ARTICLE IN PRESS

Available online at www.sciencedirect.com

ScienceDirect

Discrete Mathematics ▮▮▮ (▮▮▮▮) ▮▮▮–▮▮▮

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Note

Addition theorems on the cyclic groups of order p^ℓ

W.D. Gao[a], R. Thangadurai[b], J. Zhuang[c]

[a] Center for Combinatorics, Nankai University, Tianjin 300071 China
[b] School of Mathematics, Harish Chandra Research Institute, ChhatnagRoad, Jhusi, Allahabad 211019, India
[c] Department of Mathematics, Dalian University of Technology, Dalian, 116024, China

Received 15 September 2006; received in revised form 7 April 2007; accepted 18 April 2007

Abstract

Let p be a prime number and ℓ be any positive integer. Let G be the cyclic group of order p^ℓ and let S be any sequence in G of length $p^\ell + k$ for some positive integer $k \geqslant p^{\ell-1} - 1$ such that S do not admit a subsequence of length p^ℓ whose sum is zero in G. Then we prove that there exists an element of G which appears in S at least $k+1$ times.

MSC: primary 20D60secondary 11P70

Keywords: Inverse problems; Zero-sum problems; Finite abelian groups

1. Introduction

Throughout this paper, let G be an additive finite abelian group. Let $S = (a_1, a_2, \ldots, a_k)$ be a sequence (not necessarily distinct) of elements in G of length k. Define $\sigma(S) = \sum_{i=1}^{k} a_i$. For any integer r such that $1 \leqslant r \leqslant k$, we denote

$$\sum\nolimits_r(S) = \{a_{i_1} + a_{i_2} + \cdots + a_{i_r} | 1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant k\},$$

and $\sum_{\leqslant r}(S) = \bigcup_{m=1}^{r}(\sum_m(S))$. Thus, in our notation, we write $\sum(S) = \sum_{\leqslant k}(S)$ where $k = |S|$. Let $\mathsf{h} = \mathsf{h}(S)$ denote the maximal number of an element $a \in G$ appearing in S. Let $\mathscr{F}(G)$ be the free monoid, multiplicatively written, with basis G. For convenience, we regards S as an element of $\mathscr{F}(G)$ and write $S = a_1 a_2 \cdots a_k$. Also, we follow the same terminologies and notations as in the survey article [8] or in the recent book [11].

In 1961, Erdős–Ginzburg–Ziv [3] proved the following theorem (which we call EGZ Theorem). Let C_m denote the cyclic group of order m.

EGZ Theorem. *If* $S \in \mathscr{F}(C_m)$ *of length* $2m-1$, *then* $0 \in \sum_m(S)$. In other words, we have $\mathsf{s}(C_m) = 2m-1$.

The EGZ Theorem is tight in the following sense. It is clear that $S = 0^{m-1}1^{m-1}$ in $\mathscr{F}(C_m)$ of length $2m-2$ satisfies $0 \notin \sum_m(S)$.

E-mail addresses: gao@cfc.nankai.edu.cn (W.D. Gao), thanga@hri.res.in (R. Thangadurai), jjzhuang@eyou.com (J. Zhuang).

0012-365X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2007.04.040

Please cite this article as: W.D. Gao, et al., Addition theorems on the cyclic groups of order p^ℓ, Discrete Math. (2007), doi: 10.1016/j.disc.2007.04.040

The inverse problem to EGZ theorem (see for instance, [2]) is, for every integer k satisfying $1 \leqslant k \leqslant m-2$, to describe the structure of $S \in \mathscr{F}(C_m)$ with $|S| = m + k$ and $0 \notin \sum_m(S)$. When $k = m - 2$, the inverse problem was solved by Yuster and Peterson [14] and Bialostocki and Dierker [1]; $k = m - 3$ was solved by Flores and Ordaz [4]; and when $m - [(m+1)/4] - 1 \leqslant k \leqslant m - 2$, the inverse problem was tackled by Gao [7]. Also, for $m = p$, a prime number, Gao et al. [9] solved this inverse problem when $p - [(p+1)/3] - 1 \leqslant k \leqslant p - 2$. But it becomes difficult to describe the structure of S completely, when k is much smaller than m.

