ACTA ARITHMETICA
XXVIII (1975)

Sums of sets of group elements

by

JOHN E. OLSON (University Park, Penn.)

Dedicated to Henry B. Mann on his 70th birthday

1. Introduction. Let S be a set of s distinct non-zero elements in a group G (written additively).

Recently Szemerédi [4] proved the conjecture of Erdös and Heilbronn that if G is an abelian group of order n and $s \geqslant cn^{1/2}$ (c is an absolute constant), then the zero element has a representation as a sum $0 = a_1 + \ldots + a_t$ of distinct elements a_i in S. Earlier Erdös and Heilbronn [1] had shown that if G is the group of prime order p and $s \geqslant cp^{1/2}$, then every element in G occurs as a sum of distinct elements in S. The constant $c = 3\sqrt{6}$ given by Erdös and Heilbronn was reduced to $c = 2$ by the present author [3].

In this paper we investigate similar questions for an arbitrary group. We prove that if G has finite order n and $s \geqslant 3n^{1/2}$, then zero occurs as a sum of distinct elements in S. This will follow from the stronger result that (for any group G) there is an arrangement $a_1, \ldots, a_s$ of the elements of S such that either the sums $\varepsilon_1 a_1 + \ldots + \varepsilon_s a_s$ ($\varepsilon_i = 0$ or 1) represent at least cs^2 elements, or no element is represented exactly once. We show also that if G has finite order n, $s \geqslant 3\sqrt{2}n^{1/2}$, and not too many of the elements of S belong to a proper subgroup, then every g in G occurs as a sum of distinct elements in S.

2. Notation and preliminaries. If S is a subset of the group G, we shall denote by $|S|$ the cardinality of S, by $\bar{S}$ the complement of S in G, and by $\langle S \rangle$ the subgroup generated by S. If $A_1, \ldots, A_n$ are subsets of G, let $A_1 + \ldots + A_n$ denote the set of all sums $a_1 + \ldots + a_n$, where $a_i \in A_i$. Finally, if A is a subset of G and n is a positive integer, let $nA = A + \ldots + A$ (n times).

THEOREM 2.1 (Kemperman, Wehn). *Let A and B be finite non-empty subsets of G and let*

$$|A+B| = |A| + |B| - k.$$

Then every element $c \in A+B$ has at least k representations as a sum $c = a+b$ with $a \in A$, $b \in B$.

Theorem 2.1 goes back to results of L. Moser and P. Scherk in the case of abelian groups, and was proved for non-abelian groups by J. H. B. Kemperman and (independently) D. F. Wehn. For proof see Kemperman's paper [2]. We shall use this theorem in the proof of the following result which appears to be new.

THEOREM 2.2. *If A is a finite subset of G, $0 \in A$, and n is a positive integer, then either $nA = \langle A \rangle$ or*

$$|nA| \geqslant |A| + (n-1)[\tfrac{1}{2}(|A|+1)].$$

(Here $[m]$ denotes the greatest integer in m.)

Proof. It suffices to show that

$$(1) \qquad |nA| \geqslant |(n-1)A| + \tfrac{1}{2}|A|,$$

assuming $n > 1$ and $nA \neq \langle A \rangle$. Since $0 \in A$, we have $nA \subseteq (n+1)A$. Moreover, nA must be a proper subset of $(n+1)A$ for, otherwise, $nA = mA$ for all $m > n$ which implies $nA = \langle A \rangle$, since nA is a finite set. Choose $x \in (n+1)A$, $x \notin nA$. Hence $x = a_0 + y$ where $a_0 \in A$ and $y \in nA$. Now define k by

$$(2) \qquad |nA| = |(n-1)A| + |A| - k.$$

Since $y \in nA = (n-1)A + A$, y has, by Theorem 2.1, at least k representations as a sum $y = z + a$, with $z \in (n-1)A$, $a \in A$. Hence the set $A^* = \{a \in A \mid y - a \in (n-1)A\}$ is not empty and has size $|A^*| \geqslant k$. Since $y - A^* \subseteq (n-1)A$, we have

$$x - A^* = a_0 + y - A^* \subseteq a_0 + (n-1)A \subseteq nA.$$

Thus $nA \supseteq (n-1)A \cup (x - A^*)$. But the sets $(n-1)A$ and $x - A^*$ are disjoint since $x \notin nA$. Hence

$$|nA| \geqslant |(n-1)A| + |x - A^*| = |(n-1)A| + |A^*|,$$

and so

$$(3) \qquad |nA| \geqslant |(n-1)A| + k.$$

The inequality (1) follows from (2) and (3).

