

TRANSITIVE PERMUTATION GROUPS OF DEGREE

$p = 2q + 1, p$ AND q BEING PRIME NUMBERS. III

BY
NOBORU ITO

Introduction. Let p be a prime number such that $q = \frac{1}{2}(p - 1)$ is also a prime number. Let Ω be the set of symbols $1, \dots, p$, and let \mathfrak{G} be a nonsolvable transitive permutation group on Ω . In a previous paper [6] the following theorem has been established: If \mathfrak{G} is not triply transitive, then \mathfrak{G} is isomorphic to either $LF(2, 7)$ with $p = 7$ or $LF(2, 11)$ with $p = 11$, where $LF(2, l)$ denotes the linear fractional group over the field of l elements. Now the purpose of this work is to improve this theorem as follows, namely, the following theorem will be proved.

THEOREM. *If \mathfrak{G} is not quadruply transitive, then \mathfrak{G} is isomorphic to $LF(2, 5)$ with $p = 5$ or $LF(2, 7)$ with $p = 7$ or $LF(2, 11)$ with $p = 11$.*

Hence, in particular, if $p > 11$, then \mathfrak{G} is quadruply transitive.

The main idea of the proof given below is quite similar to that of [5], [6]. Therefore we use the same notation as in [6]. First of all, in order to prove the theorem, likewise in [6, Introduction], we can assume that (i) $p > 11$; (ii) \mathfrak{G} is simple; (iii) let \mathfrak{P} be a Sylow p -subgroup of \mathfrak{G} and let $Ns\mathfrak{P}$ be the normalizer of \mathfrak{P} in \mathfrak{G} . Then $Ns\mathfrak{P}$ has order pq ; and (iv) let \mathfrak{Q} be a Sylow q -subgroup of \mathfrak{G} . Then \mathfrak{Q} has order q and the cycle structure of a permutation ($\neq 1$) of \mathfrak{Q} consists of two q -cycles. Let $Cs\mathfrak{Q}$ and $Ns\mathfrak{Q}$ be the centralizer and the normalizer of \mathfrak{Q} and \mathfrak{G} , respectively. Then $Cs\mathfrak{Q} = \mathfrak{Q}$. Let the order of $Ns\mathfrak{Q}$ be equal to qr . Then r divides $q - 1$. Let \mathfrak{R} be a Sylow q -complement of $Ns\mathfrak{Q}$. Then \mathfrak{R} is cyclic of order r . We put $q - 1 = rs$.

X_0 , X_0^q and X_{00} denote irreducible characters of the symmetric group \mathfrak{S} over Ω , whose values are given by $\alpha(S) - 1$, $\frac{1}{2}\{\alpha(S) - 1\}\{\alpha(S) - 2\} - \beta(S)$ and $\frac{1}{2}\alpha(S)\{\alpha(S) - 3\} + \beta(S)$, respectively, where $\alpha(S)$ and $\beta(S)$ denote the number of symbols of Ω fixed by S and the number of transpositions in the cycle structure of S , respectively. Moreover, $(X, Y)(X, Y = A, B, C, D)$ denotes an irreducible character of \mathfrak{G} which has p -type X and q -type Y . By a theorem of Frobenius [6, Proposition A] \mathfrak{G} is quadruply transitive, if and only if X_0^q restricted on \mathfrak{G} and X_{00} restricted on \mathfrak{G} are irreducible. Now \mathfrak{G} will be assumed to be triply transitive [6, Theorem] but not quadruply transitive. Then it will be shown that X_0^q restricted on \mathfrak{G} is irreducible (Lemma 7) and that the decomposition of X_{00} restricted on \mathfrak{G} into its irreducible components has the following form:

Received by the editors March 23, 1964.

$$X_{00} = \sum_{i=1}^s (D, C)_i,$$

where $(D, C)_i$'s ($i = 1, \dots, s$) are q -exceptional characters of \mathfrak{G} and have degree rp (Lemma 6). Herein we get $s > 1$, because we have supposed that \mathfrak{G} is not quadruply transitive. Furthermore, by a theorem of Brauer [6, Proposition B]

$$(*) \quad (D, C)_1(G) = \frac{1}{s} \left[\frac{1}{2} \alpha(G) \{ \alpha(G) - 3 \} + \beta(G) \right]$$

is a rational integer for every q -regular element G of \mathfrak{G} , which imposes a strong restriction on the cycle structure of permutations of \mathfrak{G} because of $s > 1$.

Now using a theorem of Frame [6, Proposition G] we show that a representation corresponding to $(D, C)_i$ ($i = 1, \dots, s$) can be realized in the real number field (Lemma 8), which implies that r is even (Lemma 9). Hence let I be the involution in \mathfrak{R} .

Finally we apply an idea somewhat similar to Fryer [3]. Namely, we identify Ω with $GF(p)$, the field of p elements. Let P be an element ($\neq 1$) of \mathfrak{P} . Then we will find convenient analytic representations for P and I (Lemma 10). By means of these analytic representations we can verify the existence of a permutation of \mathfrak{G} (a word of P and I) which contradicts (*). But our present method requires the inspection of many words, though all of them have the form IP^a , where a is an integer.

1. Decompositions of X_0^0 restricted on \mathfrak{G} and X_{00} restricted on \mathfrak{G} .

LEMMA 1. *There are only four possible cases of the decomposition of X_0^0 restricted on \mathfrak{G} into the irreducible characters of \mathfrak{G} :*

- (i) X_0^0 restricted on \mathfrak{G} is irreducible.
- (ii) $X_0^0 = (A, B) + (D, A)$, where the degrees of (A, B) and (D, A) are equal to $(q - 2)p + 1$ and p , respectively.
- (iii) $X_0^0 = \sum_{i=1}^s (A, C)_i + (B, A) + \sum_{i=1}^{s-2} (B, D)_i$, where the degrees of $(A, C)_i$ ($i = 1, \dots, s$), (B, A) and $(B, D)_i$ ($i = 1, \dots, s - 2$) are equal to $(r - 1)p + 1$ with $\delta_q = -1$ [6, Proposition B], $2p - 1$ and $p - 1$, respectively.
- (iv) $X_0^0 = \sum_{i=1}^s (A, C)_i + (D, A) + \sum_{i=1}^{s-1} (B, D)_i$, where the degrees of $(A, C)_i$ ($i = 1, \dots, s$), (D, A) and $(B, D)_i$ ($i = 1, \dots, s - 1$) are equal to $(r - 1)p + 1$ with $\delta_q = -1$, p and $p - 1$, respectively.

