ON UNSOLVABLE GROUPS OF DEGREE $p = 4q + 1$, p AND q PRIMES

K. I. APPEL AND E. T. PARKER

1. This paper presents two results. They are:

THEOREM 1. *Let G be a doubly transitive permutation group of degree $nq + 1$ where q is a prime and $n < q$. If G is neither alternating nor symmetric, then G has Sylow q-subgroup of order only q.*

RESULT 2. *There is no unsolvable transitive permutation group of degree $p = 29, 53, 149, 173, 269, 293,$ or 317 properly contained in the alternating group of degree p.*

Result 2 was demonstrated by a computation on the Illiac II computer at the University of Illinois.

2. Proof of Theorem 1. Let G_1 and G_2 be largest subgroups of G fixing respectively one and two of the letters. G_2 is of index $(nq + 1)nq$ in G, so that G is of order divisible by q. A Sylow q-subgroup Q of G therefore does not fix two letters. Since the index of G_1 in G is relatively prime to q, Q fixes one letter; let 0 be the letter fixed by Q. Since G is of degree less than q^2, Q is a subdirect product of n q-cycles.

Assume now that the conclusion of the theorem is false. Then Q has at least two independent generators in the direct product of the n q-cycles. There must then be in Q a product of powers of two independent generators which is not the identity and fixes all letters of at least one of the q-cycles. Let Q_1 be the maximal subgroup of Q fixing the letters of a given q-cycle associated with Q. Choose another of these q-cycles, whose letters are not fixed by all the elements of Q_1. Let Q_2 be the maximal subgroup of Q fixing the letters of this latter q-cycle; Q_2 is of index q in Q, and hence is not merely the identity. Both Q_1 and Q_2 are maximal subgroups of Q; hence their union is Q. It follows that none of the nq letters displaced by Q is fixed by all the elements of both Q_1 and Q_2. Let x and y be letters displaced by Q and fixed by all elements of Q_1 and Q_2, respectively; let H_1 and H_2 be the largest subgroups of G fixing 0 and x, 0 and y, respectively. Then Q_1 is a Sylow q-subgroup of H_1 and Q_2 is a Sylow q-subgroup of H_2. Let N be the normalizer in G of Q_1; since G is doubly transitive, N acts doubly transitively on the set of all letters fixed by Q_1 **(2**, Theorem 5.7.1**)**.

Let $A(N)$ be the doubly transitive component of N permuting all those letters fixed by Q_1 ("component" is used as a substitute for the "transitive

Received February 18, 1966 and, in revised form, March 10, 1966.

constituent'' used by such authors as Burnside; cf. **(5)**). $A(N)$ is a homomorphic image of N; and hence a Sylow subgroup of the former is a homomorphic image of a Sylow subgroup of the latter. Since $A(N)$ is doubly transitive of degree congruent to 1 (mod q), $A(N)$ is of order divisible by q, and accordingly has a Sylow q-subgroup fixing some letter. Since $A(N)$ is transitive, $A(N)$ has a Sylow q-subgroup fixing any letter chosen in advance. Let Q^* be the (group theoretic) union of all Sylow q-subgroups of N. Let A be the component (or perhaps, for the moment, subdirect product of more than one component) of Q^* permuting those letters fixed by Q_1. Each Sylow q-subgroup of $A(N)$ is a Sylow q-subgroup of A by the construction of Q^*. Thus A has more than one Sylow q-subgroup. It follows that A is not a q-group, so that A has an element of order prime to q. $A(N)$, being doubly transitive, is primitive. A is a non-trivial normal subgroup of $A(N)$ so that A must be transitive. This ensures in turn (by taking a conjugate of our initial choice if necessary) that A has an element S of order prime to q displacing 0.

