ACTA ARITHMETICA
LXXXVIII.3 (1999)

On additive bases

by

W. Gao (Beijing) and Y. O. Hamidoune (Paris)

1. Introduction. By p we shall denote a prime number. The group of integers modulo n will be denoted by $\mathbb{Z}_n$. Let G be an abelian group and let S be a subset of G. As usual, we write

$$\Sigma(S) = \Big\{ \sum_{x \in A} x \ \Big|\ A \subset S \Big\}.$$

The *critical number* of G, denoted by $c(G)$, is the smallest s such that $\Sigma(S) = G$ for every subset S of G with cardinality s not containing 0.

The parameter $c(G)$ was first studied by Erdős and Heilbronn in [4]. They obtained the inequality $c(\mathbb{Z}_p) \le 3\sqrt{6p}$. Olson proved in [13] that $c(\mathbb{Z}_p) \le \sqrt{4p-3}+1$. The authors of [1] obtained the inequality $c(\mathbb{Z}_p) \le \sqrt{4p-7}$.

The evaluation of $c(G)$ for groups with composite order was first considered by Mann and Olson. They obtained the inequality $c(\mathbb{Z}_p \oplus \mathbb{Z}_p) \le 2p-1$ in [11]. Mann and Wou proved that $c(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 2p-2$ in [12]. Diderrich proved in [2] the inequality $p+q-2 \le c(G) \le p+q-1$, where G is an abelian group of order pq and q is a prime. He conjectured that $c(G) = |G|/p + p - 2$ if $|G|/p$ is composite, where p is the smallest prime dividing $|G|$. This conjecture is proved by Diderrich and Mann in [3] for $p = 2$. Peng [15] proved Diderrich's conjecture if G is the additive group of a finite field. Lipkin [9] obtained a proof of this conjecture in the case of cyclic groups with large order. This conjecture is proved by one of the present authors in [5] for $p \ge 43$ and by the authors of [8] for $p = 3$.

In this paper we achieve the evaluation of $c(G)$, solving the above mentioned conjecture.

2. Some tools. Recall the following well known and easy lemma.

Lemma 2.1 [10]. *Let G be a finite group. Let X and Y be subsets of G such that $X + Y \ne G$. Then $|X| + |Y| \le |G|$.*

1991 *Mathematics Subject Classification*: 11B75, 20K09.

We use the following result.

LEMMA 2.2 [2]. *Let p, q be two primes and let G be an abelian group with order pq. Let S be a subset of G such that $0 \notin S$ and $|S| = p + q - 1$. Then $\Sigma(S) = G$.*

Let G be an abelian group. Let $B \subset G$ and $x \in G$. As usual, we write $\lambda_B(x) = |(B + x) \setminus B|$. For any B, x, Olson proved in [13, 14]

$$\lambda_B(x) = \lambda_B(-x) \tag{1}$$

and

$$\lambda_B(x) = \lambda_{G\setminus B}(x). \tag{2}$$

We use the following property which is implicit in [13]: Let G be a finite abelian group. Let S be a subset of G such that $0 \notin S$. Put $B = \Sigma(S)$. For every $y \in S$, we have

$$|\Sigma(S)| \geq |\Sigma(S \setminus y)| + \lambda_B(y). \tag{3}$$

We also use the following result of Olson.

LEMMA 2.3 (Olson [14]). *Let G be an abelian group and let S be a generating subset of G such that $0 \notin S$. Let B be a subset of G such that $|B| \leq |G|/2$. Then there is $x \in S$ such that*

$$\lambda_B(x) \geq \min((|B| + 1)/2, (|S \cup -S| + 2)/4).$$

This result follows, using (1), by applying Lemma 3.1 of [14] to $S \cup -S$.

We use the following lemma which is a consequence of the main result in [6].

