

ON THE NUMBER OF SUBSEQUENCES  
WITH GIVEN SUM OF SEQUENCES  
OVER FINITE ABELIAN  $p$ -GROUPS

WEIDONG GAO AND ALFRED GEROLDINGER

ABSTRACT. Let  $G$  be an additive finite abelian  $p$ -group. For a given (long) sequence  $S$  over  $G$  and some element  $g \in G$ , we investigate the number of subsequences of  $S$  which have sum  $g$ . This refines some classical results of J.E. Olson and recent results of I. Koutis.

**1. Introduction and main result.** Let  $G$  be an additively written finite abelian group. The enumeration of subsequences of a given (long) sequence over  $G$ , which have some prescribed properties, is a classical topic in combinatorial number theory going back to P. Erdős, J.E. Olson, et al. In the meantime there is a huge variety of results achieved by many authors, see [1–6, 8–11, 14–16] and the literature cited therein, for an overview of the various types of results.

In this note we concentrate on finite abelian  $p$ -groups. In order to state our main result, we need some notations, for details see Section 2. Suppose that  $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ , where  $1 < n_1 \mid \cdots \mid n_r$  and set  $d^*(G) = \sum_{i=1}^r (n_i - 1)$ . For a sequence  $S$  over  $G$ , an element  $g \in G$  and some  $k \in \mathbf{N}_0$ , let  $N_g(S)$  ( $N_g^+(S)$ ,  $N_g^-(S)$ , respectively  $N_g^k(S)$ ) denote the number of subsequences  $T$  of  $S$  having sum  $g$  (and even length, odd length respectively, length  $k$ ).

**Theorem 1.1.** *Let  $G$  be a finite abelian  $p$ -group,  $g \in G$ ,  $k \in \mathbf{N}_0$  and  $S \in \mathcal{F}(G)$  a sequence of length  $|S| > k \exp(G) + d^*(G)$ .*

1.  $N_g^+(S) \equiv N_g^-(S) \pmod{p^{k+1}}$ .
2. If  $p = 2$ , then  $N_g(S) \equiv 0 \pmod{2^{k+1}}$ .
3. If  $j \in [0, \exp(G) - 1]$  and  $m^* = k - 1 + \lceil (1 + d^*(G))/\exp(G) \rceil$ , then the numbers  $N_g^{m \exp(G) + j}(S)$  for all  $m > m^*$  are modulo  $\pmod{p^k}$  uniquely determined by  $N_g^j(S)$ ,  $N_g^{\exp(G) + j}(S)$ ,  $\dots$ ,  $N_g^{m^* \exp(G) + j}(S)$ .

---

Received by the editors on January 20, 2005, and in revised form on May 12, 2005.

For  $k = 0$ , the first statement was proved by Olson [13, Theorem 1]. For elementary  $p$ -groups, slightly weaker results were recently obtained by Koutis, see [12, Theorems 7, 8, 9, 10], who used representation theory. We work with group algebras which have turned out to be a powerful tool in this area. However, up to now, mainly group algebras over finite fields or over the field of complex numbers were used. We work over the group algebra  $\mathbf{Z}[G]$ , and this is the reason why in the above theorem we obtain congruences not only modulo  $p$  but also modulo higher powers of  $p$ . As a further consequence of our main proposition on group algebras, we get the following result on representation numbers of sumsets.

For subsets  $A_1, \dots, A_l \subset G$  and some element  $g \in G$ , let

$$r_{A_1, \dots, A_l}(g) = \left| \left\{ (a_1, \dots, a_l) \in A_1 \times \dots \times A_l \mid g = a_1 + \dots + a_l \right\} \right|$$

denote the number of representations of  $g$  as a sum of elements of  $A_1, \dots, A_l$ . These numbers play a crucial role in the investigation of sumsets, e.g., a theorem of Kneser-Kemperman states that for  $A, B \subset G$  and  $g \in A + B$  we have  $|A + B| \geq |A| + |B| - r_{A,B}(g)$ .