Let $B(Q^*)$ be the homomorphic image of Q^* permuting the set of letters displaced by Q_1. Regarded as a permutation group on its displaced letters, Q_1 is a subgroup of $B(Q^*)$. Since N is the normalizer in G of Q_1, and Q^* is contained in N, we have Q_1 normal in Q^* and hence in $B(Q^*)$. By the inequality on the degree of G, $B(Q^*)$ can have no element of order q^2; hence Q_1 is a subdirect product of $m < n < q$ q-cycles. Since each letter permuted by $B(Q^*)$ is displaced by Q_1, each of these q-cycles appears non-trivially in some element of Q_1. Thus conjugation by any element of $B(Q^*)$ must transform each of these q-cycles into a power either of itself or of another of the q-cycles. An element ω of order q of $B(Q^*)$ cannot transform $m < q$ sets non-trivially among themselves, since q is prime; thus ω must transform each q-cycle into a power of itself. Furthermore a q-cycle cannot be transformed into any of its powers other than itself by an element of order q. Thus ω must transform each of the m q-cycles into itself, and in turn permute with each generator of Q_1. Hence ω must be a product of powers of the q-cycles forming Q_1. But $B(Q^*)$ is generated by Q_1 and elements of order q such as ω and hence is an abelian q-group.

Let S' be a pre-image of S under the homomorphism taking Q^* onto A. Then, since as noted above, the component $B(Q^*)$ of Q^* on the letters not permuted by A is abelian, the element $\alpha = (S')^q$ has the following two properties:

(i) α displaces 0;

(ii) α fixes all letters displaced by Q_1.

Carrying out the same argument with Q_2 in the role of Q_1, it is established that G has an element β such that β displaces 0 and β fixes all letters displaced by Q_2. Since Q_1 and Q_2 have no fixed letter in common other than 0, α and β displace only 0 in common. Each of α and β has a unique cycle displacing 0; call these $(0a_1 \ldots a_s)$ and $(0b_1 \ldots b_t)$ respectively, where the sets of a's and b's are disjoint. Any other pair of cycles of α and β, respectively, displace no common letter, and hence cancel out in the commutator $\alpha\beta\alpha^{-1}\beta^{-1}$. Thus

$\alpha\beta\alpha^{-1}\beta^{-1}$

$= (0a_1\, a_2 \ldots a_{s-1}\, a_s)(0b_1\, b_2 \ldots b_{t-1}\, b_t)(0a_s\, a_{s-1} \ldots a_2\, a_1)\ (0b_t\, b_{t-1} \ldots b_2\, b_1)$.

One checks that $0 \to b_t \to a_s \to 0$. But any a_i, $1 \leqslant i < s$, and any b_j, $1 \leqslant j < t$, is fixed by the commutator. Thus denial of the conclusion has led to construction of a 3-cycle. G, being primitive, therefore contains the alternating group **(1**, p. 207**)**. The theorem is proved.

3. Let $p = 4q + 1$, p and q primes, $q > 3$. We wish to decide whether there exists an unsolvable transitive permutation group G of degree p other than A_p and S_p (the alternating and symmetric groups of degree p). Should such a group exist containing odd permutations, then this G has an unsolvable subgroup of index two consisting of the even permutations of G. For this reason there is no essential loss of generality in restricting G to be a subgroup of A_p.

A transitive group of degree p is of order divisible by p, and in turn has an element of order p. This element must be a cycle on all p letters. Since all the cycles of degree p are conjugate in S_p, one may select one of these as a generator of G. It is convenient to consider the p letters permuted by G as residue classes (mod p). The simple form for a generator **a** of order p of G is then $x \to x + 1 \pmod{p}$.

S_p has Sylow p-subgroup of order only p (p prime); hence **a** must generate a Sylow p-subgroup P of G. We now use an important theorem of Burnside **(1**, p. 327**)**: If a finite group G has a Sylow p-subgroup in the centre of its normalizer in G, then G has commutator subgroup of order prime to p. Should the hypothesis of Burnside's theorem be satisfied for the Sylow p-subgroup of G, the commutator subgroup of G would be intransitive (for a transitive group of degree p is of order divisible by p). However, a transitive group of prime degree is primitive and a primitive group can have no non-trivial intransitive normal subgroup. Thus one would conclude in this situation that G is abelian (in fact, cyclic of order p) and in turn solvable. Since P is abelian, the only alternative is that G have an element **b** in the normalizer, but not in the centralizer of this Sylow subgroup.