We remark that equality may hold in Theorem 2.2. For example, suppose H is a finite subgroup of G and (assuming H is properly included in its normalizer in G) let $x + H = H + x$ for some $x \in G$, $x \notin H$. Take $A = H \cup (x + H)$. Clearly, for each positive integer n, either $nA = \langle A \rangle$ or $|nA| = (n+1)|H| = \frac{1}{2}(n+1)|A|$.

3. Main theorems. The results in this section depend on the following lemma whose proof we postpone until the next section.

LEMMA 3.1. *Let B be a non-empty proper subset of a group G such that either B or its complement $\bar{B}$ in G is finite, and let $k = \min\{|B|, |\bar{B}|\}$. Let $a_1, \ldots, a_w$ be w distinct non-zero elements of G. Assume that the subgroup $H = \langle a_1, \ldots, a_w \rangle$ generated by $a_1, \ldots, a_w$ has size $|H| \geqslant 2k$. Then*

$$|(B + a_v) \cap \bar{B}| \geqslant \min\{\tfrac{1}{2}(k+1), \tfrac{1}{4}(w+2)\}$$

for at least one index $1 \leqslant v \leqslant w$.

Remark. In the lemma, the subgroup H may be infinite, in which case the condition $|H| \geqslant 2k$ is satisfied.

If $a_1, \ldots, a_t$ is a sequence of group elements let $\Sigma = \Sigma(a_1, \ldots, a_t)$ denote the sum set

$$\Sigma = \{0, a_1\} + \{0, a_2\} + \ldots + \{0, a_t\}.$$

Note that if G is not abelian, then Σ depends on the order in which the a_i are listed. If $g \in \Sigma$, then by the *number of representations of g in Σ* we shall mean the number of t-tuples $(\varepsilon_1, \ldots, \varepsilon_t)$, $\varepsilon_i = 0$ or 1, such that $g = \varepsilon_1 a_1 + \ldots + \varepsilon_t a_t$.

THEOREM 3.1. *Let S be a set of $s \geqslant 3$ distinct non-zero elements of G such that $\langle S \rangle = G$. Then there is an arrangement $a_1, \ldots, a_s$ of the elements of S and an index $2 \leqslant q \leqslant s$ such that either $\Sigma(a_1, \ldots, a_{s-1}) = G$ or the following hold.*

(i) *For all $2 \leqslant t \leqslant q$*

$$(4) \qquad |\Sigma(a_1, \ldots, a_t)| \geqslant 4 + \tfrac{1}{8}[(s-2)(s+3) - (s-t)(s-t+5)] - \Delta(s),$$

where $O(s\log s) = \Delta(s) < s^2/72$.

(ii) *If $q < s$, then $H = \langle a_{q+1}, \ldots, a_s \rangle$ is a finite proper subgroup of G and $|H| < 2\min\{|\Sigma|, |\bar{\Sigma}|\}$, where $\Sigma = \Sigma(a_1, \ldots, a_q)$ and $\bar{\Sigma}$ is the complement of Σ in G.*

Proof. We first give the arrangement of the a_i for which the theorem holds. Choose $a_1 \in S$ arbitrarily and, having chosen $a_1, \ldots, a_{j-1}$, choose a_j from among the rest so as to maximize the size of $\Sigma(a_1, \ldots, a_j)$. Assume now that $\Sigma(a_1, \ldots, a_{s-1}) \neq G$.

For each $2 \leqslant t \leqslant s$, let $\sigma_t = |\Sigma(a_1, \ldots, a_t)|$. Since $s \geqslant 3$ we must have $\sigma_2 = 4$ (i.e. $a_2 \neq -a_1$).