LEMMA 2.4 [6]. *Let S be a subset of an abelian group G such that $S \cap -S = \emptyset$. Then*

$$|\Sigma(S)| \geq 2|S|.$$

The proof follows easily by induction. Set $B = \Sigma(S)$. By Lemma 2.3 applied to B or $G \setminus B$ and using (2), there is $s \in S$ such that $\lambda_B(s) \geq 2$. By (3), $|B| \geq |\Sigma(S \setminus x)| + 2 \geq 2|S|$. ■

3. The main result. Let X be a subset of G with cardinality k. Let $\{x_i; 1 \leq i \leq k\}$ be an ordering of X. For $0 \leq i \leq k$, set $X_i = \{x_j \mid 1 \leq j \leq i\}$ and $B_i = \Sigma(X_i)$. The ordering $\{x_1, \ldots, x_k\}$ will be called a *resolving sequence* of X if for all i, $\lambda_{B_i}(x_i) = \max\{\lambda_{B_i}(x_j); 1 \leq j \leq i\}$. The *critical index* of the resolving sequence is the smallest integer t such that X_{t-1} generates a proper subgroup of G.

Clearly, every nonempty subset S not containing 0 admits a resolving sequence. Moreover, the critical index is ≥ 1.

We shall write $\lambda_i = \lambda_{B_i}(x_i)$. By induction we have, using (3), for all $1 \le j \le k$,

$$|\Sigma(X)| \ge \lambda_k + \ldots + \lambda_j + |B_{j-1}|.$$

Put $\delta(m) = 0$ if m is odd and $= 1$ otherwise. By Lemma 2.3, $\lambda_i \ge (i + 1 + \delta(i))/2$ for all $i \ge t$. In particular, for all $s \ge t$,

$$|\Sigma(X)| \ge (k + s + 3)(k - s + 1)/4 - 1/2 + |B_{s-1}|. \tag{4}$$

Theorem 3.1. *Let G be a finite abelian group with odd order and let p be the smallest prime dividing $|G|$. Let S be a subset of G such that $0 \notin S$ and $|S| = |G|/p + p - 2$. If $|G|/p$ is composite, then $\Sigma(S) = G$.*

Proof. Set $|G| = n$. One may check easily the result for $n = 27$. Suppose $n > 27$. Set $k(n) = (n/p + p - 2)/2$. We shall write sometimes k instead of $k(n)$. Clearly we may partition $S = X \cup Y$ so that $|X| = |Y| = k$, $X \cap -X = Y \cap -Y = \emptyset$ and $|\Sigma(X)| \le |\Sigma(Y)|$.

The result holds by Lemma 2.1 if $|\Sigma(X)| > n/2$. Suppose the contrary. Since n is odd, we have

$$|\Sigma(X)| \le (n - 1)/2. \tag{5}$$

Let $\{x_i; 1 \le i \le k\}$ be a resolving sequence for X with critical index t.

We first prove that

$$t \ge 4. \tag{6}$$

Suppose on the contrary that $t \le 3$. By (5) and (4) applied with $s = 3$,

$$4 + (k - 2)(k + 6)/4 - n/2 \le 0. \tag{7}$$

Put $f(n) = 4 + (k(n) - 2)(k(n) + 6)/4 - n/2$. Observe that $f'(n) \ge 0$. Hence $f(n)$ is increasing as a function of n. Since $n \ge p^3$, we have by (7), $f(p^3) \le 0$. Hence $p^4 - 6p^3 + 5p^2 + 4p + 4 \le 0$. It follows that $p = 3$. But in this case $n > 27$ and hence $n \ge p^3 + 2p^2 = 45$. It follows that $f(n) \ge f(45) = 5/2$, contradicting (7).

By Lemma 2.4, $|B_{t-1}| \ge 2(t-1)$. Obviously $|B_t| = |B_{t-1}| + |x_t + B_{t-1}| = 2|B_{t-1}| \ge 4(t - 1)$.

By (5) and (4), applied with $s = t + 1$,

$$4t - 4 + (k - t)(k + t + 4)/4 - n/2 \le 0. \tag{8}$$

Set $F(t, n) = 4t - 4 + (k(n) - t)(k(n) + t + 4)/4 - n/2$. Notice that $\frac{\partial}{\partial t} F(t, n) = 3 - t/2$. Let us show that

$$t \ge 6. \tag{9}$$

Suppose on the contrary that $4 \le t \le 5$. Clearly $F(5, n) > F(4, n)$, and $F(4, n)$ is an increasing function of n. Now by (8), we have $F(4, p^3) \le 0$. It follows that $p^4 - 6p^3 + 5p^2 + 4p + 52 \le 0$, a contradiction.

