ACTA ARITHMETICA
101.2 (2002)

On additive bases with two elements

by

Giampiero Chiaselotti (Cosenza)

1. Introduction. Let G be a finite abelian additive group. If S is a non-empty subset, we set

$$\Sigma(S)=\Big\{\sum_{x\in B}x\ \Big|\ B\subseteq S, B\neq\emptyset\Big\}$$

and

$$X=\{m\in\mathbb{N}\mid \text{ if } S\subseteq G\setminus\{0\},\ |S|\geq m \text{ then } \Sigma(S)=G\}.$$

Let us observe that $X\neq\emptyset$ if $|G|>2$, since $|G|-1\in X$. The number

$$c(G)=\min\{m\mid m\in X\}$$

is called the *critical number* of G. It was first studied by Erdős and Heilbronn [4] for $G=\mathbb{Z}_p$, with p a prime number. Recently the parameter $c(\mathbb{Z}_q)$ has been studied for various values of q (see [4], [9], [1], [8]).

For evaluation of $c(G)$ for more general groups, the work of Diderrich [2] was fundamental. He proved that $p+q-2\leq c(G)\leq p+q-1$ if G is an abelian group of order pq, with p,q prime numbers. Moreover he conjectured that $c(G)=p+h-2$ if $|G|=ph$, where p is the smallest prime dividing $|G|$ and h is a composite integer. First, this conjecture was checked in special cases: for $p=2$ in [3], for $p\geq 43$ in [5], and for $p=3$ in [7]. Then Gao and Hamidoune [6] gave a complete proof of the conjecture.

In additive number theory we usually ask what may be said about the set $M+M$, for a given subset M of some additive structure; in particular when $M+M$ is the whole structure. In this note, if S is a non-empty subset of a finite abelian group G, we set

$$\Sigma_k(S)=\Big\{\sum_{x\in B}x\ \Big|\ B\subseteq S,\ |B|=k\Big\},$$

for any integer k with $1\leq k\leq|S|$, and we study when the subset $\Sigma_2(S)$ of $S+S$ is the whole G.

2000 *Mathematics Subject Classification*: 11B75, 20K09.

For this purpose, for integer $k \leq |G|-1$ we define

$$X_k = \{m \in \mathbb{N} \mid \forall S \subseteq G \setminus 0,\ |S| \geq m \Rightarrow \Sigma_k(S) = G\}$$

and call the number

$$c_k(G) = \min\{m \mid m \in X_k\}$$

the kth *critical number* of G. For some integer k the set X_k can be empty; in this case we set formally $c_k(G) = \infty$. If $k = 1$ note that $c_1(G) = \infty$, since if $S \subseteq G \setminus \{0\}$ we have $\Sigma_1(S) = S \neq G$. Here we determine the 2nd critical number of any finite abelian group G in terms of the order of its subgroup of elements of order 2. More precisely, if $H_G = \{2g \mid g \in G\}$ and $K_G = \{g \in G \mid 2g = 0\}$, we prove that

$$c_2(G) = \begin{cases} (|G| + |K_G|)/2 + 1 & \text{if } H_G \neq \{0\}, \\ \infty & \text{if } H_G = \{0\}. \end{cases}$$

Finally, note that $c(G) \leq c_k(G)$ for any integer k with $1 \leq k \leq |G|$.

2. The results. First we observe that the number $|G| + |K_G|$ is even. In fact, if $|G|$ is odd, then $K_G = \{0\}$. If $|G|$ is even, then $K_G \neq \{0\}$ and any element of $K_G \setminus \{0\}$ has order 2; therefore $|K_G|$ is a power of 2.

THEOREM 2.1. *Let G be an abelian group of order n. Set*

$$H_G = \{2g \mid g \in G\} \quad \textit{and} \quad K_G = \{g \in G \mid 2g = 0\}.$$

Then

$$c_2(G) = \begin{cases} (|G| + q)/2 + 1 & \textit{if } H_G \neq \{0\}, \\ \infty & \textit{if } H_G = \{0\}, \end{cases}$$

where $q = |K_G|$.

Proof. Let $\phi : G \to G$ be the homomorphism $\phi : x \mapsto 2x$; then we have $\operatorname{Ker}\phi = K_G$ and $\operatorname{Im}\phi = H_G$, therefore $G/K_G \cong H_G$. If $H_G = \{0\}$ then $G = K_G$; this implies that each element in $G \setminus \{0\}$ has order 2. In this case 0 cannot be the sum of two distinct elements of G; hence for each subset $S \subseteq G \setminus \{0\}$ we have $\Sigma_2(S) \neq G$, i.e. $c_2(G) = \infty$. We can therefore assume that $H_G \neq \{0\}$ (in this case note that $n \geq 2q$ since $|H_G| \geq 2$).