Fix an index $2 < t \leqslant s$ and let $B = \Sigma(a_1, \ldots, a_{t-1})$. Clearly

$$\Sigma(a_1, \ldots, a_t) = B \cup [(B + a_t) \cap \bar{B}],$$

and hence

$$\sigma_t = \sigma_{t-1} + |(B + a_t) \cap \bar{B}|.$$

We now use Lemma 3.1. Let $k = \min\{|B|, |\bar{B}|\}$ and $H_t = \langle a_t, \ldots, a_s \rangle$. Assume, for the moment, that $|H_t| \geqslant 2k$. Then, by Lemma 3.1, there is an index $t \leqslant v \leqslant s$ such that

$$(5) \qquad |(B + a_v) \cap \bar{B}| \geqslant \min\{\tfrac{1}{2}(k+1), \tfrac{1}{4}(s-t+3)\}.$$

By the way the a_i were arranged, equation (5) holds with $v = t$, therefore

(6) $$\sigma_t \geqslant \sigma_{t-1} + \min\{\tfrac{1}{2}(k+1), \tfrac{1}{4}(s-t+3)\}.$$

We show next that the inequality (6) remains valid if k is replaced by $|B| = \sigma_{t-1}$. Suppose not. Then $k = |\bar{B}| < |B|$ and also $s-t+3 > 2(k+1)$. Hence G is a finite group and $s-t+1 > 2k > |\bar{B}|$. But the set $C = \{0, a_t\} + \ldots + \{0, a_{s-1}\}$ has size $|C| \geqslant s-t+1 > |\bar{B}|$, hence

(7) $$|B| + |C| > |B| + |\bar{B}| = |G|.$$

It follows from (7) that $B + C = G$. Therefore $\Sigma(a_1, \ldots, a_{s-1}) = G$, contrary to our assumption. Thus

(8) $$\sigma_t \geqslant \sigma_{t-1} + \min\{\tfrac{1}{2}(\sigma_{t-1}+1), \tfrac{1}{4}(s-t+3)\},$$

provided $|H_t| \geqslant 2k$.

We now let q be the smallest index $(2 \leqslant q)$ such that

(9) $$|\langle a_{q+1}, \ldots, a_s\rangle| < 2\min\{|\Sigma|, |\bar{\Sigma}|\},$$

where $\Sigma = \Sigma(a_1, \ldots, a_q)$. (Take $q = s$ if (9) never occurs.) Hence statement (ii) holds, and the inequality (8) holds for all $2 < t \leqslant q$.

The rest of the proof is a computation based on (8). Define numbers $y_2, \ldots, y_s$ by the recursion $y_2 = 4$ and (for $2 < t \leqslant s$)

(10) $$y_t = y_{t-1} + \min\{\tfrac{1}{2}(y_{t-1}+1), \tfrac{1}{4}(s-t+3)\}.$$

Since $\sigma_t \geqslant y_t$ for all $2 \leqslant t \leqslant q$, it suffices to show

(11) $$y_t \geqslant 4 + \tfrac{1}{8}[(s-2)(s+3) - (s-t)(s-t+5)] - \Delta(s),$$

where $O(s\log s) = \Delta(s) < s^2/72$.

If $s \leqslant 10$, equation (10) reduces to $y_t = y_{t-1} + \frac{1}{4}(s-t+3)$, and a simple computation shows that equality holds in (11) with $\Delta(s) = 0$.

For $s \geqslant 11$, let $u = u(s)$ be the largest integer in the interval $3 \leqslant u < s-1$ such that

$$\tfrac{1}{2}(y_{u-1}+1) < \tfrac{1}{4}(s-u+3).$$

Hence

(12) $$2y_{u-1} + u - 1 < s.$$

Equation (10) becomes

$$y_t = \begin{cases} \tfrac{1}{2}(3y_{t-1}+1) & \text{if} \quad 3 \leqslant t \leqslant u, \\ y_{t-1} + \tfrac{1}{4}(s-t+3) & \text{if} \quad u < t \leqslant s. \end{cases}$$

Hence

(13) $$y_t = 5(\tfrac{3}{2})^{t-2} - 1 \quad (\text{for } 2 \leqslant t \leqslant u).$$