Proof. (Cf. [5], Lemma 5.) Since $X_0^0(P) = 1$, by a theorem of Brauer [6, Proposition B] an irreducible character of \mathfrak{G} of p -type A or p -type C with $\delta_p = 1$ must appear as an irreducible part of X_0^0 restricted on \mathfrak{G} . Then inspecting the degree table in [6] we see that no irreducible character of p -type C with $\delta_p = 1$ can appear. Now if it is (A, D) , then we get (i). If it is (A, B) , then it is easy to see that we get (ii). Hence let us assume that it has type

(A, C) . Since X_0^0 is a rational character, the whole family of the characters of q -type C will appear as irreducible parts of X_0^0 restricted on \mathfrak{G} . Now inspecting the degree table in [6] we see that $\delta_q = -1$ and that they have degree $(r-1)p+1$ and multiplicity 1. Thus we have that

$$X_0^0(X) = \sum_{i=1}^s (A, C)_i(X) + \dots$$

for every permutation X of \mathfrak{G} , where the part \dots does not contain $(A, C)_i$ ($i = 1, \dots, s$) any more. By a theorem of Brauer [6, Proposition B] we have that $\sum_{i=1}^s (A, C)_i(P) = s$. Therefore irreducible characters of \mathfrak{G} of p -type B or p -type C with $\delta_p = -1$ must appear in the part \dots with the sum of multiplicities at least $s-1$. But the sum of degrees of the part \dots equals $(s-1)(p-1)+p$. Hence, checking up the degree table in [6] we see that no character of p -type C with $\delta_p = -1$ can appear, and that only characters of type (B, D) with degree $p-1$ except just one character (B, A) with degree $2p-1$ or (D, A) with degree p can appear.

Let \mathfrak{H} be the maximal subgroup of \mathfrak{G} leaving the symbol 1 of Ω fixed. Let Y_0 be the character of \mathfrak{H} whose values are given by $\alpha(X) - 2$ for every permutation X of \mathfrak{H} . Then since \mathfrak{H} is doubly transitive by a previous result [6, Theorem], Y_0 is an irreducible character of \mathfrak{H} . Let Y_0^* be the character of \mathfrak{G} induced by Y_0 . Then by a theorem of Frobenius [6, Formula (11)] we have that

$$(\#) \quad Y_0^*(X) = X_0(X) + X_0^0(X) + X_{00}(X)$$

for every permutation X of \mathfrak{G} .

Now let us assume that some (B, D) appears in the part \dots with multiplicity $v > 1$. Then by $(\#)$ and by the reciprocity theorem of Frobenius we have that

$$(B, D)(X) = vY_0(X) + \dots$$

for every permutation X of \mathfrak{H} . For $X = 1$ this gives that $p-1 = v(p-2) + \dots$, which is obviously a contradiction. Thus if (B, A) appears, then we get (iii). If (D, A) appears, then we get (iv).

LEMMA 2. *There are only four possible cases of the decomposition of X_{00} restricted on \mathfrak{G} into the irreducible characters of \mathfrak{G} :*

- (i) X_{00} restricted on \mathfrak{G} is irreducible.
- (ii) $X_{00} = (A, B) + (B, D)$, where the degrees of (A, B) and (B, D) are equal to $(q-2)p+1$ and $p-1$, respectively.
- (iii) $X_{00} = \sum_{i=1}^s (A, C)_i + \sum_{i=1}^s (B, D)_i$, where the degrees of $(A, C)_i$ ($i = 1, \dots, s$) and $(B, D)_i$ ($i = 1, \dots, s$) are equal to $(r-1)p+1$ with $\delta_q = -1$ and $p-1$, respectively.

(iv) $X_{00} = \sum_{i=1}^s (D, C)_i$, where the degree of $(D, C)_i$ ($i = 1, \dots, s$) is equal to rp with $\delta_q = -1$.

Proof. (Cf. [5, Lemma 6].) Let Q be an element of \mathfrak{G} of order q . Since $X_{00}(Q) = -1$, by a theorem of Brauer [6, Proposition B] an irreducible character of \mathfrak{G} of q -type B or q -type C with $\delta_q = -1$ must appear as an irreducible component of X_{00} restricted on \mathfrak{G} . If it has q -type B , then we see from the degree table in [6] that it is an (A, B) with degree $(q-2)p+1$ or a (D, B) with degree $(q-1)p$. If it is a (D, B) , then we get (i). If it is an (A, B) , then we get (ii). Now let us assume that it has q -type C with $\delta_q = -1$. Then since X_{00} is a rational character, the whole family of the q -exceptional characters of \mathfrak{G} must appear as irreducible components of X_{00} restricted on \mathfrak{G} . Again by inspecting the degree table in [6], we see that they are of type (A, C) with degree $(r-1)p+1$ or (D, C) with degree rp . If they are of type (D, C) , we get (iv). Hence let us assume that they are of type (A, C) . Then from the degree table in [6] we see that they have multiplicity 1. Thus we obtain that

$$X_{00}(X) = \sum_{i=1}^s (A, C)_i(X) + \dots$$

for every permutation X of \mathfrak{G} , where the part \dots does not contain $(A, C)_i$ ($i = 1, \dots, s$) any more. By a theorem of Brauer [6, Proposition B] we have that $\sum_{i=1}^s (A, C)_i(P) = s$. Therefore irreducible characters of \mathfrak{G} of p -type B or p -type C with $\delta_p = -1$ must appear in the part \dots with the sum of multiplicities at least s . But the sum of degrees of the part \dots equals $s(p-1)$. Hence from the degree table in [6] we see that only characters of type (B, D) with degree $p-1$ can appear. The rest of the proof is the same as in Lemma 1.

LEMMA 3. *Neither of X_0^0 restricted on \mathfrak{G} nor X_{00} restricted on \mathfrak{G} contains (B, D) of degree $p-1$ as its irreducible component.*

Proof. (Cf. [5, Lemma 7].) By (#) and by the reciprocity theorem of Frobenius we have that

$$(B, D)(X) = Y_0(X) + L(X)$$

for every permutation X of \mathfrak{G} , where L is a linear character of \mathfrak{G} . Since \mathfrak{G} is triply transitive by a previous result [6, Theorem]. By a theorem of Frobenius [6, Proposition A] X_0 is orthogonal to both X_0^0 restricted on \mathfrak{G} and X_{00} restricted on \mathfrak{G} . Hence we have that $(B, D) \neq X_0$. Let $1_{\mathfrak{G}}$ and $1_{\mathfrak{F}}$ be principal characters of \mathfrak{G} and \mathfrak{F} , respectively. Let $1_{\mathfrak{F}}^*$ be the character of \mathfrak{G} induced by $1_{\mathfrak{F}}$. Then we have that

$$1_{\mathfrak{F}}^* = X_0 + 1_{\mathfrak{G}}.$$

Thus (B, D) restricted on \mathfrak{G} does not contain $1_{\mathfrak{G}}$ as its irreducible component. Thus we have that $L \neq 1_{\mathfrak{G}}$. Let L^* be the character of \mathfrak{G} induced by L . Then by the reciprocity theorem of Frobenius we have that

$$L^*(X) = (B, D)(X) + M(X)$$

for every permutation X of \mathfrak{G} , where M is a linear character of \mathfrak{G} . Since $L \neq 1_{\mathfrak{G}}$, we have that $M \neq 1_{\mathfrak{G}}$. Since \mathfrak{G} is assumed to be simple, this is a contradiction.

