{cases}$$

Therefore $\theta = A_0 + 2A_1 + 3A_2 + 4A_3$. We use Lemma 2.3 to obtain $\theta = A_0 + 2A_1 + 3(A_2 + \frac{1}{2}A_3) + \frac{5}{2}A_3$, and

$$\theta \geqq \begin{cases} \dfrac{11p + 10a - 45}{16} + \dfrac{5}{2} A_3 & \text{if } n \text{ is even} \\[2ex] \dfrac{11p + 10a - 5}{16} + \dfrac{5}{2} A_3 & \text{if n is odd.} \end{cases}$$

Therefore:

$$\text{degree } R^{24} \leqq p - \theta \leqq \begin{cases} \dfrac{5p - 10a + 45}{16} - \dfrac{5}{2} A_3 & \text{if } n \text{ is even} \\[2ex] \dfrac{5p - 10a + 5}{16} - \dfrac{5}{2} A_3 & \text{if } n \text{ is odd.} \end{cases}$$

Assume n is even. Then we have to prove that

$$\frac{5p-10a+45}{16}-\frac{5}{2}A_3<\frac{p+1}{3}.$$

Suppose not. Then

$$p \leqq 119-30a-120A_3 \tag{7}$$

and

$$p \leqq 119-30a. \tag{8}$$

But $|a| < \sqrt{p}$; therefore, (8) implies that $p \leqq 119+30\sqrt{p}$, hence $p < 1156$. By listing all primes $p = 4n+1$, n is even, $p < 1156$, we see that only the following satisfy (8): 17, 73, 113, 137, 193, 241, 593, 617, 673, 977 (e.g, if $p = 97 = 9^2 + 4^2$, hence $a = 9$ and (8) is not satisfied). Therefore p must be one of these. The prime 17 is not an A-prime, but Theorem 1 holds for $p = 17$ by [5]. If $p = 113$, then $6 \in A_3$, $29 \in A_3$. If $p = 137$, then $6 \in A_3$, $58 \in A_3$. If $p = 193$, then $22 \in A_3$, $47 \in A_3$. If $p = 241$, then $7 \in A_3$, $95 \in A_3$. If $p = 593$, then $57 \in A_3$, $63 \in A_3$. If $p = 617$, then $6 \in A_3$, $13 \in A_3$. If $p = 673$, then $11 \in A_3$, $47 \in A_3$. If $p = 977$, then $6 \in A_3$, $55 \in A_3$. (These can be checked by indices table). We see that if p is from the list above and $p \neq 17, 73$, then $A_3 \geqq 2$. But if $x \in A_3$, then $-(x+4) \in A_3$; therefore, $A_3 \geqq 4 > 3$. (For every p in the list we have shown $x, y \in A_3$ such that $x \not\equiv -(x+4), x \not\equiv -(y+4)$). But p satisfies (7), hence $p < 119 - 30a - 360$, which implies $p < 30\sqrt{p} - 241$ which is impossible. Thus $p = 73$, and $22 \in A_3$, $(-26) \in A_3$; thus, $A_3 \geqq 2$. As $73 = 3^2 + 8^2$, $a = -3$ and consequently 73 does not satisfy (7), a contradiction.

Assume now that n is odd and $p \neq 29$. We must show that

$$\frac{5p-10a+5}{16}-\frac{5}{2}A_3<\frac{p+1}{3}.$$

Suppose not. Then

$$p \leqq -30a-1-120A_3 \quad \text{and} \quad p \leqq 30\sqrt{p}-1-120A_3 \tag{9}$$

and

$$p \leqq -30a-1. \tag{10}$$

Hence $p \leqq 30\sqrt{p}-1$, which implies $p < 900$. By listing all primes $p = 4n+1$, n is odd, $p<900$, $p \neq 29$, we see that only the following satisfy (10): 5, 61, 173, 181, 269, 293, 389, 541, 661. Thus p must be one of them. The prime 5 is not an A-prime. If $p = 61, 181, 541, 661$, then $\pm 2 \in A_3$. (Here -2 stands for $p-2$.)

