PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 4, April 1999, Pages 951–953
S 0002-9939(99)04704-8

THE CHEVALLEY-WARNING THEOREM AND A COMBINATORIAL QUESTION ON FINITE GROUPS

B. SURY

(Communicated by David E. Rohrlich)

ABSTRACT. Recently, W. D. Gao (1996) proved the following theorem: *For a cyclic group G of prime order, and any element a in it, and an arbitrary sequence $g_1, \ldots, g_{2p-1}$ of $2p-1$ elements from G, the number of ways of writing a as a sum of exactly p of the g_i's is 1 or 0 modulo p according as a is zero or not.* The dual purpose of this note is (i) to give an entirely different type of proof of this theorem; and (ii) to solve a conjecture of J. E. Olson (1976) by answering an analogous question affirmatively for solvable groups.

1. INTRODUCTION

Let G be a finite group of order n. Given any sequence of n (not necessarily distinct) elements $g_1, g_2, \cdots, g_n$ in G, there is obviously a subsequence whose product is the identity, as seen by considering the elements $g_1, g_1g_2, \cdots, g_1g_2\cdots g_n$. In fact, Davenport posed the problem of finding the smallest $s(G)$ such that every sequence of $s(G)$ elements has a subsequence whose product is the identity. If G is a class group, the number $s(G)$ is the maximal number of prime ideals occurring in the factorisation of an irreducible element. The number $s(G)$, called the Davenport constant, has been studied by several mathematicians but hasn't been completely determined as yet even for abelian groups.

A variant of the above question is the following:

Q. *Given a sequence of $2n-1$ elements of a group G of order n, can one always choose exactly n of them, whose product (in some order) is the identity ?*

For abelian groups, the answer is known to be in the affirmative, by the Erdös-Ginzburg-Ziv theorem. In fact, recently W. D. Gao proved (see [G]) the following more general theorem: For a cyclic group G of prime order, and any element a in it, and an arbitrary sequence $g_1, \ldots, g_{2p-1}$ of $2p-1$ elements from G, the number of ways of writing a as a sum of exactly p of the g_i's is 1 or 0 modulo p according as a is zero or not.

J. E. Olson conjectured (see [O]) that the general question has a positive answer for solvable groups.

Received by the editors July 9, 1997.
1991 *Mathematics Subject Classification.* Primary 20D60, 05E15, 11T06.
Key words and phrases. Chevalley-Warning theorem, combinatorial group theory.

The dual purpose of this note is:

(i) to give an entirely different type of proof of Gao's theorem; and

(ii) to solve Olson's conjecture, thereby reducing the question for a general group to nonabelian, finite, simple groups.

2. The main results

Definition. G is a *C-W group* if it answers the question affirmatively. The notation (used for convenience) refers to the fact that the Chevalley-Warning theorem will be used in the proof.

Lemma. *If N is a normal subgroup of G, and if N and G/N are C-W groups, then so is G.*

Proof. Suppose N and G/N have orders n and m respectively. Let $g_1, g_2, \cdots, g_{2mn-1}$ be given in G. Consider the cosets $g_1N, g_2N, \cdots, g_{2m-1}N$. By hypothesis, there are m of them whose product (in some order) is the identity in G/N. After renaming, let us call them $g_1N, g_2N, \cdots, g_mN$. Again, proceed with $2m-1$ cosets from the rest of the $2mn-1-m$ cosets, and choose m of them with product, the identity. Clearly we can choose $2n-1$ such sets because after having chosen $2n-2$ such sets of m cosets, we are left with $2mn-1-m(2n-2) = 2m-1$ cosets from which we may choose the last set. Call these sets (after renaming) $S_1 = \{g_1N, g_2N, \cdots, g_mN\}, \cdots\cdots S_{2n-1} = \{g_{(2n-2)m+1}N, \cdots, g_{(2n-1)m}N\}$, where

$$g_{(i-1)m+1} \cdot g_{(i-1)m+2} \cdots g_{im} \in N \ \forall\ 1 \le i \le 2n-1.$$

Calling $h_i = g_{(i-1)m+1} \cdot g_{(i-1)m+2} \cdots g_{im}\ \forall\ 1 \le i \le 2n-1$, we may choose n of the h_i, say, $h_1, h_2, \cdots, h_n$ such that $h_1 \cdot \cdots\cdots h_n = I$. This being a product of mn elements of the original sequence in G proves the lemma. □

Definition. If $a \in G$, an abelian group of order n, and if $S = \{g_1, \ldots, g_{2n-1}\}$ is a sequence of $2n-1$ elements of G, $r(S,a)$ denotes the number of expressions of a as a product of exactly n elements of S.