From Lemmas 1, 2 and 3 we get

LEMMA 4. *Case (iv) of Lemma 1 and Cases (ii) and (iii) of Lemma 2 cannot occur. Similarly, Case (iii) of Lemma 1 cannot occur if $s > 2$.*

LEMMA 5. *Case (iii) of Lemma 1 cannot occur.*

Proof. Let us assume that this case occurs. Then by Lemmas 2, 3 and 4 we obtain that $s = 2$ and that X_{00} restricted on \mathfrak{G} is irreducible. Let \mathfrak{R} be the subgroup of \mathfrak{G} consisting of all the permutations in \mathfrak{G} each of which fixes each of the symbols 1 and 2 of Ω . Let $1_{\mathfrak{R}}$ be the principal character of \mathfrak{R} and $1_{\mathfrak{R}}^*$ be the character of \mathfrak{G} induced by $1_{\mathfrak{R}}$. Then by a theorem of Frobenius [6, Formula (8)] we have that

$$(**) \quad 1_{\mathfrak{R}}^*(X) = 1_{\mathfrak{G}}(X) + 2X_0(X) + X_0^0(X) + X_{00}(X)$$

for every permutation X of \mathfrak{G} . Thus the norm of $1_{\mathfrak{R}}^*$ is nine.

Let $(\Omega)_2$ be the set of all the ordered pairs (x, y) such that x and y are different symbols of Ω . We represent \mathfrak{G} as a permutation group $\pi(\mathfrak{G})$ on $(\Omega)_2$. Since \mathfrak{G} is assumed to be simple, this permutation representation of \mathfrak{G} is faithful. The character of $\pi(\mathfrak{G})$ is equal to $1_{\mathfrak{R}}^*$. It is known [2, §207] that the number of orbits of \mathfrak{R} as a subgroup of $\pi(\mathfrak{G})$ equals the norm of $1_{\mathfrak{R}}^*$. Put $\Gamma = \Omega - \{1, 2\}$. $(\Gamma)_2$ is to be understood likewise, $(\Omega)_2$. Then it is easy to see that $(\Gamma)_2$ is divided into three orbits Γ_i ($i = 1, 2, 3$) of \mathfrak{R} as a subgroup of $\pi(\mathfrak{G})$. Since \mathfrak{G} is triply transitive on Ω by a previous result [6, Theorem], \mathfrak{R} is transitive on Γ . Hence each Γ_i ($i = 1, 2, 3$) contains an ordered pair of the form $(3, *)$. Furthermore, since \mathfrak{G} is triply transitive, we can choose \mathfrak{R} so that \mathfrak{R} fixes the symbols 1, 2 and 3 of Ω individually. Let us consider the act of \mathfrak{R} on the set of ordered pairs of the form $(3, *)$ of Γ_i ($i = 1, 2, 3$). Then it is easy to see that the length of Γ_i ($i = 1, 2, 3$) is equal to $(p-2)rx_i$ with $x_1 + x_2 + x_3 = 4$. This implies that just one of x_i ($i = 1, 2, 3$) is equal to 2 and the other two are equal to 1. Then by a theorem of Frame [6, Proposition F] the number

$$F = \frac{\{p(p-1)\}^7(p-2)^4(p-2)^3r^32}{(p-1)^4\frac{1}{2}p(p-3)\{(r-1)p+1\}^2(2p-1)}$$

is a rational integer. Dividing F by $p^6 q^3$ we obtain that

$$F_1 = \frac{(p-2)^7 r^2 8}{\{(r-1)p+1\}^2(2p-1)}$$

is a rational integer. Since $(p-2, 2p-1) = 3$ and since r is prime to 3, we can put $2p-1 = 3^a A$ with $1 \leq a \leq 7$ and $(A, 3) = 1$. Since $(p-3, 2p-1)$ divides 5, we can put $A = 5^b B$ with $0 \leq b \leq 2$ and $(B, 5) = 1$. Then we have that $B = 1$ and $2p-1 = 3^a 5^b$. Since $2p \equiv 2 \pmod{4}$, a must be even: $a = 2a_1$. If $b = 2b_1$ is even, then we have that

$$2p-2 = 4q = (3^{a_1} 5^{b_1} + 1)(3^{a_1} 5^{b_1} - 1),$$

which is obviously a contradiction. Thus b is odd and hence $b = 1$. This implies that $p = 23$ or 1823 , which is a contradiction to a result of Parker and Nikolai [7].

LEMMA 6. *Case (iv) of Lemma 2 occurs.*

Proof. Let us assume that X_{00} restricted on \mathfrak{G} is irreducible. If X_0^0 restricted on \mathfrak{G} is irreducible, too, then by a theorem of Frobenius [6, Proposition A] \mathfrak{G} is quadruply transitive on Ω against the assumption. Hence Case (ii) of Lemma 1 must occur. Let $Ns\mathfrak{R}$ be the normalizer of \mathfrak{R} in \mathfrak{G} . Let $1_{Ns\mathfrak{R}}$ be the principal character of $Ns\mathfrak{R}$ and let $1_{Ns\mathfrak{R}}^*$ be the character of \mathfrak{G} induced by $1_{Ns\mathfrak{R}}$. Then by a theorem of Frobenius [6, formula (9)] we have that

$$(\# \#) \quad 1_{Ns\mathfrak{R}}^*(X) = 1_{\mathfrak{G}}(X) + X_0(X) + X_{00}(X)$$

for every permutation X of \mathfrak{G} . Thus by $(**)$ and $(\# \#)$ the norms of $1_{\mathfrak{G}}^*$ and $1_{Ns\mathfrak{R}}^*$ are equal to 8 and 3, respectively.