If H is a group of prime degree p with a normal subgroup of order p, then up to conjugacy in S_p of residue classes (mod p), H is generated by **a** and **b**, which are respectively $x \to x + 1 \pmod{p}$ and $x \to tx \pmod{p}$, $t \not\equiv 0$ or $1 \pmod{p}$. The order of H is then np, where n is a divisor of $p - 1$ and is the order of **b**. For G of degree $p = 4q + 1$, n is a divisor of $4q$. Using the restriction that G be contained in A_p, it may be assumed that n is a divisor of $2q$; for the other elements **b** are odd permutations. N. Ito **(3)** has shown by deep methods that a transitive permutation group of prime degree p, a Sylow p-subgroup of which has normalizer of order $2p$, is solvable unless p is a Fermat prime. No integer of the form $4q + 1$, q prime, is a Fermat prime. Thus we conclude that unsolvable G of the type under discussion must have normalizer of its Sylow p-subgroup divisible by pq. G must include the element **b**: $x \to r^4x \pmod{p}$ where r is a primitive root of p. The residue class 0 is fixed by **b**, and

the other residue classes are permuted in cycles of length q; one of these cycles is transitive on the quartic residues of p, and the others on cosets thereof in the multiplicative group of the field of order p.

An unsolvable transitive permutation group of prime degree is doubly transitive **(1)**. Theorem 1 thus applies immediately when $q > 3$; $\mathbf{b}$ generates a Sylow q-subgroup Q of G. We now apply the theorem of Burnside to Q. If Q is in the centre of its normalizer, then the commutator subgroup of G must be solvable and, in turn, G must be solvable. Since Q is cyclic, G must have an element $\mathbf{c}$ such that $\mathbf{c}$ does not commute with $\mathbf{b}$ but transforms $\mathbf{b}$ into a power of itself. As pointed out above, it is superfluous to consider other than even permutations for choices of $\mathbf{c}$.

A Sylow p-subgroup of G has no such element $\mathbf{c}$ in its normalizer. Thus $\mathbf{a}$ and $\mathbf{c}$ must generate a group with more than one Sylow p-subgroup. A solvable group has a normal elementary abelian subgroup. The only possibility for a normal abelian subgroup of a primitive group of degree p is that this subgroup be of order p. However, any normal subgroup of $\{\mathbf{a}, \mathbf{c}\}$ of order divisible by p contains all Sylow p-subgroups, so it cannot be abelian. Thus $\{\mathbf{a}, \mathbf{c}\}$ is unsolvable, and in fact must contain $\mathbf{b}$ by the arguments above. We let G henceforth be $\{\mathbf{a}, \mathbf{c}\}$. While it is plausible than an unsolvable group of the sort under discussion might not be generated by only two such permutations $\mathbf{a}$ and $\mathbf{c}$, any minimal example for a given degree must have this property. The search process is made more efficient by restricting attention to candidates for minimal examples of groups of interest. Further, in restricting the search to potential minimal extensions of $\{\mathbf{a}, \mathbf{b}\}$ we may assume that $\mathbf{c}$ is of prime order.