**Theorem 1.2.** *Let  $G$  be a finite abelian  $p$ -group,  $g \in G$ ,  $k, l \in \mathbf{N}$  and  $A_1, \dots, A_l$  subsets of  $G$  such that  $|A_1| \equiv \dots \equiv |A_l| \equiv 0 \pmod{p}$ . If  $l > k \exp(G) + d^*(G)$ , then  $r_{A_1, \dots, A_l}(g) \equiv 0 \pmod{p^{k+1}}$ .*

**2. Preliminaries.** Let  $\mathbf{N}$  denote the set of integers, and let  $\mathbf{N}_0 = \mathbf{N} \cup \{0\}$ . For  $a, b \in \mathbf{Z}$ , we set  $[a, b] = \{x \in \mathbf{Z} \mid a \leq x \leq b\}$ . All abelian groups will be written additively, and for  $n \in \mathbf{N}$ , let  $C_n$  denote a cyclic group with  $n$  elements. If  $A$  and  $B$  are sets, then  $A \subset B$  means that  $A$  is contained in  $B$  but may be equal to  $B$ .

Let  $G$  be a finite abelian group. By the fundamental theorem on finite abelian groups, there exist uniquely determined integers  $n_1, \dots, n_r \in \mathbf{N}$  such that  $G \cong C_{n_1} \oplus \dots \oplus C_{n_r}$ , where either  $r = n_1 = 1$  or  $1 < n_1 \mid \dots \mid n_r$ . Then  $n_r = \exp(G)$  is the *exponent* of  $G$ , and we set  $d^*(G) = \sum_{i=1}^r (n_i - 1)$ .  $G$  is a  $p$ -group if  $\exp(G)$  is a power of  $p$ , and it is an *elementary  $p$ -group* if  $\exp(G) = p$  for some prime  $p \in \mathbf{N}$ . An  $s$ -tuple  $(e_1, \dots, e_s)$  of elements of  $G \setminus \{0\}$  is called a *basis* of  $G$ , if  $G = \langle e_1 \rangle \oplus \dots \oplus \langle e_s \rangle$ . For every  $g \in G$ ,  $\text{ord}(g) \in \mathbf{N}$  denotes the *order* of  $g$ .

Let  $\mathcal{F}(G)$  denote the free abelian monoid with basis  $G$ , and let  $S \in \mathcal{F}(G)$ . Then  $S$  is called a *sequence over  $G$* , and it will be written in the form

$$S = \prod_{i=1}^l g_i = g_1 \cdot \dots \cdot g_l = \prod_{g \in G} g^{v_g(S)} \quad \text{where all } v_g(S) \in \mathbf{N}_0.$$

A sequence  $T \in \mathcal{F}(G)$  is called a *subsequence* of  $S$ , if  $v_g(T) \leq v_g(S)$  for every  $g \in G$ . The unit element  $1 \in \mathcal{F}(G)$  is called the *empty sequence*. We denote by

- $|S| = l = \sum_{g \in G} v_g(S) \in \mathbf{N}_0$  the *length* of  $S$ ,
- $\sigma(S) = \sum_{i=1}^l g_i = \sum_{g \in G} v_g(S)g \in G$  the *sum* of  $S$ , and by
- $\Sigma(S) = \{ \sum_{i \in I} g_i \mid \emptyset \neq I \subset [1, l] \} \subset G$  the *set of subsums* of  $S$ .

For  $g \in G$  and  $k \in \mathbf{N}_0$ ,

$$N_g^k(S) = \left| \left\{ I \subset [1, l] \mid \sum_{i \in I} g_i = g \text{ and } |I| = k \right\} \right|$$

denotes the number of subsequences  $T$  of  $S$  having sum  $\sigma(T) = g$  and length  $|T| = k$  (counted with the multiplicity of their appearance in  $S$ ). Then

$$N_g(S) = \sum_{k \geq 0} N_g^k(S), \quad \text{and} \quad N_g^+(S) = \sum_{k \geq 0} N_g^{2k}(S)$$

respectively  $N_g^-(S) = \sum_{k \geq 0} N_g^{2k+1}(S)$

denote the number of subsequences  $T$  of  $S$  having sum  $\sigma(T) = g$  and even, respectively odd, length. Since, in our convention, the empty sequence is a zero-sum sequence of length zero, we always have  $N_0(S) \geq N_0^+(S) \geq 1$ .