Let $\{\Omega\}_2$ be the family of all the subsets of Ω each of which consists of two different symbols of Ω . We represent \mathfrak{G} as a permutation group $\pi\{\mathfrak{G}\}$ on $\{\Omega\}_2$. Since \mathfrak{G} is simple, this permutation representation of \mathfrak{G} is faithful. The character of $\pi\{\mathfrak{G}\}$ is equal to $1_{Ns\mathfrak{R}}^*$. It is known [2, §207] that the number of orbits of $Ns\mathfrak{R}$ as a subgroup of $\pi\{\mathfrak{G}\}$ equals the norm of $1_{Ns\mathfrak{R}}^*$. $\{\Gamma\}_2$ is to be understood likewise, $\{\Omega\}_2$. Then it is easy to see that $(\Gamma)_2$ is divided into two orbits Γ_1 and Γ_2 of \mathfrak{R} as a subgroup of $\pi(\mathfrak{G})$ and that $Ns\mathfrak{R}$ as a subgroup of $\pi\{\mathfrak{G}\}$ is transitive on $\{\Gamma\}_2$. Then by the proof of Lemma 4 of [6] the lengths of Γ_1 and Γ_2 are equal to each other and hence it is equal to $\frac{1}{2}(p-2)(p-3)$. By a theorem of Frame [6, Proposition F], the number

$$F = \frac{\{p(p-1)\}^6 (p-2)^4 \frac{1}{4} (p-2)^2 (p-3)^2}{(p-1)^4 \frac{1}{2} p(p-3)p\{(q-2)p+1\}}$$

is a rational integer. Since $(p-2, (q-2)p+1) = 1$, dividing F by

$$p^4 4q^2(p-2)^6,$$

we obtain that

$$F_1 = \frac{(p-3)}{2\{(q-2)p+1\}}$$

is a rational integer, which is obviously a contradiction.

As we already have noticed in the introduction, using a theorem of Brauer [6, Proposition B] we get the following important formula from Lemma 6:

$$(*) \quad (D, C)_1(G) = \frac{1}{s} \left[\frac{1}{2} \alpha(G) \{ \alpha(G) - 3 \} + \beta(G) \right]$$

for every q -regular element G of \mathfrak{G} .

Now let us consider $\pi\{\mathfrak{G}\}$. The character of $\pi\{\mathfrak{G}\}$ is equal to $1_{Ns\mathfrak{R}}$. By $(\# \#)$ and by Lemma 6 the decomposition of $1_{Ns\mathfrak{R}}$ into its irreducible components has the following form:

$$(i) \quad 1_{Ns\mathfrak{R}} = 1_{\mathfrak{G}} + X_0 + \sum_{i=1}^s (D, C)_i.$$

Moreover, let Δ be an orbit of $Ns\mathfrak{R}$ as a subgroup of $\pi\{\mathfrak{G}\}$ with length x . Let $C(\Delta)$ be the commuter of $\pi\{\mathfrak{G}\}$ as the permutation matrix group corresponding to Δ . Using Schur's lemma we can reduce $C(\Delta)$ to a diagonal form:

$$\left\{ \begin{array}{ccc} p-1 \text{ times} & rp \text{ times} & rp \text{ times} \\ a, b, \dots, b, c_1, \dots, c_1, \dots, c_s, \dots, c_s \end{array} \right\},$$

where a, b and c_i ($i = 1, \dots, s$) are algebraic integers. Then using a method Wielandt [8, §29] we see that a and b are rational integers, and furthermore we obtain the following three equalities:

$$(ii) \quad a = x,$$

$$(iii) \quad 0 = a + b(p-1) + rp \sum_{i=1}^s c_i,$$

$$(iv) \quad \frac{1}{2} p(p-1)a = a^2 + b^2(p-1) + rp \sum_{i=1}^s |c_i|^2.$$

LEMMA 7. X_0^0 restricted on \mathfrak{G} is irreducible.

Proof. Let us assume that X_0^0 restricted on \mathfrak{G} is reducible. Then Case (ii) of Lemma 1 occurs. Using (i) and $(**)$ we see that the norms of $1_{Ns\mathfrak{R}}$ and

$1_{\mathfrak{K}}$ are equal to $s + 2$ and $s + 7$, respectively. It is known that the number of orbits of \mathfrak{K} as a subgroup of $\pi(\mathfrak{G})$ and of $Ns\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$ is equal to the norms of $1_{\mathfrak{K}}$ and of $1_{Ns\mathfrak{K}}$, respectively [2, §207]. Hence it is easy to see that $(\Gamma)_2$ is divided into $s + 1$ orbits $\Gamma_1, \dots, \Gamma_{s+1}$ of \mathfrak{K} as a subgroup of $\pi(\mathfrak{G})$. Let x_i be the length of Γ_i ($i = 1, \dots, s + 1$). Since \mathfrak{G} is triply transitive by a previous result [6, Theorem], \mathfrak{K} is transitive on Γ . Hence each Γ_i ($i = 1, \dots, s + 1$) contains an ordered pair of the form $(3, *)$. Furthermore, since \mathfrak{G} is triply transitive, we can choose \mathfrak{K} so that \mathfrak{K} fixes the symbols 1, 2 and 3 of Ω individually. Let us consider the act of \mathfrak{K} on the set of ordered pairs of the form $(3, *)$ of Γ_i ($i = 1, \dots, s + 1$). Then it is easy to see $x_i = (p - 2)ry_i$ ($i = 1, \dots, s + 1$) with

$$(v) \quad \sum_{i=1}^{s+1} y_i = 2s.$$

Similarly, $\{\Gamma\}_2$ is divided into s orbits $\Gamma(1), \dots, \Gamma(s)$ of $Ns\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$. By (v) there exist at least two different j 's ($1 = s + 1$) such that $y_j = 1$. Now let us assume that there exist just two such j 's. Then the other $s - 1$ y_j 's must be equal to 2. Now by a theorem of Frame [6, Proposition F] the number

$$F = \frac{\{p(p-1)\}^{s+5}(p-2)^4(p-2)^{s+1}r^{s+1}2^{s-1}}{(p-1)^4p\{(q-2)p+1\}p^sr^s}$$

is a rational integer. Since $(p - 2, (q - 2)p + 1) = 1$, dividing F by

$$p^4q^{s+1}(p-2)^{s+5}$$

we obtain that

$$F_1 = \frac{2^{2s}r}{(q-2)p+1}$$

is a rational integer. Since $(q - 2)p + 1 = (p - 2)sr - 2$, we have that $(r, (q - 2)p + 1) = 2$. This implies that $(q - 2)p + 1 = 2^A$. If $A = 2B$ is even, then we obtain that $(q - 2)p = (2^B + 1)(2^B - 1)$, which implies that $2^B + 1 > p$. This contradicts that $p = 2q + 1$. But this is a contradiction, because of $q \equiv 2 \pmod{3}$. Thus A must be odd. Then we obtain that $(q - 2)p + 2 \equiv 0 \pmod{3}$. In fact, if $q \equiv 1 \pmod{3}$, then $p \equiv 2q + 1 \equiv 0 \pmod{3}$, and if $q \equiv 3$, then $p = 7$. Therefore we can assume that there must exist at least three different j 's ($1 \leq j \leq s + 1$) such that $y_j = 1$. Then one of such Γ_j 's can be considered as an orbit, say $\Gamma(j)$, of $Ns\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$. Then the length of $\Gamma(j)$ equals $\frac{1}{2}(p - 2)r$. In particular, this implies that r is even. By a previous result [4, Theorem 2] we can assume that $r \geq 4$. Now in the preceding consideration put $\Delta = \Gamma(j)$. Then we have (ii), (iii) and (iv) with $x = \frac{1}{2}(p - 2)r$. From (ii) and (iii) we obtain that $-r - b$