Designate the four sets of q residue classes each permuted transitively by the cycles of $\mathbf{b}$ as W, X, Y, Z, including respectively r, r^2, r^3, and r^4 (r a primitive root of p). Each of the four sets is mapped by $\mathbf{c}$ either onto itself or onto another one of the sets. There is a basic dichotomy in the form of the permutation $\mathbf{c}$, according as $\mathbf{c}$ maps each of the sets W, X, Y, and Z onto itself or induces a permutation of these sets. In the first case, $\mathbf{c}$ fixes exactly one symbol in each set, and transforms each cycle of $\mathbf{b}$ into its tth power where $\mathbf{c}^{-1}\mathbf{b}\mathbf{c} = \mathbf{b}^t$. Specifying t and the ordered quadruple $(w, x, y, z) \pmod q$ of symbols fixed by $\mathbf{c}$ in the respective cycles of $\mathbf{b}$ determines $\mathbf{c}$. (In our notation for ordered quadruples, an i in position j denotes the fact that r^{4i+j} is the fixed symbol in the jth cycle, $j = 1, 2, 3, 4$.)

When $\mathbf{c}$ is specified by t and $(w, x, y, z) \pmod q$, $\{\mathbf{a}, \mathbf{c}\}$ is determined by the order of $\mathbf{c}$ and the quadruple. This is the case since two elements $\mathbf{c}$ of equal order and the same quadruple of fixed symbols generate the same group with $\mathbf{b}$. Thus, for a given $(w, x, y, z) \pmod q$ and a given prime order of $\mathbf{c}$, one need consider only one $\mathbf{c}$ and equivalently one exponent t. Transforming by the permutation $g: x \to rx \pmod p$ reduces the number of $\mathbf{c}$ to consider, for $\mathbf{g}^{-1}\mathbf{a}\mathbf{g} = \mathbf{a}^r$ so that $\{\mathbf{a}, \mathbf{c}\}$ and $\{\mathbf{a}, \mathbf{g}^{-1}\mathbf{c}\mathbf{g}\}$ are conjugate in S_p. Transforming $\mathbf{c}$ by $\mathbf{g}^4$ replaces (w, x, y, z) by $(w + 1, x + 1, y + 1, z + 1)$. Repeated transformations of $\mathbf{c}$ by $\mathbf{g}^4$ permits normalization of $\mathbf{c}$ to have zero in a chosen one

of the positions. Transformation of $\mathbf{c}$ by $\mathbf{g}$ sends (w, x, y, z) into $(z + 1, w, x, y)$. Thus, the fixed set case for $\mathbf{c}$ requires consideration of only one representative of each equivalence class under the above transformations for each prime order of $\mathbf{c}$ dividing $q - 1$.

In case $\mathbf{c}$ permutes non-trivially the sets W, X, Y, Z, $\mathbf{c}$ must have order 2 or 3. Let $\mathbf{c}$ be of order 3 with appropriate exponent t specified. Transforming $\mathbf{c}$ by $1, \mathbf{g}, \mathbf{g}^2, \mathbf{g}^3$ allows one the liberty of specifying which set, say Z, is fixed. Transforming further by powers of $\mathbf{g}^4$ permits further normalization of $\mathbf{c}$ in that it may be assumed that $\mathbf{c}$ fixes the symbol 0 in set Z.

There are two essentially distinct classes of cases, depending on whether $\mathbf{c}$ permutes the sets $(W, X, Y)(Z)$ or $(W, Y, X)(Z)$, the "forward" or "backward" cases. In the "forward" case, $\mathbf{c}$ fixes the initial symbol in the cycle of $\mathbf{b}$ on Z and maps the cycle onto its tth power. The cycle on W is mapped onto the tth power of the cycle on X, likewise for X and Y, Y and W. For the "backward" case, the roles of X and Y are reversed. For either of these, $\mathbf{c}$ is fully determined (assuming symbol 0 is fixed in Z) by specifying the map under $\mathbf{c}$ of symbol 0 in set W, and the map in turn of that symbol. This requires two parameters (mod q) for each of the two types of permutations $\mathbf{c}$.