Let  $R$  be a commutative ring (by a ring, we always mean a ring with unit element). The *group algebra*  $R[G]$  of the group  $G$  over the ring  $R$  is a free  $R$ -module with basis  $\{X^g \mid g \in G\}$  (built with a symbol  $X$ ), where multiplication is defined by

$$\left( \sum_{g \in G} a_g X^g \right) \left( \sum_{g \in G} b_g X^g \right) = \sum_{g \in G} \left( \sum_{h \in G} a_h b_{g-h} \right) X^g.$$

We view  $R$  as a subset of  $R[G]$  by means of  $a = aX^0$  for all  $a \in R$ . The *augmentation map*

$$\varepsilon: R[G] \rightarrow R, \quad \text{defined by} \quad \varepsilon\left(\sum_{g \in G} a_g X^g\right) = \sum_{g \in G} a_g$$

is an epimorphism of  $R$ -algebras. Its kernel  $\text{Ker}(\varepsilon) = I_G$  is called the *augmentation ideal*, and  $\{1 - X^g \mid 0 \neq g \in G\}$  is an  $R$ -basis of  $I_G$ .

### 3. Proof of the main results.

**Lemma 3.1.** *Let  $G$  be a finite abelian  $p$ -group,  $R$  a commutative ring and  $k \in \mathbf{N}_0$ .*

1. *If  $g \in G$ , then*

$$(1 - X^g)^{k \text{ord}(g)} \in p^k R[G].$$

2. *If  $(e_1, \dots, e_r)$  is a basis of  $G$  and  $m_1, \dots, m_r \in \mathbf{N}_0$  with  $m_1 + \dots + m_r > k \exp(G) + d^*(G)$ , then*

$$\prod_{i=1}^r (1 - X^{e_i})^{m_i} \in p^{k+1} R[G].$$

*Proof.* 1. Let  $g \in G$ ,  $m \in \mathbf{N}_0$  and  $\text{ord}(g) = p^m$ . If  $m = 0$ , then  $g = 0$ ,  $X^0 = 1$  and  $1 - X^g = 0 \in p^k R[G]$ . Suppose that  $m \in \mathbf{N}$ . Since the binomial coefficient  $\binom{p^m}{i}$  is divisible by  $p$  for every  $i \in [1, p^m - 1]$ , we obtain that

$$\begin{aligned} (1 - X^g)^{p^m} &= \sum_{i=0}^{p^m} \binom{p^m}{i} (-1)^i X^{ig} \\ &= 1 + (-1)^{p^m} X^0 + \sum_{i=1}^{p^m-1} \binom{p^m}{i} (-1)^i X^{ig} \in pR[G] \end{aligned}$$

whence

$$(1 - X^g)^{kp^m} \in p^k R[G].$$

2. Let  $(e_1, \dots, e_r)$  be a basis of  $G$  with  $\text{ord}(e_i) = n_i$  for every  $i \in [1, r]$  and suppose that  $n_1 \leq \dots \leq n_r$ . Furthermore, let  $m_1, \dots, m_r \in \mathbf{N}_0$  be such that  $m_1 + \dots + m_r > k \exp(G) + d^*(G)$ . For every  $i \in [1, r]$ , we set  $m_i = k_i n_i + t_i$  with  $t_i \in [0, n_i - 1]$ . Then we infer that

$$\sum_{i=1}^r (k_i n_i + t_i) > k \exp(G) + d^*(G) = k n_r + \sum_{i=1}^r (n_i - 1),$$

whence

$$\sum_{i=1}^r k_i n_r \geq \sum_{i=1}^r k_i n_i \geq k n_r + 1 \quad \text{and} \quad \sum_{i=1}^r k_i \geq k + 1.$$

By step 1, we have  $(1 - X^{e_i})^{m_i} = (1 - X^{e_i})^{k_i n_i + t_i} \in p^{k_i} R[G]$ , and thus

$$\prod_{i=1}^r (1 - X^{e_i})^{m_i} \in p^{k_1 + \dots + k_r} R[G] \subset p^{k+1} R[G]. \quad \square$$

We continue with two propositions which may be of independent interest.