$\equiv 0 \pmod{p}$ and that $4b = yr$ with an odd integer y . Then we can put $b = zp - r$ with an integer z and we obtain that $4zp - 4r = yr$. Thus we can put $4z = wr$ with an odd integer w , and we obtain that $y = wp - 4$. Now from (iv) we obtain that $(4b)^2 = r^2(wp - 4)^2 \leq 4p(p - 2)r$, which implies that $r(wp - 4)^2 \leq 4p(p - 2)$. Thus we see that w must be positive. If $w \geq 3$, then we have that $(3p - 4)^2 \leq 4p(p - 2)/r \leq p(p - 2)$, which implies that $4p^2 + 8 \leq 11p$. This is a contradiction. Thus we must have that $w = 1$ and $4b = rp - 4r = r(p - 4)$. Put this value of b into (iv) and multiply by 16. Then we obtain that

$$4p(p - 1)(p - 2)r = 4(p - 2)^2 r^2 + r^2(p - 4)^2(p - 1) + 16pr \sum_{i=1}^s |c_i|^2.$$

Dividing it by r we obtain that

$$(vi) \quad 4p(p - 1)(p - 2) = 4(p - 2)^2 r + r(p - 4)^2(p - 1) + 16p \sum_{i=1}^s |c_i|^2.$$

From (vi) we see that $r \equiv 0 \pmod{4}$ and $r \not\equiv 0 \pmod{8}$. Put $r = 4r_1$ with an odd natural number r_1 . Then dividing (vi) by 8 we obtain that

$$qp(p - 2) = 2r_1(p - 2)^2 + r_1 q(p - 4)^2 + 2p \sum_{i=1}^s |c_i|^2.$$

If $r_1 \geq 3$, then we obtain that $p(p - 2)/(p - 4)^2 \geq 3$, which implies that $11p \geq p^2 + 24$. This is a contradiction. Thus r_1 must be equal to 1 and $r = 4$.

Now let us consider the irreducible character (D, A) of \mathfrak{G} of degree p in X_0^0 restricted on \mathfrak{G} . Since X_0^0 is rational, (D, A) is rational, too. By (#) we have that

$$(D, A)(X) = Y_0(X) + Z(X)$$

for every permutation X of \mathfrak{S} , where Z is a (reducible) rational character of \mathfrak{S} of degree 2 (cf. 5, Lemma 9). If Z is irreducible, by a theorem of Brauer [6, Proposition B] Z must have q -type C . But then Z cannot be rational. Thus Z is a sum of two linear characters of \mathfrak{S} : $Z = L_1 + L_2$. If $L_1 = L_2$, then let L_1^* be the character of \mathfrak{G} induced by L_1 . Then by the reciprocity theorem of Frobenius, we have that $L_1^* = 2(D, A) + \dots$. Since the degree of L_1^* is equal to p , this is obviously a contradiction. Thus we obtain that $L_1 \neq L_2$. Furthermore, since $1_{\mathfrak{S}} = 1_{\mathfrak{G}} + X_0$, we have that $L_1 \neq 1_{\mathfrak{S}} \neq L_2$ and that L_1 and L_2 must be algebraically conjugate. Let the field of characters L_i ($i = 1, 2$) be the field of m th roots of unity. Then the degree of this field equals $\phi(m) = 2$. Thus we obtain that $m = 3$ or $m = 4$. Let \mathfrak{S}' be the commutator subgroup of \mathfrak{S} . Then the index of \mathfrak{S}' in \mathfrak{S} is divisible by m . By Sylow's theorem we have that $\mathfrak{S} = \mathfrak{S}'Ns\Omega$. Thus the order of $Ns\Omega$ which

equals $4q$ is divisible by m . Thus we obtain that $m = 4$. This implies that \mathfrak{S} contains a subgroup \mathfrak{M} of index 2. Let e be the character of \mathfrak{S} whose kernel is \mathfrak{M} . Let e^* be the character of \mathfrak{G} induced by e . Using a theorem of Brauer and Tuan [6, Proposition C] we see that $e^* = (D, A)_1$ is an irreducible character of \mathfrak{G} , which is different from (D, A) because of $L_i \neq e$ ($i = 1, 2$). Then the first q -block $B_1(q)$ of \mathfrak{G} contains four characters $1_{\mathfrak{G}}$, (D, A) , $(D, A)_1$ and (A, B) . Since $r = 4$, by a theorem of Brauer [1] we must have the following degree equation in $B_1(q)$.

$$1 + p + p = rp + (q - 2)p + 1.$$

This is absurd. Thus X_0 restricted on \mathfrak{G} must be irreducible.

By Lemmas 6 and 7 we have that

$$X_{00}(G) - X_0(G) = 2\beta(G) - 1 = \sum_{i=1}^s (D, C)_i(G) - X_0(G)$$

for every permutation G of \mathfrak{G} . Thus we obtain the following equality:

$$(vii) \quad \sum_{G \in \mathfrak{G}} \{\beta(G)\}^2 = \frac{1}{4} (s + 2)g,$$

where g is the order of \mathfrak{G} .

2. q -exceptional characters $(D, C)_i$ ($i = 1, \dots, s$).

LEMMA 8. *A representation corresponding to $(D, C)_i$ ($i = 1, \dots, s$) can be realized in the real number field.*

Proof. Let e_q be a primitive q th root of unity and let \mathbb{Q} be the rational number field. Then by a theorem of Brauer [1] all the $(D, C)_i$'s ($i = 1, \dots, s$) are $\mathbb{Q}(e_q)$ -conjugate. Thus all the $(D, C)_i$'s ($i = 1, \dots, s$) have the same quadratic signature [6, Introduction]. Now by a theorem of Frame [6, Proposition G] we can count the number R of real orbits of $Ns\mathfrak{R}$ as a subgroup of $\pi\{\mathfrak{G}\}$ in the following way:

$$\begin{aligned} R &= \frac{1}{g} \sum_{G \in \mathfrak{G}} \left[\frac{1}{2} \alpha(G^2) \{\alpha(G^2) - 1\} + \beta(G^2) \right] \\ &= \frac{1}{g} \sum_{G \in \mathfrak{G}} \left[\frac{1}{2} \{\alpha(G) + 2\beta(G)\} \{\alpha(G) + 2\beta(G) - 1\} + 2\delta(G) \right] \end{aligned}$$

where $\delta(G)$ denotes the number of 4-cycles in the cycle structure of G as a permutation of \mathfrak{G} . Then using (vii) we obtain that

$$R = \frac{1}{2} s + 2 + \frac{2}{g} \sum_{G \in \mathfrak{G}} \delta(G).$$

On the other hand, we have that $R = 2 + \epsilon s$, where $\epsilon = 1, 0$ or -1 , according as $(D, C)_i$'s ($i = 1, \dots, s$) have the quadratic signature 1, 0 or -1 , respectively. Comparing with two expressions of R we obtain that $\epsilon = 1$.