Let us show that

$$t \geq n/p^2 + p - 1. \tag{10}$$

Assume the contrary and set $G(n) = F(n/p^2+p-2, n)$. Since $n/p^2+p-2 \geq 6$ (we recall that $n > 27$), we have by (8),

$$G(n) \leq 0. \tag{11}$$

Observe that $G'(n) = 4/p^2 + n/(8p^2) - 1/(4p) - n/(2p^4) - 3/8 \geq 0$. In particular $G(n)$ is an increasing function. By (11), we have $p^4 - 6p^3 - 11p^2 + 132p - 188 \leq 0$, contradicting (11).

Let H be the proper subgroup generated by X_{t-1}. Let p' be the smallest prime divisor of n/p. By (10), $|H \cap S| \geq n/(pp') + p' - 1$. If n/p is the product of two primes, then by Lemma 2.2, $\Sigma(S \cap H) = H$. If n/p is the product of more than two primes, then by the induction hypothesis, $\Sigma(S \cap H) = H$.

Since $|H| > n/(pp')$, we see easily that $q = |G|/|H|$ is a prime. Clearly $|S \setminus H| \geq q - 1$. Let $a_1, \ldots, a_{q-1}$ be distinct elements from $S \setminus H$. We denote by $\overline{a}_i$ the image of a_i in G/H under the canonical morphism.

By the Cauchy–Davenport Theorem (cf. [10]), $\{0, \overline{a}_1\} + \ldots + \{0, \overline{a}_{p-1}\} = G/H$. It follows that $\Sigma(a_1, \ldots, a_{p-1}) + H = G$. The theorem now follows since $\Sigma(S \cap H) = H$. ∎

Acknowledgements. This joint paper was written when the first author held an Austrian Lise Meitner Fellowship (Project No. M00397-MAT). He would like to thank the FWF for the assistance and Alfred Geroldinger for his hospitality.

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, October 1997.

[6] Y. O. Hamidoune, *Adding distinct congruence classes* , Combin. Probab. Comput. 7 (1998), 81–87.

[7] Y. O. Hamidoune and G. Zémor, *On zero-free subset sums*, Acta Arith. 78 (1996), 143–152.

[8] Y. O. Hamidoune, A. S. Lladó and O. Serra, *On sets with a small subset sum*, Combin. Probab. Comput., to appear.

[9] E. Lipkin, *Subset sums of sets of residues*, in: Conference on the Structure Theory of Set Addition, CIRM, Marseille, 1993, 187–197.
[10] H. B. Mann, *Addition Theorems*, 2nd ed., R. E. Krieger, New York, 1976.
[11] H. B. Mann and J. E. Olson, *Sums of sets of elements in the elementary abelian group of type* (p, p), J. Combin. Theory 2 (1967), 275–284.
[12] H. B. Mann and Y. F. Wou, *Addition theorem for the elementary abelian group of type* (p, p), Monatsh. Math. 102 (1986), 273–308.
[13] J. E. Olson, *An addition theorem modulo* p, J. Combin. Theory 5 (1968), 45–52.
[14] —, *Sums of sets of group elements*, Acta Arith. 28 (1975), 147–156.
[15] C. Peng, *An addition theorem in elementary abelian groups*, J. Number Theory 27 (1987), 58–62.

Department of Computer Science
and Technology
University of Petroleum
Shangping Shiuku Road
Beijing 10200, China
E-mail: wdgao@publlc.fhnet.cn.net

Université P. et M. Curie
E. Combinatoire
Case 189
4, Place Jussieu
75252 Paris Cedex, France
E-mail: yha@ccr.jussieu.fr

Received on 3.3.1998
and in revised form on 21.9.1998 (3347)