Instead of describing the structure of S completely, one considers the problem of determining the following constant. For $k \in \mathbb{N}$ we define

$$\mathsf{h}(G, k) = \min \left\{ \mathsf{h}(S) | S \in \mathscr{F}(G) \quad \text{with } |S| = |G| + k \quad \text{and} \quad 0 \notin \sum_{|G|}(S) \right\}.$$

The main result in [7] implies that $\mathsf{h}(C_m, k) \geqslant k + 1$ whenever $m - [(m+1)/4] - 1 \leqslant k \leqslant m - 2$. Also, the authors in [10] shows that $\mathsf{h}(C_p, k) \geqslant k + 1$ for every prime p and every k such that $1 \leqslant k \leqslant p - 2$. It is natural to ask whether $\mathsf{h}(C_m, k) \geqslant k + 1$ holds for every k such that $1 \leqslant k \leqslant m - 2$. We conjecture the following.

Conjecture 1. Let $m \geqslant 2$ be any integer and let k be an integer such that $1 \leqslant k \leqslant m - 2$. Then $\mathsf{h}(C_m, k) \geqslant k + 1$.

In this article, we prove the following theorem.

Theorem 1. *Let $m = p^\ell$ for some prime p and some integer $\ell > 1$. If $p^{\ell-1} - 1 \leqslant k \leqslant p^\ell - 2$ then $\mathsf{h}(C_m, k) \geqslant k + 1$.*

Using the same technique of the proof of Theorem 1, we shall be able to prove the following theorem.

Theorem 2. *Let p be a prime, and ℓ be any positive integer. Let S be a sequence in $C_{p^\ell} \setminus \{0\}$ of length p^ℓ. If $\mathsf{h} = \mathsf{h}(S) \geqslant p^{\ell-1} - 1$, then,*

$$\sum_{\leqslant \mathsf{h}}(S) = \sum(S).$$

Further, we conjecture the following.

Conjecture 2. Let $m \geqslant 2$ be any integer. If S is a sequence of elements in $C_m \setminus \{0\}$ of length $|S| = m$, then, $\sum_{\leqslant \mathsf{h}}(S) = \sum(S)$ where $\mathsf{h} = \mathsf{h}(S)$.

2. Main theorems

As already mentioned in Section 1, our terminology and notations are consistent with the survey article [8]. For convenience we repeat some key notions, and moreover we formulate our main tools. Every group homomorphism $\varphi : G \to H$ extends to a homomorphism $\varphi : \mathscr{F}(G) \to \mathscr{F}(H)$ which maps a sequence $S = g_1 \cdot \dots \cdot g_l$ to $\varphi(S) = \varphi(g_1) \cdot \dots \cdot \varphi(g_l)$.

Let $A, B \subset G$ be non-empty subsets. Then the stabilizer of A is denoted by $\mathrm{Stab}(A)$ and defined as $\mathrm{Stab}(A) = \{g \in G \mid g + A = A\}$. This is the maximal subgroup $H \subset G$ such that $A + H = A$, and A is the union of cosets of $\mathrm{Stab}(A)$ in G (see [[11, Proposition 5.2.3]). For $g \in G$, let

$$r_{A,B}(g) = |\{(a, b) \in A \times B | g = a + b\}| = |A \cap (g - B)|$$

denote the number of representations of g as a sum of an element of A and an element of B. Proofs of the following results may be found in ([13, Theorem 4.4]) and [11, Theorems 5.2.10 and 5.7.3]). Theorem 2.3 was first proved in [5] and for the sake of completion, we shall present a different proof.