LEMMA 9. r is even.

Proof. Let Q be an element of \mathfrak{G} of order q . Since by Lemma 8 $(D, C)_i$'s are real characters, we obtain that $(D, C)_i(Q) = (D, C)_i(Q^{-1})$ ($i = 1, \dots, s$). Then using a theorem of Brauer [6, Proposition B] we see that $X(Q) = X(Q^{-1})$ for every irreducible character X of \mathfrak{G} . Thus Q and Q^{-1} are conjugate in \mathfrak{G} . Therefore r is even.

Now let P be an element ($\neq 1$) of \mathfrak{P} . Let Q be an element in $N_s \mathfrak{P}$ of order q . Let I be an involution such that $IQI = Q^{-1}$, whose existence is secured by Lemma 9.

3. **Analytic representations for P and I .** Now we identify Ω with $GF(p)$. Then we choose $x' = x + 1$ as an analytic representation for P . We can put $Q^{-1}PQ = P^{a^2}$, that is, $PQ = QP^{a^2}$, where a is a certain primitive root modulo p . Since P is transitive on $GF(p)$, we can assume that Q fixes the element 0 of $GF(p)$. Let $f(x)$ be an analytic representation for Q . Then we have that $f(x+1) = f(x) + a^2$. From this we see that $x' = a^2x$ is an analytic representation for Q . Then Q transfers squares and nonsquares in $GF(p)$ to squares and nonsquares in $GF(p)$, respectively. Since $IQI = Q^{-1}$, I fixes the element 0 of $GF(p)$. Since Q is transitive on the set of nonzero squares in $GF(p)$, we can assume that I fixes the element 1 of $GF(p)$. Let $g(x)$ be an analytic representation for I . Then using $IQ = Q^{-1}I$ we obtain that $a^2g(x) = g(a^{-2}x)$. Taking $x = 1$ we obtain that $a^2 = g(a^{-2})$ and recurrently $a^{2i} = g(a^{-2i})$. Similarly we obtain that $g(a^{-2i-1}) = a^2g(a^{-2i+1})$. From these equalities we see that

$$x' = \begin{cases} 1/x & \text{if } x \text{ is a nonzero square in } GF(p), \\ a^2/x & \text{if } x \text{ is a nonsquare in } GF(p) \end{cases}$$

is an analytic representation for I .

Now we notice that because of $p = 2q + 1$, -1 is a nonsquare in $GF(p)$ and every square in $GF(p)$ other than 0 and 1 is a square of some primitive root modulo p . Thus replacing Q by its suitable power, we see that a can be any primitive root modulo p . Therefore we obtain the following lemma.

LEMMA 10. Take $x' = x + 1$ as an analytic representation for P . Then

$$x' = \begin{cases} 1/x & \text{if } x \text{ is a nonzero square in } GF(p), \\ b/x & \text{if } x \text{ is a nonsquare in } GF(p) \end{cases}$$

is an analytic representation for I , where b ($\neq 0, 1$) is any square in $GF(p)$.

Let us consider the permutation IP^c in \mathfrak{G} , where c is a nonzero square in $GF(p)$. Using Lemma 10 the analytic representation of IP^c can be described as follows: (I) $x' = (1 + cx)/x$ if $x \neq 0$ is a square in $GF(p)$; (II) $x' = (b + cx)/x$ if x is a nonsquare in $GF(p)$; (III) $0' = c$. Similarly, the analytic representation of $(IP^c)^2$ can be described as follows: (IV) $x' = \{x + c(1 + cx)\}/(1 + cx)$ if $x \neq 0$ and $1 + cx$ are squares in $GF(p)$, where $1 + cx \neq 0$ because c and x are squares in $GF(p)$ and -1 is a nonsquare in $GF(p)$; (V) $x' = \{bx + c(1 + cx)\}/(1 + cx)$ if $x \neq 0$ is a square in $GF(p)$ and if $1 + cx$ is a nonsquare in $GF(p)$; (VI) $x' = \{x + c(b + cx)\}/(b + cx)$, if x and $b + cx$ are nonsquares in $GF(p)$; (VII) $x' = \{bx + c(b + cx)\}/(b + cx)$, if x is a nonsquare in $GF(p)$ and if $b + cx \neq 0$ is a square in $GF(p)$; (VIII) $0' = 1/c$; (IX) $(-b/c)' = c$.

4. The case where 2 is a nonsquare in $GF(p)$. Let m be a square in $GF(p)$. Then we denote by \sqrt{m} the quadratic residual solution, namely, the solution which is a square in $GF(p)$, of the equation $x^2 = m$.

Since $p \equiv -1 \pmod{3}$, using the quadratic reciprocity law we see that 3 is a square in $GF(p)$.

LEMMA 11. *We can assume that 13 is a nonsquare in $GF(p)$.*

Proof. Let us assume that 13 is a square in $GF(p)$. Take $b = -2$ in Lemma 10 and consider IP^3 with $c = 3$. At first we show that $\alpha(IP^3) = 2$. Let us assume that $x' = x$ in (I). Then we get $x^2 = 1 + 3x$. Hence we obtain that $x = \frac{1}{2}(3 \pm \sqrt{13})$. Since $\frac{1}{2}(3 + \sqrt{13})(3 - \sqrt{13}) = -1$, just one of the solutions is a square in $GF(p)$. Let us assume that $x' = x$ in (II). Then we get $x^2 = 3x - 2$, which implies that $x = 2$. Next we show that $\beta(IP^3) = 0$. In order to do this we have only to show that any element of $GF(p)$ which is fixed by $(IP^3)^2$ is already fixed by IP^3 . Herein we want to notice that the solutions $x' = x$ of (IV) and of (VII) are coincident with those of (I) and (II), respectively. In fact, let us assume that $x' = x$ in (IV). Then we get $x + cx^2 = x + c(1 + cx)$. Dividing this by c we obtain that $x^2 = 1 + cx$. Let us assume that $x' = x$ in (VII). Then we get $bx + cx^2 = bx + c(b + cx)$. Dividing this by c we obtain that $x^2 = b + cx$. Therefore we need consider only (V) and (VI). Let us assume that $x' = x$ in (V). Then we get $x + 3x^2 = -2x + 3(1 + 3x)$, which implies that $(x - 1)^2 = 2$. This is a contradiction, because we have assumed that 2 is a nonsquare in $GF(p)$. The same holds on (VI).

Now from (*) we obtain that $DC_1(IP^3) = -1/s$, which must be an integer. But since we have assumed that $s > 1$, this is a contradiction.

