ON A CONJECTURE OF ERDÖS AND RÉNYI

BY

R. J. MIECH

Let G be a finite Abelian group of order n, $a_1, \cdots, a_k$ be a sequence of elements of G, and let

$$B = B(a_1, \cdots, a_k) = \{\varepsilon_1 a_1 + \cdots + \varepsilon_k a_k : \varepsilon_i = 0 \text{ or } 1, i = 1, \cdots k\}.$$

Note that if $B = G$ then we must have $k \geq (\log n)/\log 2$. In a recent paper [1] Erdös and Rényi raised the question: how large must k be in order that every element b of G have approximately the same number of representations of the form

$$b = \varepsilon_1 a_1 + \cdots + \varepsilon_k a_k$$

for nearly every sequence $a_1, \cdots, a_k$ of G? In other words, how large must k be in order that nearly every sequence $a_1, \cdots, a_k$ of G will generate G in a uniform fashion? They proved that any k such that

$$k \geq (2 \log n + c)/\log 2,$$

where c is a certain constant, is sufficient and they conjectured that the coefficient of $\log n$ in this inequality, 2, could not be replaced by anything better. The purpose of this paper is to show that the 2 can be replaced by $\frac{3}{2}$ for most groups and that the conjecture, if it is true, is valid only for groups of a particular nature.

Several definitions are needed before precise results can be stated. Let G_k be the Cartesian product of k copies of G, let P be the probability measure on G_k whose value at each point of G_k is n^{-k}, and let, for each b in G, $V_k(b)$ be the random variable whose value at each point $(a) = (a_1, \cdots, a_k)$ of G_k is given by

$$V_k(b, (a)) = N\{(\varepsilon_1, \cdots, \varepsilon_k) : \varepsilon_1 a_1 + \cdots + \varepsilon_k a_k = b\}$$

where $N\{\mathfrak{U}\}$ is the number of elements in the set $\mathfrak{U}$. Suppose, furthermore, that if G is expressed as a direct sum of cyclic groups of prime power order then r of the summands have orders that are powers of 2. Then we have the

THEOREM. *Let G be a finite Abelian group of order n and let P, $V_k(b)$, and r be defined as above. Let ε and δ be any fixed positive numbers. Then if k is any integer such that*

$$k \geq \left(\max\left\{\frac{3}{2}\log n, \log n + r \log 2\right\} + 4 \log \frac{1}{\epsilon} + \log\right) \frac{1}{\log 2} + 8$$

Received December 9, 1965.