Proposition. *Let p be a prime, and S a sequence of $2p-1$ integers. Then, in $\mathbb{Z}/p$, we have*

$$r(S,a) \equiv \begin{cases} 1 & if\ a \equiv 0\ mod\ p, \\ 0 & otherwise. \end{cases}$$

In particular, groups of prime order are C-W groups.

Proof. Let $g_1, g_2, \cdots, g_{2p-1}$ be a sequence of integers. The idea is to find a polynomial over integers mod p whose zero-counting function also counts the expressions of the form $\sum_S a_i = a$, where S is exactly of cardinality p. We first look at the case $a = 0$. In this case, we start with the polynomials $f = (\sum_{i=1}^{2p-1} g_i X_i^{p-1})^2$ and $g = (\sum_{i=1}^{2p-1} X_i^{p-1})^2$ both homogeneous of degree $2p-2$ in $2p-1$ variables. We consider any combination $h = \alpha.f + \beta.g$ where α and β are non-zero integers mod p. By the theorem of Chevalley-Warning, such a polynomial has $N(h)$ zeros, with $N(h) \equiv 0 \bmod p$; therefore there is a zero , say $x_1, x_2, \cdots, x_{2p-1}$, which is nontrivial mod p. Now, we choose α and β such that $-\frac{\alpha}{\beta}$ is not a square mod p. This forces both $\sum_{i=1}^{2p-1} g_i x_i^{p-1} \equiv 0 \equiv \sum_{i=1}^{2p-1} x_i^{p-1}$. Write $S = \{i : x_i \neq 0\ mod\ p\}$. Then, $\sum_S g_i x_i^{p-1} = 0 = \sum_S x_i^{p-1}$. Since $x_i^{p-1} = 1$ when $x_i \neq 0 \bmod p$, the cardinality $\mid S \mid \equiv 0 \bmod p$. But, since S is nonempty and has less than $2p$ elements, it is forced that $\mid S \mid = p$. Thus, $\sum_S g_i \equiv 0\ mod\ p$. Thus, certainly $r(S,0) > 0$. Let us

count $r(S,0)$ more precisely now. Since each of the p non-zero x_i's in a non-trivial zero of h contributes $p-1$ times, we get $N(h) = 1 + r(S,0)(p-1)^p$ where the 1 corresponds to the trivial zero of h. As $N(h) \equiv 0 \bmod p$, we can compare mod p, to get $r(S,0) \equiv 1 \bmod p$.

To deal with the case of some $a \not\equiv 0 \bmod p$, we need only consider the polynomial $\Phi = \alpha(\sum_{i=1}^{2p-1} g_i X_i^{p-1} - aX_{2p}^{p-1})^2 + \beta(\sum_{i=1}^{2p-1} X_i^{p-1})^2$. Since, obviously,

$$\{x : \Phi(x) = 0\} = \{x : \Phi(x) = 0 = x_{2p}\} \cup \{x : \Phi(x) = 0 \neq x_{2p}\}$$

it is evident that

$$N(\Phi) = N(h) + (p-1)^p r(S,a)$$

where h is the above polynomial we had earlier.

Thus, we get $r(S,a) \equiv 0 \bmod p$ for $a \not\equiv 0$.

Remarks. (a) It is easy to see that if p is not a prime, we need not have $r(S,a)$ in the residue classes predicted by the proposition.

(b) It is trivial to see that we cannot replace $2p-1$ by a smaller number in the proposition.

Corollary. *Solvable groups are C-W groups.*

Proof. By induction on the derived length, the proof reduces by the lemma to abelian groups, and, for abelian groups the induction argument reduces to the prime case dealt with in the proposition.

Finally we remark that, by the lemma, an affirmative answer to the question in the case of nonabelian, finite simple groups, implies one for arbirary finite groups.

Acknowledgement

Very recently, the author was informed that the idea of using the Chevalley-Warning theorem has already been used by N. Alon to prove the Erdös-Ginzburg-Ziv theorem in 'Handbook of combinatorics', Eds. North Holland 1995.

References

[G] W. D. Gao - Two addition theorems on groups of prime order, J. Number Theory, Vol.56 (1996) 211-213.

[O] J. E. Olson - On a combinatorial problem of Erdös, Ginzburg and Ziv, J. Number Theory, Vol.8 (1976) 52-57. MR **53:**2883

School Of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Bombay 400 005, India

E-mail address: sury@math.tifr.res.in