LEMMA 12. *We can assume that 5 is a nonsquare and 7 is a square in $GF(p)$.*

Proof. At first let us assume that 5 is a square and 7 is a nonsquare in $GF(p)$. Take $b = -2$ in Lemma 10 and consider IP with $c = 1$. Likewise,

in Lemma 11 we can show that $\alpha(IP) = 2$ and $\beta(IP) = 0$. In fact let us assume that $x' = x$ in (I). Then we get $x^2 = 1 + x$. Hence we obtain that $x = \frac{1}{2}(1 \pm \sqrt{5})$. Since $\frac{1}{4}(1 + \sqrt{5})(1 - \sqrt{5}) = -1$, just one of the solutions is a square in $GF(p)$. Let us assume that $x' = x$ in (II). Then we get $x^2 = -2 + x$. Hence we obtain that $x = \frac{1}{2}(1 \pm \sqrt{-7})$. Since $\frac{1}{4}(1 + \sqrt{-7})(1 - \sqrt{-7}) = 2$, just one of the solutions is a nonsquare in $GF(p)$. Now let us assume that $x' = x$ in (V). Then we get $x + x^2 = -2x + 1 + x$, which implies that $(x + 1)^2 = 2$. This is a contradiction. The same holds on (VI). Therefore using (*) we obtain the same contradiction as in Lemma 11.

Next let us assume that both 5 and 7 are squares or nonsquares in $GF(p)$. Then we get $\alpha(IP) = 1$ and $\beta(IP) = 0$. In order to get a contradiction from (*) we only have to know that IP is q -regular. Now IP is really q -regular, because the cycle structure of IP contains a 3-cycle $(0, 1, 2)$.

LEMMA 13. *If 13 is a nonsquare and if 7 is a square in $GF(p)$, then there exists a permutation in G contradicting (*).*

Proof. Take $b = 4$ in Lemma 10 and consider IP^c with $c^2 = 12$ in $GF(p)$. We show that $\alpha(IP^c) = 2$ and $\beta(IP^c) = 0$. In fact, let us assume that $x' = x$ in (I). Then we get $x^2 = -1 + cx$. Hence we obtain that $x = \frac{1}{2}c \pm 2$. Since $(\frac{1}{2}c + 2)(\frac{1}{2}c - 2) = -1$, just one of the solutions is a square in $GF(p)$. Let us assume that $x' = x$ in (II). Then we get $x^2 = 4 + cx$. Hence we obtain that $x = \frac{1}{2}c \pm \sqrt{7}$. Since $(\frac{1}{2}c + \sqrt{7})(\frac{1}{2}c - \sqrt{7}) = -4$, just one of the solutions is a nonsquare in $GF(p)$. Now let us assume that $x' = x$ in (V). Then we get $x + cx^2 = 4x + c + 12x$, which implies that $\{x - (5c/8)\}^2 = 91/16 = 7.13/16$. By assumption this is a contradiction. The same holds on (VI).

5. The case where 2 is a square in $GF(p)$. The idea of the proof in this case is almost the same as in §4. The elements 2 and 3 are squares in $GF(p)$. At first we show that the elements 5, 7, 11, 13 and 17 can be assumed as squares in $GF(p)$. Then the key lemma (Lemma 19), which is also quite elementary, shows that under these circumstances we can assume that all the elements in $GF(p)$ are squares in $GF(p)$, which is obviously an absurdity.

LEMMA 14. *We can assume that 17 is a square in $GF(p)$.*

Proof. Let us assume that 17 is a nonsquare in $GF(p)$. Take $b = 4$ in Lemma 10 and consider IP^c with $c^2 = 8$. We show that $\alpha(IP^c) = 2$ and $\beta(IP^c) = 0$. Let us assume that $x' = x$ in (I). Then we get $x^2 = cx + 1$. Hence we obtain that $x = \frac{1}{2}c \pm \sqrt{3}$. Since $(\frac{1}{2}c + \sqrt{3})(\frac{1}{2}c - \sqrt{3}) = -1$, just one of the solutions is a square in $GF(p)$. Let us assume that $x' = x$ in (II). Then we get $x^2 = cx + 4$. Hence we obtain that $x = \frac{1}{2}c \pm \sqrt{6}$. Since $(\frac{1}{2}c + \sqrt{6})(\frac{1}{2}c - \sqrt{6}) = -4$, just one of the solutions is a nonsquare in $GF(p)$. Let us assume that $x' = x$ in (V). Then we get $cx^2 - 3x = c + 8x$,

which implies that $\{x - (11c/16)\}^2 = 153/32 = 9.17/32$. This is a contradiction. The same holds on (VI).

LEMMA 15. *We can assume that 13 is a square in $GF(p)$.*

Proof. Let us assume that 13 is a nonsquare in $GF(p)$. Take $b = 3$ in Lemma 10 and consider IP^2 with $c = 2$. We show that $\alpha(IP^2) = 2$ and $\beta(IP^2) = 0$. Let us assume that $x' = x$ in (I). Then we get $x^2 = 1 + 2x$. Hence we obtain that $x = 1 \pm \sqrt{2}$. Since $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$, just one of the solutions is a square in $GF(p)$. Let us assume that $x' = x$ in (II). Then we get $x^2 = 3 + 2x$. Hence we obtain that $x = -1$. Let us assume that $x' = x$ in (V). Then we get $2x^2 + x = 3x + 2(1 + 2x)$, which implies that $\{x - (3/2)\}^2 = 13/4$. This is a contradiction. The same holds on (VI).

LEMMA 16. *We can assume that 5 is a square in $GF(p)$.*

Proof. Using Lemma 15, let 13 be a square in $GF(p)$. Let us assume that 5 is a nonsquare in $GF(p)$. Take $b = 4$ in Lemma 10 and consider IP^3 with $c = 3$. We show that $\alpha(IP^3) = 2$ and $\beta(IP^3) = 0$. Let us assume that $x' = x$ in (I). Then we get $x^2 = 3x + 1$. Hence we obtain that $x = \frac{1}{2}(3 \pm \sqrt{13})$. Since $\frac{1}{4}(3 + \sqrt{13})(3 - \sqrt{13}) = -1$, just one of the solutions is a square in $GF(p)$. Let us assume that $x' = x$ in (II). Then we get $x^2 = 3x + 4$. Hence we obtain that $x = -1$. Let us assume that $x' = x$ in (V). Then we get $3x^2 + x = 4x + 3(1 + 3x)$, which implies that $(x - 2)^2 = 5$. This is a contradiction. The same holds on (VI).

