CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Elsevier - Publisher Connector

JOURNAL OF NUMBER THEORY 1, 8–10 (1969)

A Combinatorial Problem on Finite Abelian Groups, I*

JOHN E. OLSON

Department of Mathematics,
The University of Wisconsin, Madison, Wisconsin 53706

Communicated by H. B. Mann

Received February 2, 1968

If G is a finite Abelian group, for what number s is it true that an arbitrary sequence of length s of group elements has a subsequence whose product is 1? This question is answered for p-groups.

1. Let G be a finite Abelian group. Define $s = s(G)$ to be the smallest positive integer such that, for any sequence $g_1, g_2, \ldots, g_s$ (repetition allowed) of group elements, there exist indices

$$1 \leq i_1 < \ldots < i_t \leq s$$

for which $g_{i_1} g_{i_2} \ldots g_{i_t} = 1$. In this paper we determine $s(G)$ for all finite Abelian p-groups G.

The problem of finding $s(G)$ was proposed by H. Davenport (Midwestern Conference on Group Theory and Number Theory, Ohio State University, April 1966) in the following connection. If G is the class group of an algebraic number field F, then $s(G)$ is the maximal number of prime ideals (counting multiplicity) in the decomposition of an irreducible integer in F.

2. Let G be a finite Abelian p-group with invariants $p^{e_1}, p^{e_2}, \ldots, p^{e_r}$. We show

$$s(G) = 1 + \sum (p^{e_i} - 1). \tag{1}$$

The right-hand side of (1) is an obvious lower bound for $s(G)$. For let $x_1, \ldots, x_r$ be a basis for G where x_i has order p^{e_i}. Form a sequence of length $\sum (p^{e_i} - 1)$ in which each x_i occurs $p^{e_i} - 1$ times. No subsequence has product 1.

* Sponsored by the Mathematics Research Center, United States Army, Madison, Wisconsin, under Contract No. DA–31–124–ARO–D–462.

In the other direction, we prove a theorem which we state in terms of the group-ring of G over the rational integers.

THEOREM 1. *If* $g_1,\dots,g_k \in G$ *and* $k \geq 1+\sum(p^{e_i}-1)$, *then*

$$(1-g_1)(1-g_2)\dots(1-g_k) \equiv 0 \pmod{p}. \tag{2}$$

Interpret the congruence (2) combinatorially: For $g \in G$ look at all subsequences of $g_1,\dots,g_k$ that have product g. Let $E(g)$ count those of even length and let $O(g)$ count those of odd length. Equation (2) shows that

$$E(g)-O(g) \equiv \begin{cases} 0 \pmod{p} \text{ if } g \neq 1, \\ -1 \pmod{p} \text{ if } g = 1. \end{cases}$$

In particular, we cannot have $E(1) = O(1) = 0$, and this proves (1).

Proof of (2). Again let $x_1,\dots,x_r$ be a basis for G where x_i has order p^{e_i}. If, for some i, $g_i = uv$, we may "reduce" the product

$$J = (1-g_1)\dots(1-g_k)$$

to the form

$$J = (1-g_1)\dots(1-g_{i-1})(1-u)(1-g_{i+1})\dots(1-g_k) + u(1-g_1)\dots(1-g_{i-1})(1-v)(1-g_{i+1})\dots(1-g_k).$$

Since each g_i is a product of the basis elements x_j we may, by repeated application of this reduction procedure, arrive at the following expression for J.

$$J = \sum_\sigma g_\sigma J_\sigma,$$

where each $g_\sigma \in G$ and each J_σ is a product of the form

$$J_\sigma = (1-x_1)^{f_1}(1-x_2)^{f_2}\dots(1-x_r)^{f_r}. \tag{3}$$

Here the f_i are nonnegative integers which depend on the index σ, and $\sum f_i = k$. Since $k > \sum(p^{e_i}-1)$ we must have $f_i \geq p^{e_i}$ for some i in (3). But

$$(1-x_i)^{p^{e_i}} \equiv 0 \pmod{p}.$$

Thus $J_\sigma \equiv 0 \pmod{p}$ for each σ, and this proves (2).

We may state Theorem 1 in more general form. For $g \in G$, define $\alpha(g) = p^n$ where n is the largest integer such that g is a p^nth power in G ($\alpha(1) = \infty$). If $g = h^{p^n}$, then $(1-g) \equiv (1-h)^{p^n} \pmod{p}$. We have, therefore,

THEOREM 2. *If* $g_1,\dots,g_k \in G$ *and* $\sum \alpha(g_i) \geq 1+\sum(p^{e_i}-1)$, *then*

$$(1-g_1)(1-g_2)\dots(1-g_k) \equiv 0 \pmod{p}.$$

3. If G is any finite Abelian group and H is a subgroup of G, then clearly $s(G) \leq s(H) \cdot s(G/H)$. Hence the results for p-groups give upper estimates for $s(G)$ in the general case. We conjecture, however, that if $G = C_1 \times \ldots \times C_r$ is the direct product of cyclic groups C_i of order $|C_i| = c_i$ where $c_i | c_{i+1}$, then $s(G) = 1 + \sum (c_i - 1)$.

Acknowledgment

The author wishes to express his gratitude to Professor Henry B. Mann for his interest and stimulation.