From (12) and (13) we get

(14) $$10(\tfrac{3}{2})^{u-3} + u - 3 < s.$$

For $2 \leqslant t \leqslant s$ we have

$$y_t = 4 + \sum_{j=3}^{t} \tfrac{1}{4}(s-j+3) - \sum_{j=3}^{r} \tfrac{1}{4}(s-j+3) + \sum_{j=3}^{r} \tfrac{1}{2}(y_{j-1}+1),$$

where $r = \min\{u, t\}$. Hence

$$\begin{aligned} y_t &\geqslant 4 + \sum_{j=3}^{t} \tfrac{1}{4}(s-j+3) - \sum_{j=3}^{u} \tfrac{1}{4}(s-j+3) + \sum_{j=3}^{u} \tfrac{1}{2}(y_{j-1}+1) \\ &= 4 + \tfrac{1}{8}[(s-2)(s+3) - (s-t)(s-t+5)] - \Delta(s), \end{aligned}$$

where

$$\begin{aligned} \Delta(s) &= -\sum_{j=3}^{u} \tfrac{1}{2}(y_{j-1}+1) + \sum_{j=3}^{u} \tfrac{1}{4}(s-j+3) \\ &= -y_u + 4 + \tfrac{1}{8}[(s-2)(s+3) - (s-u)(s-u+5)]. \end{aligned}$$

Thus (11) holds with

(15) $$\Delta(s) = \tfrac{1}{8}\{2s(u-2) + u(5-u) + 26 - 8y_u\}.$$

By (14) $u = O(\log s)$, hence by (15) $\Delta(s) = O(s\log s)$. If $u \geqslant 10$, then by (14) $s > 18(u-2)$, and so by (15) $\Delta(s) < \frac{1}{4}s(u-2) < s^2/72$. By computing the value of y_u from (13) for each u in the range $3 \leqslant u \leqslant 9$, it is easy to verify from (15) that $\Delta(s) < s^2/72$. This completes the proof.

THEOREM 3.2. *Let S be a set of s distinct non-zero elements of G. Then there is an arrangement $a_1, \ldots, a_s$ of the elements of S such that either*

(A) *every element in $\Sigma = \Sigma(a_1, \ldots, a_s)$ has at least two representations in Σ, or*

(B) $|\Sigma| > 1 + cs^2$, *where* $c = \frac{1}{8} - O(\log s/s) > \frac{1}{9}$.

Proof. The proof is by induction on s. Statement (B) holds trivially for small s (with $c = \frac{1}{8}$), so assume $s \geqslant 6$. Our induction hypothesis is that, for smaller s, the theorem is true in the weaker form with $c = \frac{1}{9}$. We may assume without loss of generality that $\langle S\rangle = G$. Now let $a_1, \ldots, a_s$ be the arrangement and $2 \leqslant q \leqslant s$ the index given by Theorem 3.1. We may assume that $\Sigma(a_1, \ldots, a_{s-1}) \neq G$, since otherwise statement (A) holds. Hence, by Theorem 3.1,

(16) $$|\Sigma(a_1, \ldots, a_t)| > 3 + cs^2 - \tfrac{1}{8}(s-t)(s-t+5)$$

holds for all $2 \leqslant t \leqslant q$, where $c = \frac{1}{8} - O(\log s/s) > \frac{1}{9}$. If $q = s$ we are done. Assume $q < s$. Thus $H = \langle a_{q+1}, \ldots, a_s\rangle$ is a proper subgroup of G. Now let $1 \leqslant v \leqslant q$ be the largest index such that $a_v \notin H$. We now apply our induction hypothesis to the set of $s-v$ elements $a_{v+1}, \ldots, a_s$. Thus after relabelling these elements, either

(17) $$|\Sigma(a_{v+1}, \ldots, a_s)| > 1+\tfrac{1}{9}(s-v)^2,$$

or every element in $\Sigma(a_{v+1}, \ldots, a_s)$ has at least two representations. But the latter possibility implies that every element of $\Sigma(a_1, \ldots, a_s)$ has at least two representations. We may assume, therefore, that (17) holds. Since $a_{v+1}, \ldots, a_s \in H$ and $a_v \notin H$, the set $\Sigma(a_v, a_{v+1}, \ldots, a_s)$ contains twice as many elements as $\Sigma(a_{v+1}, \ldots, a_s)$. Hence