LEMMA 17. *We can assume that 11 is a square in $GF(p)$.*

Proof. Using Lemma 16 let 5 be a square in $GF(p)$. Let us assume that 11 is a nonsquare in $GF(p)$. Take $b = 3$ in Lemma 10 and consider IP^c with $c^2 = 6$. We show that $\alpha(IP^c) = 2$ and $\beta(IP^c) = 0$. Let us assume that $x' = x$ in (I). Then we get $x^2 = 1 + cx$. Hence we obtain that $x = \frac{1}{2}(c \pm \sqrt{10})$. Since $\frac{1}{4}(c + \sqrt{10})(c - \sqrt{10}) = -1$, just one of the solutions is a square in $GF(p)$. Let us assume that $x' = x$ in (II). Then we get $x^2 = 3 + cx$. Hence we obtain that $x = \frac{1}{2}(c \pm 3\sqrt{2})$. Since $\frac{1}{4}(c + 3\sqrt{2})(c - 3\sqrt{2}) = -3$, just one of the solutions is a nonsquare in $GF(p)$. Let us assume that $x' = x$ in (V). Then we get $cx^2 + x = 3x + c(1 + cx)$, which implies that $\{x - (2c/3)\}^2 = 11/3$. This is a contradiction. The same holds on (VI).

LEMMA 18. *We can assume that 7 is a square in $GF(p)$.*

Proof. Using Lemmas 15 and 16 let 5 and 13 be squares in $GF(p)$. Take $b = 2$ in Lemma 10 and consider IP^c with $c^2 = 5$. We show that $\alpha(IP^c) = 2$ and $\beta(IP^c) = 0$. Let us assume that $x' = x$ in (I). Then we get $x^2 = 1 + cx$. Hence we obtain that $x = \frac{1}{2}(c \pm 3)$. Since $\frac{1}{4}(c + 3)(c - 3) = -1$, just one of the solutions is a square in $GF(p)$. Let us assume that $x' = x$ in (II). Then we get $x^2 = 2 + cx$. Hence we obtain that $x = \frac{1}{2}(c \pm \sqrt{13})$. Since

$\frac{1}{4}(c + \sqrt{13})(c - \sqrt{13}) = -2$, just one of the solutions is a nonsquare in $GF(p)$. Let us assume that $x' = x$ in (V). Then we get

$$x + cx^2 = 2x + c(1 + cx),$$

which implies that $\{x - (3c/5)\}^2 = 14/5$. This is a contradiction. The same holds on (VI).

LEMMA 19. *We can assume that every element in $GF(p)$ is a square in $GF(p)$.*

Proof. Let l be the least prime number which is a quadratic nonresidue modulo p . Then by Lemmas 14–18, l is greater than 17. Let us assume that $l \equiv 1 \pmod{3}$. Then take $b = 9$ in Lemma 10 and consider IP^c with $c^2 = l - 16$, where, by assumption, $l - 16$ is a square in $GF(p)$. We show that $\alpha(IP^c) = 2$ and $\beta(IP^c) = 0$. Let us assume that $x' = x$ in (I). Then we get $x^2 = cx + 1$. Since, by assumption, $c^2 + 4 = l - 12$ is a square in $GF(p)$, we obtain that $x = \frac{1}{2}(c \pm (l - 12)^{1/2})$. Since $\frac{1}{4}(c + (l - 12)^{1/2})(c - (l - 12)^{1/2}) = -1$, just one of the solutions is a square in $GF(p)$. Let us assume that $x' = x$ in (II). Then we get $x^2 = cx + 9$. Since we have assumed that $l \equiv 1 \pmod{3}$, $l + 20$ is divisible by 3. If $(l + 20)/3 > l$, then $l < 10$. Thus $(l + 20)/3$ is less than l and therefore it is a square in $GF(p)$. Hence we obtain that $x = \frac{1}{2}(c \pm (l + 20)^{1/2})$. Since $\frac{1}{4}(c + (l + 20)^{1/2})(c - (l + 20)^{1/2}) = -9$, just one of the solutions is a nonsquare in $GF(p)$. Let us assume that $x' = x$ in (V). Then we get $x + cx^2 = 9x + c(1 + cx)$, which implies that $x - \{(l - 8)c/2(l - 16)\}^2 = l(l - 12)/4(l - 16)$. This is a contradiction. The same holds on (VI).

Now let us assume $l \equiv 2 \pmod{3}$. Then take $b = 4$ in Lemma 10 and consider IP^c with $c^2 = l - 9$, where, by assumption, $l - 9$ is a square in $GF(p)$. We show that $\alpha(IP^c) = 2$ and $\beta(IP^c) = 0$. Let us assume that $x' = x$ in (I). Then we get $x^2 = cx + 1$. Since, by assumption, $c^2 + 4 = l - 5$ is a square in $GF(p)$, we obtain that $x = \frac{1}{2}(c \pm (l - 5)^{1/2})$. Since $\frac{1}{4}(c + (l - 5)^{1/2}) \cdot (c - (l - 5)^{1/2}) = -1$, just one of the solutions is a square in $GF(p)$. Let us assume that $x' = x$ in (II). Then we get $x^2 = 4 + cx$. Since we have assumed that $l \equiv 2 \pmod{3}$, $l + 7$ is divisible by 3. If $(l + 7)/3 > l$, then $l < 3$. Thus $(l + 7)/3$ is less than l and therefore it is a square in $GF(p)$. Hence we obtain that $x = \frac{1}{2}(c \pm (l + 7)^{1/2})$. Since $\frac{1}{4}(c + (l + 7)^{1/2})(c - (l + 7)^{1/2}) = -4$, just one of the solutions is a nonsquare in $GF(p)$. Let us assume that $x' = x$ in (V). Then we get $x + cx^2 = 4x + c(1 + cx)$, which implies that $\{x - (l - 6)c/2(l - 9)\}^2 = l(l - 8)/4(l - 9)$. This is a contradiction. The same holds on (VI).

REFERENCES

1. R. Brauer, *On permutation groups of prime degree and related classes of groups*, Ann. of Math. (2) 44(1943), 57-79.
2. W. Burnside, *Theory of groups of finite order*, Cambridge Univ. Press, Cambridge, 1911.

3. K. D. Fryer, *A class of permutation groups of prime degree*, *Canad. J. Math.* 7(1955), 24-34.
4. N. Ito, *A note on transitive groups of degree p* , *Osaka Math. J.* 14(1962), 213-218.
5. ———, *Transitive permutation groups of degree $p = 2q + 1$, p and q being prime numbers*. I, *Bull. Amer. Math. Soc.* 69(1963), 165-192.
6. ———, *Transitive permutation groups of degree $p = 2q + 1$, p and q being prime numbers*. II, *Trans. Amer. Math. Soc.* 113(1964), 454-487.
7. E. T. Parker and P. J. Nikolai, *A search for analogues of the Mathieu groups*, *Math. Comp.* 12(1958), 38-43.
8. H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.

NAGOYA UNIVERSITY,
NAGOYA, JAPAN