If $p = 173$, then $-2 \in A_3$, $82 \in A_3$. If $p = 269$, then $-2 \in A_3$, $3 \in A_3$. If $p = 293$, then $-2 \in A_3$, $23 \in A_3$. If $p = 389$, then $-2 \in A_3$, $43 \in A_3$. Hence $A_3 \geqq 2$ and by (9) we get $p \leqq 30\sqrt{p} - 241$ which is impossible. Again, this is a contradiction.

If $p = 29$, then $A_0 = 7$, $A_1 = 4$, $A_2 = 0$, $A_3 = 1$, $A_4 = 2$ and $A_k = 0$, $k > 4$. Hence 29 is an A-prime as $A_4 \neq 0$. Degree $R^{24} \leqq p - A_0 - 2A_1 - 3A_2 - 4A_3 = 10$. Therefore, $\mu \leqq 10$ (μ is the minimal degree of G). If $\mu < 10 = (p+1)/3$, then we finish as in the cases above. Thus we can assume $\mu = 10$ which yields degree $R^{24} = 10$. But $2 \in A_0$, $10 \in A_0$, $11 \in A_0$, $14 \in A_0$, $17 \in A_0$, $18 \in A_0$, $26 \in A_0$; $8 \in A_1$, $12 \in A_1$, $15 \in A_1$, $19 \in A_1$; $27 \equiv -2 \in A_3$; $3 \in A_4$, $21 \in A_4$. Therefore, using Lemmas (1.2), (1.3), and the fact that $3 \in A_4$, we obtain: $R^{24} = (3, 4, 5, 6, 7, 21, 22, 23, 24, 25)^{24}$. Hence $(R^{24})^5 = R^{120} = 1$. We conclude that $\mu = 10$, and G contains a permutain of degree μ and of order 5. By [6, p. 646] and $\mu = 10 < (29/2)(1 - 1/5) - 2/5$, we get that G contains AL_{29}, and $G = S_p$, as q is an odd permutation. The theorem is proved.

3. Other groups satisfying (P^{**})

We shall prove that in some cases, the list of forbidden k's in the definition of A-prime can be shortened and Theorem 1 still holds.

Definition. Let p be a prime of the form $p = 4n + 1$ and let a be the odd base of p. We shall say that p is an A^* prime if: (i) n is even and $-\infty < a < 19$ or n is odd and $-\infty < a < 23$, and (ii) There exists $k \neq 0, 1, 2, 3, 5$ such that $A_k \neq 0$.

Theorem 2. *If p is an A^*-prime and G satisfies (p^{**}), then G coincides with S_p.*

Proof. By Theorem 1, we can assume $A_k = 0$, $k \neq 0, 1, 2, 3, 5, 11$. By the definition of A^*-prime, we must have $A_{11} \neq 0$, and by the results of Section 1, we get $R^{12} \neq 1$, $R^8 \neq 1$ in all cases. As in Theorem 1, we must show only that degree $R^{12} < (p+1)/3$ or degree $R^8 < (p+1)/3$. By assumption, using (1), (2), (i) and (ii) of Lemma 2.3, we get:

$$A_2 + A_3 + A_5 + A_{11} = \begin{cases} \dfrac{p+2a-3}{8} & \text{if } n \text{ is } \textit{even} \\ \\ \dfrac{p+2a+5}{8} & \text{if } n \text{ is odd} \end{cases} \tag{1*}$$

and

$$3A_2 + 4A_3 + 6A_5 + 12A_{11} = \begin{cases} \dfrac{p+a}{2} & \text{if } n \text{ is even} \\[2ex] \dfrac{p+a+4}{2} & \text{if } n \text{ is odd .} \end{cases} \tag{2*}$$