(18) $$|\Sigma(a_v, \ldots, a_s)| > 2+\tfrac{2}{9}(s-v)^2.$$

We may assume that $v \geqslant 3$ since, if $v=1$ or 2 and $s \geqslant 6$, the right hand side of (18) exceeds $1+\frac{1}{8}s^2$. Put $A=\Sigma(a_1, \ldots, a_{v-1})$ and $B=\Sigma(a_v, \ldots, a_s)$. Clearly

$$\Sigma = \Sigma(a_1, \ldots, a_s) = A+B.$$

We may assume that at least one element of Σ has a unique representation as a sum $a+b$, $a \in A$, $b \in B$, for otherwise every element of Σ has at least two representations in Σ. Hence, by Theorem 2.1,

(19) $$|\Sigma| \geqslant |A|+|B|-1.$$

Taking $t=v-1$ in (16) we get

(20) $$|A| > 3+cs^2-\tfrac{1}{8}(s-v+1)(s-v+6).$$

Hence, by (18), (19) and (20),

$$|\Sigma| > 4+cs^2+\tfrac{2}{9}(s-v)^2-\tfrac{1}{8}(s-v+1)(s-v+6) > 1+cs^2.$$

This proves the theorem.

Taking $c=\frac{1}{9}$ in Theorem 3.2, we get as a direct consequence the following result for a finite group.

COROLLARY 3.2.1. *If S is a set of s distinct non-zero elements in a finite group of order n and $s \geqslant 3n^{1/2}$, then there is an arrangement $a_1, \ldots, a_s$ of the elements of S such that every element in $\Sigma = \Sigma(a_1, \ldots, a_s)$ has at least two representations in Σ. In particular, 0 occurs non-trivially in Σ.*

For the group of prime order p it is known (see [3]) that *every* element of the group can be written as a sum of distinct elements from a set S provided $|S| > 2p^{1/2}$. We next use Theorem 3.1 to prove a similar result for an arbitrary finite group.

THEOREM 3.3. *Let S be a set of s distinct non-zero elements in a finite group G of order n, where $s \geqslant cn^{1/2}$ and $c \geqslant 3\sqrt{2}$. Assume that no proper subgroup H of G contains more than $c|H|^{1/2}$ of the elements in S. Then there is an arrangement $a_1, \ldots, a_s$ of the elements of S such that $\Sigma(a_1, \ldots, a_s) = G$, and every element of G has at least two representations in $\Sigma(a_1, \ldots, a_s)$.*

Remark. The proof is such that the bound $c \geqslant 3\sqrt{2}$ can be improved if the smallest prime divisor of n is greater than 2. In fact, we shall prove the theorem assuming

(21) $$c \geqslant 3\left(\frac{8p-2}{8p-9}\right)^{1/2},$$

where p is the smallest prime divisor of n.

Proof. Our hypothesis implies $\langle S\rangle = G$, so we may apply Theorem 3.1. Let q $(2 \leqslant q \leqslant s)$ be the index and $a_1, \ldots, a_s$ the arrangement given in Theorem 3.1. It suffices to show that $\Sigma(a_1, \ldots, a_{s-1}) = G$. Suppose not. Then

(22) $$\begin{aligned}|\Sigma(a_1, \ldots, a_t)| &\geqslant 4+\tfrac{1}{8}[(s-2)(s+3)-(s-t)(s-t+5)]-s^2/72\\ &> 1+\tfrac{1}{9}s^2-\tfrac{1}{8}(s-t)^2-\tfrac{1}{2}(s-t),\end{aligned}$$

for all $2 \leqslant t \leqslant q$. We must have $q < s-1$, since otherwise (22) implies

$$|\Sigma(a_1, \ldots, a_{s-1})| > \tfrac{1}{9}s^2 > n,$$

which is impossible. Now let $\Sigma = \Sigma(a_1, \ldots, a_q)$ and let $H = \langle a_{q+1}, \ldots, a_s\rangle$. H is a non-trivial proper subgroup of G satisfying $|H| < 2|\bar{\Sigma}| = 2(n-|\Sigma|)$. Hence