**Proposition 3.2.** *Let  $G$  be a finite abelian  $p$ -group,  $R$  a commutative ring,  $I_G \subset R[G]$  the augmentation ideal and  $k, l \in \mathbf{N}_0$  such that  $l > k \exp(G) + d^*(G)$ . Then*

$$\left( I_G + pR[G] \right)^l \subset p^{k+1} R[G].$$

*In particular, if  $g_1, \dots, g_l \in G$ , then*

$$\prod_{i=1}^l (1 - X^{g_i}) \in p^{k+1} R[G].$$

*Proof.* We proceed in two steps. First we settle the indicated special case.

1. For every  $i \in [1, l]$ , let  $g_i \in G$  and  $f_i = 1 - X^{g_i}$ . We assert that  $f_1 \cdots f_l \in p^{k+1}R[G]$ .

Let  $(e_1, \dots, e_r)$  be a basis of  $G$  with  $\text{ord}(e_i) = n_i$  for every  $i \in [1, r]$ . For every  $i \in [1, l]$ , we set  $g_i = \sum_{\nu=1}^r l_{i,\nu} e_\nu$  where  $l_{i,\nu} \in [0, n_\nu - 1]$  for every  $\nu \in [1, r]$ . Then, for every  $i \in [1, l]$ , we have

$$1 - X^{g_i} = 1 - X^{\sum_{\nu=1}^r l_{i,\nu} e_\nu} = 1 - \prod_{\nu=1}^r (1 - (1 - X^{e_\nu}))^{l_{i,\nu}} = \sum_{\nu=1}^r (1 - X^{e_\nu}) f_{i,\nu}$$

with  $f_{i,1}, \dots, f_{i,r} \in R[G]$ . Therefore, we obtain that

$$\begin{aligned} \prod_{i=1}^l (1 - X^{g_i}) &= \prod_{i=1}^l \sum_{\nu=1}^r (1 - X^{e_\nu}) f_{i,\nu} \\ &= \sum_{\substack{\mathbf{m} \in [0, l]^r \\ m_1 + \dots + m_r = l}} f_{\mathbf{m}} (1 - X^{e_1})^{m_1} \cdots (1 - X^{e_r})^{m_r} \end{aligned}$$

where all  $f_{\mathbf{m}} \in R[G]$  and  $\mathbf{m} = (m_1, \dots, m_r)$ . Since  $m_1 + \dots + m_r = l > k \exp(G) + d^*(G)$ , the assertion follows from Lemma 3.1.2.

2. Let  $s \in [0, k]$  and recall that  $\{1 - X^g \mid g \in G \setminus \{0\}\}$  is an  $R$ -basis of  $I_G$ . Then  $l - s > (k - s) \exp(G) + d^*(G)$ , whence step 1 implies that

$$(I_G)^{l-s} \subset p^{k+1-s}R[G].$$

Therefore, we obtain that

$$(I_G + pR[G])^l \subset \sum_{s=0}^l (I_G)^{l-s} (pR[G])^s \subset p^{k+1}R[G]. \quad \square$$

**Proposition 3.3.** *Let  $G$  be an elementary 2-group and  $S \in \mathcal{F}(G)$ . Then*

$$N_0(S) = N_g(S) \quad \text{for every } g \in \Sigma(S).$$

*Proof.* Let  $S = g_1 \cdots g_l \in \mathcal{F}(G)$ ,  $g \in \Sigma(S) \setminus \{0\}$ ,

$$\{I_1, \dots, I_t\} = \left\{ I \subset [1, l] \mid \sum_{i \in I} g_i = 0 \right\}$$

and

$$\{J_1, \dots, J_s\} = \left\{ J \subset [1, l] \mid \sum_{j \in J} g_j = g \right\}.$$

Let  $I, J, J' \subset [1, l]$  be subsets, and let  $I \Delta J = (I \setminus J) \cup (J \setminus I)$  denote the symmetric difference. Since  $(\mathcal{P}([1, l]), \Delta)$ , that is, the family of subsets of  $[1, l]$  with the symmetric difference as the law of composition, is an elementary 2-group,  $I \Delta J = I \Delta J'$  implies that  $J = J'$ . Since  $G$  is an elementary 2-group, we infer that

$$\sum_{i \in J_1 \Delta I_\nu} g_i = g \quad \text{for all } \nu \in [1, t]$$

and

$$\sum_{j \in J_1 \Delta J_\mu} g_j = 0 \quad \text{for all } \mu \in [1, s].$$

This implies that

$$\begin{aligned} N_0(S) &= t = |\{J_1 \Delta I_\nu \mid \nu \in [1, t]\}| \leq N_g(S) \\ &= s = |\{J_1 \Delta J_\mu \mid \mu \in [1, s]\}| \leq N_0(S). \quad \square \end{aligned}$$

*Proof of Theorem 1.1.* Suppose that  $S = g_1 \cdot \dots \cdot g_l \in \mathcal{F}(G)$ .