Subtracting three times (1*) from (2*) yields:

$$A_3 + 3A_5 + 9A_{11} = \begin{cases} \dfrac{p-2a+9}{8} & \text{if } n \text{ is even} \\[2ex] \dfrac{p-2a+1}{8} & \text{if } n \text{ is odd.} \end{cases} \tag{3*}$$

Assume n is even. By Section 1, as in the proof of Theorem 1, we obtain that R^{12} leaves at least $A_0 + 2A_1 + 3A_2 + 6A_5$ symbols of $GF(p)$ fixed. Therefore, degree $R^{12} \leqq p - (A_0 + 2A_1 + 3A_2 + 6A_5) = (p+a)/2 - 3A_2 - 6A_5$ (Lemma 2.3). If this number is less than $(p+1)/3$, the theorem follows. Therefore, it can be assumed that $(p+a)/2 - 3A_2 - 6A_5 \geqq (p+1)/3$, which implies that $3A_2 + 6A_5 \leqq (p+3a-2)/6$. By (2*) we get $(p+a)/2 = 3A_2 + 4A_3 + 6A_5 + 12A_{11} \leqq (p+3a-2)/6 + 4A_3 + 12A_{11}$, which implies that

$$4A_3 + 12A_{11} \geqq \frac{p+1}{3}. \tag{4*}$$

As before, we obtain that R^8 leaves at least $A_0 + 2A_1 + 4A_3$ symbols of $GF(p)$ fixed. Therefore, degree $R^8 \leqq p - (A_0 + 2A_1 + 4A_3) = (p+a)/2 - 4A_3$. We shall now show that this number is less than $(p+1)/3$. If not, $4A_3 \leqq (p+3a-2)/6$. By (4*), we get $(p+1)/3 \leqq 4A_3 + 12A_{11} \leqq (p+3a-2)/6 + 12A_{11}$ which implies that $9A_{11} \geqq (p-3a+4)/8$. By (3*) we get $(p-2a+9)/8 = 9A_{11} + A_3 + 3A_5 \geqq A_3 + 3A_5 + (p-3a+4)/8$ which implies $A_3 + 3A_5 \leqq (a+5)/8$. If $s(3) = +$, then $p = 24m + 1$ and the theorem holds by Corollary 2. Thus, we may assume $s(3) = -$, and then $-3 \in A_5 \geqq 1$. Therefore, $A_3 \leqq (a+5)/8 - 3 = (a-19)/8 < 0$ as $a < 19$, a contradiction.

If n is odd, we get (Lemmas (1.2) and (1.3)) that R^{12} leaves at least $A_0 + 2A_1 + 3A_2 + 6A_5 + 4$ symbols of $GF(p)$ fixed. Hence (Lemma 2.3), degree $R^{12} \leqq (p - (A_0 + 2A_1 + 3A_2 + 6A_5 + 4)) = (p+a+4)/2 - 3A_2 - 6A_5 - 4$. If this number is less than $(p+1)/3$, the theorem follows. Thus we can assume that $(p+a+4)/2 - 3A_2 - 6A_5 - 4 \geqq (p+1)/3$ which implies $3A_2 + 6A_5 \leqq (p+3a-14)/6$. By (2*), we get

$$4A_3 + 12A_{11} \geqq \frac{p+13}{3}. \tag{5*}$$

As before, we see (using Section 1) that degree $R^8 \leqq p - (A_0 + 2A_1 + 4A_3) = (p+a+4)/2 - 4A_3$. We must show that this number is less than $(p+1)/3$. Suppose it is not. Then $4A_3 \leqq (p+3a+10)/6$ and by (5*) we get $9A_{11} \leqq (p-3a+16)/8$. Substituting this into (3*) implies that $A_3 + 3A_5 \leqq (a-15)/8$. But $A_3 \neq 0$ since $-2 \in A_3$; therefore $3A_5 \leqq (a-15)/8-1 = (a-23)/8 < 0$, as $a < 23$, a contradiction.