(23) $$n\left(\frac{2d-1}{2d}\right) > |\Sigma|,$$

where $|H| = n/d$. By (22) we have

(24) $$|\Sigma| > \tfrac{1}{9}s^2-\tfrac{1}{8}(s-q)^2-\tfrac{1}{2}(s-q).$$

Hence, by (23) and (24),

(25) $$n\left(\frac{2d-1}{2d}\right) > \tfrac{1}{9}s^2-\tfrac{1}{8}(s-q)^2-\tfrac{1}{2}(s-q).$$

Clearly $\Sigma(a_1, \ldots, a_{s-1}) = \Sigma+C$, where $C = \{0, a_{q+1}\}+\ldots+\{0, a_{s-1}\}$. The inequality $|\Sigma|+|C| > n$ implies $\Sigma+C = G$, contrary to assumption. Therefore $|\Sigma|+|C| \leqslant n$. Since $|C| \geqslant s-q$, we have $n \geqslant |\Sigma|+(s-q)$, and therefore, by (24),

(26) $$n > \tfrac{1}{9}s^2-\tfrac{1}{8}(s-q)^2+\tfrac{1}{2}(s-q).$$

Adding the inequalities (25) and (26), we get

(27) $$n\left(\frac{4d-1}{4d}\right) > \tfrac{1}{9}s^2-\tfrac{1}{8}(s-q)^2.$$

Now $s \geqslant cn^{1/2}$ and, since H contains at most $c(n/d)^{1/2}$ of the elements in S, $s-q \leqslant c(n/d)^{1/2}$. Hence, by (27),

(28) $$c^2 < 9\left(\frac{8d-2}{8d-9}\right).$$

Since $d \geqslant p$, where p is the smallest prime divisor of n, the inequality (28) contradicts the bound on c given in (21). Thus $\Sigma(a_1, \ldots, a_{s-1}) = G$ and the theorem is proved.

Assuming $s \geqslant cn^{1/2}$, we may now strengthen the conclusion of Corollary 3.2.1. Again assume c satisfies (21), where p is the smallest prime divisor of n.

COROLLARY 3.3.1. *Let S be a set of non-zero elements from a finite group G of order n of size $|S| \geqslant cn^{1/2}$. Then G contains a subgroup H, and S contains t distinct elements $a_1, \ldots, a_t$, such that $\Sigma(a_1, \ldots, a_t) = H$, $t \geqslant c|H|^{1/2}$, and every element of H has at least two representations in $\Sigma(a_1, \ldots, a_t)$.*

Proof. Simply let H be a subgroup of G such that $|S \cap H| \geqslant c|H|^{1/2}$, but $|S \cap K| \leqslant c|K|^{1/2}$ for all proper subgroups K of H. Then apply Theorem 3.3 to the set $S \cap H$.

Note that each theorem in this section asserts that there is an arrangement $a_1, \ldots, a_s$ of the elements of S such that something is true for $\Sigma(a_1, \ldots, a_s)$. We leave open the question of what can be said about $\Sigma(a_1, \ldots, a_s)$ for an *arbitrary* arrangement $a_1, \ldots, a_s$.

4. Proof of Lemma 3.1. To prove Lemma 3.1 we shall use Theorem 2.2 and a modification of the averaging process due to Erdös and Heilbronn [1].

First, we may assume without loss of generality that $k = |B| \leqslant |\bar{B}|$. This is because, for $g \in G$,

$$|(B+g) \cap \bar{B}| = |(\bar{B}+g) \cap B|. \tag{29}$$

To prove (29) assume first that B is finite. Hence

$$\begin{aligned}|(B+g) \cap \bar{B}| &= |B+g| - |(B+g) \cap B| \\ &= |B-g| - |B \cap (B-g)| = |(B-g) \cap \bar{B}| = |B \cap (\bar{B}+g)|.\end{aligned}$$

By symmetry (29) holds if $\bar{B}$ is finite.