1. By Proposition 3.2, with  $R = \mathbf{Z}$ , we obtain that

$$\prod_{i=1}^l (1 - X^{g_i}) = \sum_{g \in G} \left( N_g^+(S) - N_g^-(S) \right) X^g \in p^{k+1} \mathbf{Z}[G],$$

whence the assertion follows.

2. If  $p = 2$ , then again by Proposition 3.2 we get

$$\begin{aligned} \sum_{g \in G} N_g(S) X^g &= \prod_{i=1}^l (1 + X^{g_i}) \\ &= \prod_{i=1}^l (-(1 - X^{g_i}) + 2) \in (I_G + 2R[G])^l \in 2^{k+1} \mathbf{Z}[G]. \end{aligned}$$

3. Let  $C$  be a cyclic group of order  $\exp(G)$ , and suppose that  $C = \langle e \rangle \subset G \oplus C$  such that every  $h \in G \oplus C$  has a unique representation  $h = g + je$  where  $g \in G$  and  $j \in [0, \exp(G) - 1]$ . By [7, Theorem 7.1], the polynomial ring in the indeterminate  $T$  over the group ring  $\mathbf{Z}[G \oplus C]$  is (isomorphic to) the group ring of  $G \oplus C$  over the polynomial ring  $\mathbf{Z}[T]$ , so

$$\mathbf{Z}[G \oplus C][T] = \mathbf{Z}[T][G \oplus C].$$

We consider the element

$$(*) \quad \prod_{i=1}^l (1 + X^{g_i}T - X^eT) = \sum_{h \in G \oplus C} p_h X^h \in \mathbf{Z}[T][G \oplus C]$$

where all  $p_h \in \mathbf{Z}[T]$ , and start with the following assertion:

**Assertion.** *For every  $h \in G \oplus C$  and every  $m > k \exp(G) + d^*(G)$ , the coefficient of  $T^m$  in  $p_h$  is divisible by  $p^k$ .*

*Proof of the Assertion.* We have

$$\prod_{i=1}^l (1 + X^{g_i}T - X^eT) = \prod_{i=1}^l (1 + (X^{g_i} - 1)T - (X^e - 1)T) = \sum_{m=0}^l b_m T^m$$

where every  $b_m \in \mathbf{Z}[G \oplus C]$  is a sum of elements of the form

$$c(X^{g_{i_1}} - 1) \cdot \dots \cdot (X^{g_{i_u}} - 1)(X^e - 1)^{m-u} \quad \text{with } c \in \mathbf{Z}.$$

If  $m > k \exp(G) + d^*(G) = 1 + (k - 1) \exp(G \oplus C) + d^*(G \oplus C)$ , then Proposition 3.2 implies that elements of this form lie in  $p^k \mathbf{Z}[G \oplus C]$ . Therefore, for every  $m > k \exp(G) + d^*(G)$ , we have  $b_m \in p^k \mathbf{Z}[G \oplus C]$ , whence the assertion follows.

Let now  $g \in G$ ,  $j \in [0, \exp(G) - 1]$ ,  $w = \lceil (1 + d^*(G))/\exp(G) \rceil$  and  $m \geq k + w$ . Then

$$m \exp(G) + j \geq (k + w) \exp(G) \geq k \exp(G) + d^*(G) + 1,$$

whence the coefficient of  $T^{m \exp(G) + j}$  in  $p_g$  is divisible by  $p^k$ . On the other hand, (\*) shows that this coefficient is equal to

$$\sum_{i=0}^m N_g^{(m-i) \exp(G) + j} (S)(-1)^{i \exp(G)} \binom{l - ((m-i) \exp(G) + j)}{i \exp(G)}$$



Therefore, we finally obtain that

$$\sum_{i=0}^m N_g^{(m-i)\exp(G)+j}(S) (-1)^{i\exp(G)} \binom{l - ((m-i)\exp(G) + j)}{i\exp(G)} \equiv 0 \pmod{p^k}.$$