Definition. Let p be a prime of the form $p = 24n + 17$ and let a be the odd base of p. We shall say that p is an A^{**}-prime if $a < 19$ and there exists $k \neq 0,1,2,5$ such that $A_k \neq 0$.

Theorem 3. *If p is an A^{**}-prime and G satisfies (p^{**}), then G coincides with S_p.*

Proof. By Theorem 2, we can assume $A_k = 0$, $k \neq 0,1,2,3,5$. By definition of A^{**}-prime, we must have $A_3 \neq 0$. Also, $-3 \in A_5 \neq 0$ as $s(2) = +$, $s(3) = -$. Hence, Section 1 (a) yields that $R^8 \neq 1$ and $R^{12} \neq 1$. As in Theorem 2, we must show only that degree $R^8 < (p+1)/3$ or degree $R^{12} < (p+1)/3$. As in the proof of Theorem 2, in the case that n is even, we get degree $R^8 \leqq (p+a)/2 - 4A_3$. If this number is less than $(p+1)/3$, the theorem follows; therefore, we assume that $(p+a)/2 - 4A_3 \geqq (p+1)/3$ which implies that $4A_3 \leqq (p+3a-2)/6$.

As in the proof of Theorem 2, we obtain that degree $R^{12} \leqq (p+a)/2 - 3A_2 - 6A_5$. Assume $p \neq 17, 41$; then $(p+a)/2 - 3A_2 - 6A_5 < (p+1)/3$ as required, because otherwise $4A_3 + 12A_{11} \geqq (p+1)/3$ (which follows as (4*) in the proof of Theorem 2). But $A_{11} = 0$; hence, $(p+3a-2)/6 \geqq 4A_3 \geqq (p+1)/3$ which implies that $p \leqq 3a - 4 < 53$ (as $a < 19$), contradicting $p \neq 17, 41$. If $p = 17$, the theorem holds by [5]. If $p = 41$, $A_5 \geqq 1$ as $-3 \in A_5$, $A_2 \geqq 2$ as $3 \in A_2, -6 \in A_2$. Therefore, degree $R^{12} \leqq (p+a)/2 - 3A_2 - 6A_5 \leqq (41+5)/2 - 6 - 6 = 11 < (p+1)/3 = 14$.

Hence the theorem holds for $p = 41$. (We note that 41 is an A^{**}-prime as $7 \in A_3 \neq 0$, as $A_k = 0$, but 41 is neither an A-prime nor an A^*-prime, as $A_k = 0, k \neq 0,1,2,3,5$.)

Remark. If $p = 4n + 1$ is a specific prime, then we know all A_k's and can make better approximation of degree R^{24}, R^{12}, R^8, as we did for $p=41$. Examples of A^{**}-primes are primes of the form: $a < 19$ and $p = (4q)^{2^n} + 1$, $q = 1,5,7,11,23,35,37$, as can be checked.

REFERENCES

1. A. Bochert, *Übet die Classe der transitiven Substitutionengruppen*, Math. Ann. **40** (1892) 176–193.
2. A. Brauer, *Über Sequenzen von Potenzresten*, Akad. Wiss. Berlin, Sitz 1928, 9–16.
3. S. Chowla, *The Riemann Hypothesis and Hilbert's Tenth Problem*, Blackie and Son Ltd., London and Glasgow, 1965.
4. B. Huppert, *Endliche Gruppen*, Springer - Verlag, Berlin - Heidelberg - New York, 1967.
5. N. Ito, *On transitive permutation groups of Fermat prime degree*, Proc. Int. Conf. Theory of Groups. Austr. Natl. Univ. Canberra, 1965, 191–202.
6. W. A. Manning, *The degree and class of multiply transitive groups* II, Trans. Amer. Math. Soc. **31** (1929) 643–653.
7. I. M. Vinogradov, *Elements of Number Theory*, Dover Publication, Inc., 1954.
8. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York and London.

DEPARTMENT OF MATHEMATICAL SCIENCES
TEL AVIV UNIVERSITY