Let S be a non-empty subset of G such that $0 \notin S$ and $|S| \geq (n+q)/2+1$. Let $a \in G$. We claim that $a \in \Sigma_2(S)$. Let $a_1, \ldots, a_m$ be $m = (n+q)/2+1$ distinct elements of S. We set

$$A = \{a_1, \ldots, a_m\}, \qquad B = a - A = \{a - a_1, \ldots, a - a_m\}.$$

Since $|G| = n \geq |A \cup B| = |A| + |B| - |A \cap B|$, it follows that

$$|A \cap B| \geq 2m - n = 2\left(\frac{n+q}{2} + 1\right) - n = q + 2.$$

There exist therefore $q+2$ distinct elements $a_{i_1},\dots,a_{i_{q+2}}$ of A such that

$$a_{i_1} = a - a_{j_1},\ \dots,\ a_{i_{q+2}} = a - a_{j_{q+2}},$$

where $a_{j_1},\dots,a_{j_{q+2}}$ are elements of A. We obtain

$$a = a_{i_1} + a_{j_1} = \dots = a_{i_{q+2}} + a_{j_{q+2}},$$

where $a_{i_1},\dots,a_{i_{q+2}},a_{j_1},\dots,a_{j_{q+2}}$ are elements of A.

Now, if $a_{i_k} \neq a_{j_k}$ for some $k \in \{1,\dots,q+2\}$, then $a = a_{i_k} + a_{j_k} \in \Sigma_2(S)$; thus now we suppose that

$$a_{i_1} = a_{j_1},\ \dots\ , a_{i_{q+2}} = a_{j_{q+2}},$$

i.e.

$$a = 2a_{i_1} = 2a_{i_2} = \dots = 2a_{i_{q+2}}. \tag{1}$$

Set $K_a = \{x \in G \mid 2x = a\}$. By (1) it follows that $K_a \neq \emptyset$. For every $c \in K_a$ the map $K_G \to K_a$, $x \mapsto x + c$, is onto and one-to-one; whence $q = |K_G| = |K_a|$. This implies that G contains exactly q distinct elements, say $y_1,\dots,y_q$, for which $2y_i = a$ $(i = 1,\dots,q)$; but this contradicts (1) since $a_{i_1},\dots,a_{i_{q+2}}$ are themselves distinct. Thus we have proved our claim. This also proves that $c_2(G) \leq (n+q)/2 + 1$. We now want to construct a subset $S \subseteq G\setminus\{0\}$ having exactly $(n+q)/2$ distinct elements and such that $\Sigma_2(S) \neq G$.

Let $a \in H_G \setminus \{0\}$. By definition of H_G there exists $c \in G\setminus\{0\}$ such that $2c = a$. If $K_G + c$ is the coset $\{k + c \mid k \in G\}$, we have $|G \setminus (K_G + c)| = n - q$ (where $n-q$ is even ≥ 2 since $n \geq 2q$, say $n - q = 2m$). We now observe that $G\setminus(K_G+c)$ can be partitioned into disjoint pairs of the type $\{x, a-x\}$, with $a - x \neq x$. In fact, if $x \in G \setminus (K_G + c)$, also $a - x \in G \setminus (K_G + c)$ (otherwise $a - x = k + c$ with $k \in K_G$ implies $x = -k - c + a = -k - c + 2c = -k + c$, which is absurd); moreover, $a - x \neq x$ (otherwise $a = 2x = 2c$ implies $2(x - c) = 0$, i.e. $x - c \in K_G$). Now, since two pairs $\{x, a - x\}$, $\{y, a - y\}$ with $x, y \in G \setminus (K_G + c)$ either coincide or are disjoint, we can suppose that $G \setminus (K_G + c)$ has the form

$$\{x_1,\dots,x_m, a - x_1,\dots,a - x_m\},$$

where $m = (n - q)/2$.

First assume that $0 \notin \{x_1,\dots,x_m\}$. In this case we set

$$S = \{x_1,\dots,x_m\} \cup (K_G + c).$$

Then $0 \notin S$ (if $0 \in K_G + c$, then $c \in K_G$ implies that $0 = 2c = a$, which is impossible) and $|S| = m + q = (n - q)/2 + q = (n + q)/2$. We prove that $a \notin \Sigma_2(S)$. In fact, $a \in \Sigma_2(S)$ if and only if one of the following conditions is satisfied:

(i) $a = x_i + x_j$, where $i, j \in \{1, \dots, m\}$ and $i \neq j$; but then $a - x_j = x_i \in S$, and this contradicts the definition of S.