Theorem 2.1 (*Kneser*). *If $h \in \mathbb{N}$, $A_1, \dots, A_h \subset G$ are non-empty subsets and H the stabilizer of $A_1 + \dots + A_h$, then*

$$|A_1 + A_2 + \dots + A_h| \geqslant |A_1| + |A_2| + \dots + |A_h| - (h-1)|H|.$$

Please cite this article as: W.D. Gao, et al., Addition theorems on the cyclic groups of order p^ℓ, Discrete Math. (2007), doi: 10.1016/j.disc.2007.04.040

Theorem 2.2 (*Kemperman–Scherk*). *If $A, B \subset G$ are non-empty subsets, then*

$$|A+B| \geqslant |A| + |B| - \min\left\{r_{A,B}(g) | g \in A+B\right\}.$$

Theorem 2.3 (*Gao*). *Let $S \in \mathscr{F}(G)$ be a sequence of length $|S| \geqslant |G|$, $h' = \max\{\mathrm{ord}(g) | g \in \mathrm{supp}(S)\}$ and $h = \min\{\mathsf{h}(S), h'\}$. Then $0 \in \sum_{\leqslant h}(S)$.*

Proof. If $h(S) \geqslant h'$ then $h = h'$, and some element g occurs in S at least $\mathrm{ord}(g)$ times. Therefore, $g^{\mathrm{ord}(g)}$ is a zero-sum subsequence of S. Hence, $0 \in \sum_{\mathrm{ord}(g)}(S) \subset \sum_{\leqslant h}(S)$. So, we may assume that $h(S) < h'$. Thus, $\mathsf{h} = \mathsf{h}(S)$, and one can distribute the terms of S into h disjoint non-empty subsets $B_1, \ldots, B_h$ of G. For any two non-empty subsets A, B of G, let $A \oplus B = A \cup B \cup (A+B)$, and the definition can be generalized to three or more subsets by induction.

Assume to the contrary that $0 \notin \sum_{\leqslant h}(S)$, then $0 \notin B_i$ and

$$0 \notin B_1 \oplus B_2 \subset B_1 \oplus B_2 \oplus B_3 \subset \cdots \subset B_1 \oplus B_2 \oplus B_3 \oplus \cdots \oplus B_h.$$

Set $A_i = \{0\} \cup B_i$ for $i = 1, \ldots, h$. Applying Theorem 2.2 to $A_1 + A_2$, we get,

$$|A_1 + A_2| \geqslant |A_1| + |A_2| - 1 = |B_1| + |B_2| + 1.$$

Since $0 \notin B_1 \oplus B_2 \oplus B_3$, again we can apply Theorem 2.2 to

$$A_1 + A_2 = \{0\} \cup (B_1 \oplus B_2) \quad \text{and} \quad A_3 = \{0\} \cup B_3,$$

we obtain that,

$$\begin{aligned}|A_1 + A_2 + A_3| &\geqslant |A_1 + A_2| + |A_3| - 1 \geqslant |B_1| + |B_2| + 1 + |B_3| + 1 - 1\\ &\geqslant |B_1| + |B_2| + |B_3| + 1.\end{aligned}$$

By continuing the above process, we final arrive at

$$|A_1 + A_2 + \cdots + A_h| \geqslant |B_1| + |B_2| + \cdots + |B_h| + 1 = |G| + 1,$$

a contradiction. □

For the proofs of Theorems 1 and 2, we assume that $G = C_{p^\ell}$ where p is a prime number and $\ell > 1$ is an integer.

Proof of Theorem 1. Let k be an integer with $k \geqslant p^{\ell-1} - 1$. Let $S \in \mathscr{F}(G)$ of length $p^\ell + k$. To prove the theorem, it is enough to prove that if $\mathsf{h}(S) \leqslant k$, then, $0 \in \sum_{p^\ell}(S)$. Since $|S| = p^\ell + k$, we easily see that $0 \in \sum_{p^\ell}(S)$ is equivalent to $\sigma(S) \in \sum_k(S)$. Therefore, it is enough to prove $\sigma(S) \in \sum_k(S)$.

Let H be the stabilizer of $\sum_k(S)$. If $H = G$, then $\sum_k(S) = G$ and hence $\sigma(S) \in \sum_k(G)$. Now, suppose that $H \neq G$. We distinguish two cases.