If $\mathbf{c}$ is of order 2 and permutes the sets W, X, Y, Z non-trivially, then $\mathbf{c}$ either transposes all four sets in two pairs, or transposes two sets and fixes two. In the latter case, however, $\mathbf{c}$ would consist of $q + (q - 1)$ transpositions and hence not be in A_p. For $\mathbf{c}$ transposing the four sets in two pairs, there are two essentially distinct cases. The first of these is for $\mathbf{c}$ mapping $(W, X)(Y, Z)$, the pairs of sets "adjacent" in the 4-cycle generated by r. The other alternative is $(W, Y)(X, Z)$ with pairs "opposite." The other pattern of two pairs of transpositions on the sets, $(W, Z)(Y, X)$, is seen to be equivalent under conjugation by $\mathbf{g}$ to $(W, X)(Y, Z)$. In each case, $\mathbf{c}$ is fully determined by specifying the image under $\mathbf{c}$ of the symbol 0 in the set W. This requires just one parameter for each type of permutation $\mathbf{c}$.

Let π be an element of G. Suppose π is a permutation consisting of an r-cycle, r prime, and a non-empty collection of cycles of length relatively prime to r. If m is the product of the lengths of the cycles of length prime to r, then π^m is an r-cycle contained in G. Since G is a subgroup of A_p, $r \geqslant 3$, and G is $(p - r + 1)$-ply transitive **(1**, p. 207**)**. But then G contains A_p **(4)**. Hence, if $\{\mathbf{a}, \mathbf{c}\}$ contains a permutation of the type described above, it must be A_p. Since the principal theorem above is due to Netto, we shall say that a group containing such an element π satisfies Netto's criterion.

4. The computer program prepared to verify Result 2 sequentially constructs all the necessary elements $\mathbf{c}$ described above and then examines permutations of the form $\mathbf{ca}^j$ to determine whether any of these permutations satisfy Netto's criterion. The program and the various checks which were performed to attempt to ensure its correctness will be explained in some detail.

In terms of complexity, the major subroutine of the program was the check

on the Netto criterion. Because most of the actual computation time was spent in the subroutine, an attempt was made to make it relatively efficient. The subroutine was presented the permutation π in the form of p words in locations C to $C + p - 1$ of the form $(C + i, C + \pi(i), 0, 0)$ (Illiac II is a machine which employs quarter words for its fixed point computations and so this format was rather natural.) The basic loop consisted of starting with a word $(C + i, C + \pi(i), 0, 0)$ marking it with a -1 in the fourth quarter word, adding one to the cycle length count, and checking to see if the word in location $C + \pi(i)$ is marked (in which case the cycle is complete). We are indebted to Professor C. W. Gear for suggesting a method of utilizing the six words of extra high-speed memory of Illiac II to avoid memory references to obtain instructions and greatly increase the efficiency of this loop.

In a special tabular region P prepared as part of the program, the odd numbers less than 800 are each assigned a quarter word, the number $n = 8i + 2j + 1$ $(0 \leqslant j \leqslant 3)$ is assigned the $(j + 1)$st quarter word of word i of P. If n is prime, its assigned word contains its primitive root (any positive entry would do, but the primitive root was used in another subroutine), and if it is composite it is assigned the negative number (in the 13 bit two's complement quarter word arithmetic of Illiac II)

$$2^{12} + \sum_{i=0}^{11} 2^i a_{i+1}$$

where, for $1 \leqslant i \leqslant 11$, $a_i = 1$ if p_i divides n (where $p_1 = 3$) and $a_{12} = 1$ if some prime larger than $p_{11}(37)$ divides n. This enables us to find all the odd prime divisors of any number less than 800 by first shifting to eliminate powers of 2 and then picking off the small divisors without performing any division. For prime divisors exceeding 37, the situation is somewhat more complicated, but their infrequent occurrence makes it feasible to treat them somewhat less efficiently.

A region T is used to keep track of the prime occurrences in cycle lengths. The positions in T correspond to those in P and for each cycle of π if the length is prime, one is added to the corresponding quarter word in T; while if a prime r occurs as a factor in the length of cycle of π, two is added to the corresponding quarter word in T. After all cycles of π have been traced, T is examined for any entries of one corresponding to odd primes smaller than p and if any such occurs, the group under consideration is eliminated.