(ii) $a = x_i + (k + c)$, where $i \in \{1, \dots, m\}$ and $k \in K_G$; in this case we have $x_i = a - k - c = 2c - k - c = -k + c \in K_G + c$, which is impossible.

(iii) $a = (k+c)+(\overline{k}+c)$, where k and $\overline{k}$ are two distinct elements of K_G; but then $a = k + \overline{k} + 2c = k + \overline{k} + a$ implies $k + \overline{k} = 0$ and since $k \in K_G$ we also have $k + k = 0$, i.e. $k = \overline{k}$, which is absurd. Hence $a \notin \Sigma_2(S)$.

If $0 \in \{x_1, \dots, x_m\}$, then $0 \notin \{a - x_1, \dots, a - x_m\}$ and thus we set

$$S = \{a - x_1, \dots, a - x_m\} \cup (K_G + c).$$

In this case we also have $0 \notin S$, $|S| = (n+q)/2$ and $a \notin \Sigma_2(S)$ (the conditions analogous to (i)–(iii) are excluded in the same way as above). Hence in both cases $a \notin \Sigma_2(S)$ and thus $\Sigma_2(S) \neq G$. This shows that $c_2(G) \geq (n+q)/2+1$. Hence

$$c_2(G) = \frac{n+q}{2} + 1 \quad \text{if } H_G \neq \{0\}. \ \blacksquare$$

Corollary. *Let $\mathbb{Z}_n$ be the group of integers modulo n, with $n > 2$. Then*

$$c_2(\mathbb{Z}_n) = \begin{cases} (n+3)/2 & \text{if } n \text{ is odd,} \\ (n+4)/2 & \text{if } n \text{ is even.} \end{cases}$$

Proof. If n is odd, we have $K_{\mathbb{Z}_n} = \{0\}$ and $H_{\mathbb{Z}_n} = \mathbb{Z}_n \neq \{0\}$; if n is even, then $K_{\mathbb{Z}_n} = \{0, n/2\}$ and $H_{\mathbb{Z}_n} \neq \{0\}$ since $|H_{\mathbb{Z}_n}| = n/2 \neq 0$. In both cases the result follows directly from Theorem 2.1. ∎

Finally note that if G is an abelian group of order n and $S \subseteq G \setminus \{0\}$ has at least $\lceil n/2 \rceil + 1$ elements, then $G \setminus H_G \subseteq \Sigma_2(S)$.

In fact, let $a \in G \setminus H_G$ and take $m = \lceil n/2 \rceil$ elements $a_1, \dots, a_m$ in S. We set

$$A = \{a_1, \dots, a_m\} \quad \text{and} \quad B = \{a - a_1, \dots, a - a_m\}.$$

Now, if $a_i = a - a_j$ for some pair i, j with $i \neq j$, then $a = a_i + a_j \in \Sigma_2(S)$; on the other hand the condition $a_i = a - a_i$ cannot be satisfied because $a \notin H_G$. We can suppose therefore that $A \cap B = \emptyset$. Then

$$|A \cup B| = |A| + |B| = 2\left\lceil \frac{n}{2} \right\rceil \geq n$$

implies that $A \cup B = G$. Hence the remaining element of $S \setminus A$ must be contained in B. This proves that $a \in \Sigma_2(S)$, i.e. $G \setminus H_G \subseteq \Sigma_2(S)$.

References

[1] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic subspaces of Grassmann derivations*, Bull. London Math. Soc. 26 (1994), 140–146.

[2] G. T. Diderrich, *An addition theorem for abelian groups of order pq*, J. Number Theory 7 (1975), 33–48.
[3] G. T. Diderrich and H. B. Mann, *Combinatorial problems in finite abelian groups*, in: A Survey of Combinatorial Theory, J. L. Srivasta *et al.* (eds.), North-Holland, Amsterdam, 1973, 95–100.
[4] P. Erdős and H. Heilbronn, *On the addition of residue classes* mod p, Acta Arith. 9 (1964), 149–159.
[5] W. Gao, *On the size of additive bases of finite groups*, preprint, 1997.
[6] W. Gao and Y. O. Hamidoune, *On additive bases*, Acta Arith. 88 (1999), 233–237.
[7] Y. O. Hamidoune, A. S. Lladó and O. Serra, *On sets with a small subset sum*, Combin. Probab. Comput. 8 (1999), 461–466.
[8] E. Lipkin, *Subset sums of sets of residues*, Astérisque 258 (1999), xiii, 187–193.
[9] J. E. Olson, *An addition theorem modulo p*, J. Combin. Theory 5 (1968), 45–52.

Dipartimento di Matematica
Università della Calabria
87036 Arcavacata di Rende (Cosenza)
Italy
E-mail: chiaselo@unical.it

Received on 3.8.2000
and in revised form on 18.12.2000 (3862)