Since the coefficient of  $N_g^{m\exp(G)+j}(S)$  in this congruence equals 1, the assertion follows by induction on  $m$  (starting with  $m = m^* + 1 = k + w$ ).  $\square$

*Proof of Theorem 1.2.* Let  $k, l \in \mathbf{N}$  with  $l > k \exp(G) + d^*(G)$  and  $A_1, \dots, A_l$  subsets of  $G$  such that  $|A_1| \equiv \dots \equiv |A_l| \equiv 0 \pmod{p}$ . For every  $i \in [1, l]$ , we set  $f_i = \sum_{g \in A_i} X^g \in \mathbf{Z}[G]$ , whence  $\varepsilon(f_i) \in pR$ . Thus, Proposition 3.2 implies that

$$f = f_1 \cdot \dots \cdot f_l \in p^{k+1}\mathbf{Z}[G].$$

If we set  $f = \sum_{g \in G} c_g X^g$ , then clearly  $c_g$  equals the representation number  $r_{A_1, \dots, A_l}(g)$ , whence the assertion follows.  $\square$

**Acknowledgments.** We would like to thank the referee for a careful reading and for suggesting several improvements of the manuscript.

REFERENCES

1. A. Bialostocki, P. Dierker, D. Grynkiewicz and M. Lotspeich, *On some developments of the Erdős-Ginzburg-Ziv Theorem II*, Acta Arith. **110** (2003), 173–184.
2. A. Bialostocki and M. Lotspeich, *Some developments of the Erdős-Ginzburg-Ziv theorem*, Sets, graphs and numbers **60**, Colloquium Math. Soc. J. Bolyai (1992), 97–117.
3. B. Bollobás and I. Leader, *The number of  $k$ -sums modulo  $k$* , J. Number Theory **78** (1999), 27–35.
4. Z. Füredi and D.J. Kleitman, *The minimal number of zero sums*, Combinatorics, J. Bolyai Math. Soc. (1993), 159–172.
5. W. Gao, *On the number of zero sum subsequences*, Discrete Math. **163** (1997), 267–273.
6. ———, *On the number of subsequences with given sum*, Discrete Math. **195** (1999), 127–138.

7. R. Gilmer, *Commutative semigroup rings*, The University of Chicago Press, Chicago, 1984.
8. D.J. Grynkiewicz, *On a conjecture of Hamidoune for subsequence sums*, *Integers* **5** (2005), paper A07.
9. F. Halter-Koch, *A generalization of Davenport's constant and its arithmetical applications*, *Colloq. Math.* **63** (1992), 203–210.
10. Y.ould Hamidoune, *Subsequence sums*, *Comb. Probab. Comput.* **12** (2003), 413–425.
11. M. Kisin, *The number of zero sums modulo  $m$  in a sequence of length  $n$* , *Mathematika* **41** (1994), 149–163.
12. I. Koutis, *Dimensionality restrictions on sums over  $\mathbf{Z}_p^d$* , Technical Report CMU-CS-07-103, Carnegie Mellon University, Computer Science Department.
13. J.E. Olson, *A combinatorial problem on finite abelian groups I*, *J. Number Theory* **1** (1969), 8–10.
14. V. Ponomarenko, *Minimal zero sequences of finite cyclic groups*, *Integers* **4** (2004), paper A24.
15. C. Reiher, *On Kemnitz' conjecture concerning lattice points in the plane*, *Ramanujan J.* **13** (2007), 333–337.
16. W.A. Schmid, *On zero-sum subsequences in finite abelian groups*, *Integers* **1** (2001), Paper A01.

CENTER FOR COMBINATORICS, NANKAI UNIVERSITY, TIANJIN 300071, P.R. CHINA

**Email address:** [wdgao\\_1963@yahoo.com.cn](mailto:wdgao_1963@yahoo.com.cn)

INSTITUT FÜR MATHEMATIK, KARL-FRANZENSUNIVERSITÄT, HEINRICHSTRASSE 36, 8010 GRAZ, AUSTRIA

**Email address:** [alfred.geroldinger@uni-graz.at](mailto:alfred.geroldinger@uni-graz.at)