Since the effective operation of this subroutine is clearly central to the program, and since it would be difficult to check it fully in the main program, it was checked by a routine which gave it various permutations π and made sure not only that they were properly accepted or rejected, but also that the region T had the appropriate entries. We feel that this subroutine is correct.

The other subroutine of interest is the routine which creates permutations **c**. First, we create the cycles of **b**. For $p = 4q + 1$, p, q, prime $p > 16$, 2 must have order q, $2q$, or $4q$ and since 2 is not a quadratic residue of p, 2 is a primitive

root of p. Hence the construction of **b** was straightforward. Since $p = 4q + 1$, p, q prime, $q > 2$, implies $q \equiv 1 \pmod 6$, $p \equiv 5 \pmod{24}$, in particular, 2 and 3 divide $q - 1$; hence for every degree considered, elements **c** of orders 2 and 3 appeared. For some of these degrees larger prime orders for **c** also appeared. We shall consider in detail the construction of **c** fixing the sets W, X, Y, Z. First, we note that by the normalization procedure we may consider quadruples $(w, x, y, 0) \pmod q$. Furthermore $(w, x, y, 0)$ is equivalent to $(1, w, x, y)$, which in turn is equivalent to $(1 - y, w - y, x - y, 0)$, which will be called a shift of $(w, x, y, 0)$. Hence quadruples $(w, x, y, 0)$ are generated in lexicographic order and a quadruple is discarded if any of its three shifts lexicographically precedes it. (The lexicographic discard section of each routine was isolated and checked with some care.) When a quadruple is accepted, using a table of powers of the least primitive root of q and indices $\pmod q$, the permutation **c** is constructed.

The construction of **ca** is quite trivial since if the image of i under **c** is $\pi(i)$, the image of i under **ca** is $\pi(i) + 1 \pmod p$.

Although $p = 13$ does not satisfy all of the requirements on p we have given, the program was written to process degree 13 (not requiring a **c** of order 3). For 13, two outputs, one of which was a pair of generators for LF(3, 3) and the other of which was a spurious **c** which could not be eliminated by the Netto criterion on $\mathbf{ca}^i$, $i = 1, \ldots, 12$, were obtained. For all other degrees considered, all groups $G = \{\mathbf{a}, \mathbf{c}\}$ were found to be alternating by the Netto criterion.

For a group with three distinct divisors of q, the number of permutations **c** to be considered is roughly q^3, since each divisor gives at least q choices of **c** due to fixed W, X, Y, Z. Hence, for degree 317, $q = 79$ and about 500,000 groups had to be considered. If, as seems likely, almost all groups were eliminated on the first permutation $\pi = \mathbf{ca}$ of length 317, about 150,000,000 symbols had to be traced through their respective cycles. The time required for the computation for $p = 317$ exceeded four hours. The total time for computation for $p = 13, 29, 53, 149, 269$, and 293 was about five hours. Since the complexity increases as the fourth power of the degree, it did not seem reasonable to try larger values of p. The program was run twice to lower the possibility that any possible machine malfunction affected the result.

References

1. W. Burnside, *Theory of groups of finite order*, 2nd ed. (Cambridge, 1911).
2. M. Hall, Jr., *The theory of groups* (New York, 1959).
3. N. Ito, *Zur Theorie der Permutationsgruppen von Grad p*, Math. Z., *74* (1960), 299–301.
4. G. A. Miller, *Limits of the degree of transitivity of substitution groups*, Bull. Amer. Math Soc., *22* (1915), 68–71.
5. E. T. Parker, *On quadruply transitive groups*, Pacific J. Math., *9* (1959), 829–836.
6. E. T. Parker and J. Nikolai, *A search for analogues of the Mathieu groups*, Math Comput., *12* (1958), 38–43.

University of Illinois