Case 1: $(1 < |H| < p^\ell)$. Since $\sum_k(S)$ is a union of cosets of H, it suffices to show that there is some $y \in \sum_k(S)$ such that $\sigma(S) - y \in H$. Let $\Phi : G \to G/H$ denote the natural epimorphism. Since

$$|S| = p^\ell + k \geqslant (|H| - 1)|G/H| + (2|G/H| - 1) = (|H| - 1)|G/H| + \mathsf{s}(G/H),$$

S allows a product decomposition of the form $S = S_1 \cdot \cdots \cdot S_{|H|}S'$, where $S_1, \ldots, S_{|H|}, S' \in \mathscr{F}(G)$ and, for every $i \in [1, |H|]$, $\Phi(S_i)$ has sum zero and length $|S_i| = |G/H|$. Then $|S'| = k$, $\sigma(S') \in \sum_k(S)$ and $\sigma(S) - \sigma(S') = \sigma(S_1 \cdots S_{|H|}) \in H$.

Case 2: $(H = \{0\})$ Let N be the subgroup of G with $|N| = p$. Then, $\sum_k(S) + N \not\subset \sum_k(S)$. Therefore, there is a subsequence W of S such that $\sigma(W) + N \not\subset \sum_k(S)$ and $|W| = k$. Suppose $W = b_1 b_2 \cdots b_k$. Since $h \leqslant k$, one can distribute the elements of S into k disjoint subsets $B_1, B_2, \ldots, B_k$ with $b_i \in B_i$ for $i = 1, 2, \ldots, k$. Set $A_i = B_i \cup \{0\}$ for $i = 1, 2, \ldots, k$. Then,

$$\sigma(W) + N \in A_1 + \cdots + A_k + N \not\subset \sum_k(S) \quad \text{but} \quad A_1 + A_2 + \cdots + A_k \subset \sum_k(S).$$

Please cite this article as: W.D. Gao, et al., Addition theorems on the cyclic groups of order p^ℓ, Discrete Math. (2007), doi: 10.1016/j.disc.2007.04.040

Therefore, $A_1 + \cdots + A_k + N \not\subset A_1 + \cdots + A_k$. Since every subgroup of G contains N, $\{0\}$ is the maximal subgroup M such that $A_1 + \cdots + A_k + M = A_1 + \cdots + A_k$. Now apply Theorem 2.1 to $A_1 + \cdots + A_k$, we derive that

$$|A_1 + \cdots + A_k| \geqslant |A_1| + \cdots + |A_k| - (k-1) = p^\ell + 1 = |G| + 1.$$

This is impossible and hence the theorem. □

Proof Theorem 2. By the definition, it is clear that $\sum_{\leqslant h}(S) \subset \sum(S)$. It is enough to prove the other inclusion. Let H be the stabilizer of $\sum_{\leqslant h}(S)$. If $H = G$, then $G = \sum_{\leqslant h}(S) \subset \sum(S)$ which would imply $\sum(S) = G = \sum_{\leqslant h}(S)$ and we are done. Hence we can assume that $H \neq G$. Now, we consider two cases as follows.

Case 1: $(1 < |H| < p^\ell)$. Since $\sum_{\leqslant h}(S)$ is a union of cosets of H, it suffices to show that, for every element $x \in \sum(S)$, there exists an element $y \in \sum_{\leqslant h}(S)$ such that $x - y \in H$. By the definition of $\sum(S)$, it is clear that $x = \sigma(T)$ for some subsequence T of S.

Let $\Phi : G \to G/H$ be the natural epimorphism. Since $|G/H| \leqslant p^{\ell-1}$, we see that there is a subsequence T_0 of T such that $\sigma(\Phi(T)) = \sigma(\Phi(T_0)) + 0 = \sigma(\Phi(T_0))$ and $0 \leqslant |T_0| \leqslant p^{\ell-1} - 1$ (here we adopt the convention that the sum of the empty sequence is zero). Therefore, $x - \sigma(T_0) = \sigma(T) - \sigma(T_0) \in H$. But $\sigma(T_0) \in \sum_{\leqslant h}(S)$ (note that when T_0 is the empty sequence, we apply Theorem 2.3). This proves that $\sum(S) \subset \sum_{\leqslant h}(S)$. Therefore, we get $\sum(S) = \sum_{\leqslant h}(S)$.