Next, define a mapping λ from G to the non-negative integers by

$$\lambda(g) = |(B+g) \cap \bar{B}|.$$

The mapping λ is "sub-additive", i.e.

$$\lambda(x+y) \leqslant \lambda(x) + \lambda(y), \tag{30}$$

as shown by the simple calculation:

$$\begin{aligned}\lambda(x+y) &= |(B+x+y) \cap \bar{B}| = |(B+x) \cap (\bar{B}-y)| \\ &= |(B+x) \cap (\bar{B}-y) \cap \bar{B}| + |(B+x) \cap (\bar{B}-y) \cap B| \\ &\leqslant |(B+x) \cap \bar{B}| + |(\bar{B}-y) \cap B| = |(B+x) \cap \bar{B}| + |(B+y) \cap \bar{B}| \\ &= \lambda(x) + \lambda(y).\end{aligned}$$

Now let $\alpha = \max\{\lambda(a_i) \mid 1 \leqslant i \leqslant w\}$. We divide the proof into two cases.

Case 1: $w \geqslant 2k-1$. Let $C = \{a_1, \ldots, a_{2k-1}\}$. Thus

$$\sum_{c \in C} \lambda(c) \leqslant (2k-1)\alpha. \tag{31}$$

On the other hand

$$\begin{aligned}\sum_{c\in C} \lambda(c) &= \sum_{c \in C} |(B+c) \cap \bar{B}| = \sum_{c \in C} [|B| - |(B+c) \cap B|] \\ &= |C||B| - \sum_{c \in C} |(B+c) \cap B| \geqslant |C||B| - \sum_{\substack{x \in G \\ x \neq 0}} |(B+x) \cap B| \\ &= |C||B| - |B|(|B|-1).\end{aligned}$$

Hence

$$\sum_{c \in C} \lambda(c) \geqslant k^2. \tag{32}$$

By (31) and (32), $\alpha \geqslant k^2/(2k-1) > k/2$. Hence $\alpha \geqslant \frac{1}{2}(k+1)$ and the lemma is proved in this case.

Case 2: $w \leqslant 2k-2$. As in Case 1 we shall construct a set C of size $|C| = 2k-1$. Form the set $A = \{0, a_1, \ldots, a_w\}$ and let

$$u = [\tfrac{1}{2}(|A|+1)] = \begin{cases} \frac{1}{2}(w+2) & \text{if } w \text{ is even}, \\ \frac{1}{2}(w+1) & \text{if } w \text{ is odd}. \end{cases}$$

We now use Theorem 2.2. Since, by hypothesis, the group $\langle A \rangle$ has order at least $2k$, we conclude from Theorem 2.2 that $|nA| \geqslant 2k$ or $|nA| \geqslant (w+1)+(n-1)u$, for each positive integer n. Define integers r and q by

$$2k = (w+1)+(r-2)u+q, \quad 0 \leqslant q < u. \tag{33}$$

Note that $r \geqslant 2$ because $w \leqslant 2k-2$. Hence $|rA| \geqslant 2k$ and

$$|nA| \geqslant (w+1)+(n-1)u \quad (1 \leqslant n \leqslant r-1).$$

Therefore rA has a subset C of non-zero elements of size $|C| = 2k-1$ such that

$$|nA \cap C| \geqslant w+(n-1)u \quad (1 \leqslant n \leqslant r-1).$$

If $c \in nA$, then $\lambda(c) \leqslant n\alpha$ by (30). Hence

$$\sum_{c \in C} \lambda(c) \leqslant w\alpha + u2\alpha + \ldots + u(r-1)\alpha + qr\alpha = \alpha(w-u+\tfrac{1}{2}r^2u - \tfrac{1}{2}ru+rq).$$

Since $r \geqslant 2$ and $u \geqslant 1$, we have $\frac{1}{2}ru \geqslant \frac{1}{2}r+u-1$, hence

$$\begin{aligned}\sum_{c \in C} \lambda(c) &\leqslant \alpha(1+w-2u+\tfrac{1}{2}r^2u - \tfrac{1}{2}r+rq) \\ &\leqslant \alpha(\tfrac{1}{2}r^2u - \tfrac{1}{2}r+rq) = \tfrac{1}{2}\alpha r(ru-1+2q).\end{aligned}$$

Using (33) to eliminate r, we get

$$\sum_{c\in C}\lambda(c)\leqslant\frac{a}{2u}(2k-1+2u-w-q)(2k-2+2u-w+q)$$
$$\leqslant\frac{a}{2u}(2k-1+2u-w)(2k-2+2u-w).$$

Hence

$$\sum_{c\in C}\lambda(c)\leqslant\begin{cases}\dfrac{a}{w+2}(2k+1)(2k) & \text{if } w \text{ is even},\\[2mm] \dfrac{a}{w+1}(2k)(2k-1) & \text{if } w \text{ is odd}.\end{cases}$$

Since $w\leqslant 2k-2$, $\dfrac{2k+1}{w+2}<\dfrac{2k}{w+1}$, hence

$$\sum_{c\in C}\lambda(c)<\frac{4k^2a}{w+1}.$$

On the other hand $\sum_{c\in C}\lambda(c)\geqslant k^2$, exactly as in Case 1, so $a>\frac{1}{4}(w+1)$. Hence $a\geqslant\frac{1}{4}(w+2)$ and the lemma is proved.

References

[1] P. Erdös and H. Heilbronn, *On the addition of residue classes* mod p, Acta Arith. 9 (1964), pp. 149–159.

[2] J. H. B. Kemperman, *On complexes in a semigroup*, Indag. Math. 18 (1956), pp. 247–254.

[3] J. E. Olson, *An addition theorem modulo p*, J. Combinatorial Theory 5 (1968), pp. 45–52.

[4] E. Szemerédi, *On a conjecture of Erdös and Heilbronn*, Acta Arith. 17 (1970), pp. 227–229.

DEPARTMENT OF MATHEMATICS
PENNSYLVANIA STATE UNIVERSITY
University Park, Pennsylvania

Received on 29. 3. 1974 (548)

ACTA ARITHMETICA
XXVIII (1975)

A note on a cyclotomic diophantine equation

by

VEIKKO ENNOLA (Turku)

1. Introduction. Let $m\geqslant 3$ be a natural number, $\zeta_m=\exp(2\pi i/m)$, and let $K_m=Q(\zeta_m)$ denote the cyclotomic field over the rationals Q. We shall prove the following result:

THEOREM A. *If $q\geqslant 3$, β is a unit in K_m, and the equation*

$$(1)\qquad a^q=\beta+1$$

has a solution $a\in K_m$, then $a=0$ or a is a root of unity.

In the special case when m is a prime >3 and a is required to be a unit in K_m, this result has been recently proved by Newman [5]. His proof depends on the following theorem (for prime values of m):

THEOREM B. *If m is any integer $\geqslant 4$, $2\leqslant g\leqslant m-2$, and $q\geqslant 2$, then the only solution $a\in K_m$ of the equation*

$$(2)\qquad 1+\zeta_m+\zeta_m^2+\ldots+\zeta_m^{g-1}=a^q$$

is given by $q=2$, $m=12$, $g=7$, $a=\pm\zeta_m^5(1-\zeta_m)^{-1}$.

In particular, if m is prime, then (2) does not have solutions with $q\geqslant 2$. This fact was stated as a conjecture by Newman [4] and was first proved by the author [1]. A very elegant proof of a more general result was given by Loxton [3]. The proof given by Newman [5] is incorrect. (The formula for $\eta^n-\zeta$ on p. 87 is wrong.) In the general case Theorem B has been proved by the author [2].

Using the ideas of Newman we shall prove Theorem A directly without leaning on Theorem B. It is possible that the new method will cause a simplification in the proof of Theorem B which is extremely complicated.

2. Proof of Theorem A. We assume that (1) has a solution, where a is nonzero and not a root of unity, and deduce a contradiction. Without loss of generality, we may assume that $q=4$ or that q is an odd prime. By extending the field K_m if necessary, we may also assume that $q|m$. We use the following well-known fact: If γ is any unit in K_m, then there