Case 2: $(H = \{0\})$. Let N be the subgroup of G with $|N| = p$. Then, $\sum_{\leqslant h}(S) + N \not\subset \sum_{\leqslant h}(S)$. Therefore, there is a subsequence W of S such that $\sigma(W) + N \not\subset \sum_{\leqslant h}(S)$ and $1 \leqslant |W| \leqslant h$. Suppose $W = b_1 b_2 \cdots b_t$ with $1 \leqslant t \leqslant h$. Clearly, one can distribute the elements S into h disjoint subsets $B_1, B_2, \ldots, B_h$ with $b_i \in B_i$ for $i = 1, 2, \ldots, t$. Set $A_i = B_i \cup \{0\}$ for $i = 1, 2, \ldots, h$. Then,

$$\sigma(W) + N \in A_1 + \cdots + A_h + N \not\subset \sum_{\leqslant h}(S), \quad \text{but} \quad A_1 + \cdots + A_h \subset \sum_{\leqslant h}(S).$$

Therefore, $A_1 + \cdots + A_h + N \not\subset A_1 + \cdots + A_h$. Since every subgroup of G contains N, $\{0\}$ is the maximal subgroup M such that $A_1 + \cdots + A_h + M = A_1 + \cdots + A_h$. Now apply Theorem 2.1 to $A_1 + \cdots + A_h$, we derive that

$$|A_1 + \cdots + A_h| \geqslant |A_1| + \cdots + |A_h| - (h-1) = p^\ell + 1 = |G| + 1$$

and hence we get $G = B_1 + \cdots + B_h \subset \sum_{\leqslant h}(S)$. This is impossible and hence the theorem. □

Acknowledgements

This paper is completed while the first author is visiting the Department of Mathematics, Massachusetts Institute of Technology supported partly by MOE of China and he would like to thank all their assistance. This work has been supported partially by NSFC with Grant no. 10271080.

References

[1] A. Bialostocki, P. Dierker, On Erdős–Ginzburg–Ziv theorem and the Ramsey numbers for stars and matchings, Discrete Math. 110 (1992) 1–8.
[2] Y. Caro, Zero-sum problems—a survey, Discrete Math. 152 (1996) 93–113.
[3] P. Erdös, A. Ginzburg, A. Ziv, Theorem in the additive number theory, Bull. Res. Counc. Isr. 10F (1961) 41–43.
[4] C. Flores, O. Ordaz, On the Erdős–Ginzburg–Ziv theorem, Discrete Math. 152 (1996) 321–324.
[5] W.D. Gao, Some problems in additive group theory and number theory, Ph.D. Thesis, Sichuan University, Sichuan, PR China, 1994.
[7] W.D. Gao, An addition theorem for finite cyclic groups, Discrete Math. 163 (1996) 257–265.
[8] W.D. Gao, A. Geroldinger, Zero-sum problems in finite abelian groups: a survey, Exposition Math. 24 (4) (2006) 337–369.
[9] W.D. Gao, A. Panigrahi, R. Thangadurai, On the structure of p-zero-sum free sequences and its application to a variant of Erdős–Ginzburg–Ziv theorem, Proc. Indian Acad. Sci. Math. Sci. 115 (1) (2005) 67–77.
[10] W.D. Gao, R. Thangadurai, On a variant of Kemnitz conjecture, J. Combin. Theory Ser. A. 107 (2004) 69–86.
[11] A. Geroldinger, F. Halter-Koch, Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory, Pure and Applied Mathematics, vol. 278, Chapman & Hall, CRC, London, Boca Raton, FL, 2006.
[13] M.B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Springer, Berlin, 1996.
[14] B. Peterson, T. Yuster, A generalization of an addition theorem for solvable groups, Canad. J. Math. XXXVI (3) (1984) 529–536.

Please cite this article as: W.D. Gao, et al., Addition theorems on the cyclic groups of order p^ℓ, Discrete Math. (2007), doi: 10.1016/j.disc.2007.04.040