ON THE NUMBER OF SUBSEQUENCES WITH GIVEN SUM OF SEQUENCES IN 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 in 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 in 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 [2, 4, 10, 5, 6, 3, 15, 1, 9, 13, 14, 8] and the literature cited there, 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 $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$, where $1 < n_1 \mid \ldots \mid n_r$ and set $\mathsf d^*(G) = \sum_{i=1}^r (n_i - 1)$. For a sequence S in G, an element $g \in G$ and some $k \in \mathbb N_0$, let $\mathsf N_g(S)$ ($\mathsf N_g^+(S)$, $\mathsf N_g^-(S)$ resp. $\mathsf N_g^k(S)$) denote the number of subsequences T of S having sum g (and even length, odd length resp. length k).

Theorem 1.1. *Let G be a finite abelian p-group, $g \in G$, $k \in \mathbb N_0$ and $S \in \mathcal F(G)$ a sequence of length $|S| > k \exp(G) + \mathsf d^*(G)$.*

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

For $k = 0$, the first statement was proved by J.E. Olson [12, Theorem 1]. For elementary p-groups, slightly weaker results were recently obtained by I. Koutis (see [11, Theorems 7, 8, 9 and 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 $\mathbb Z[G]$, 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 $A_1, \ldots, A_l \subset G$ and some element $g \in G$, let

$$\mathsf r_{A_1,\ldots,A_l}(g) = \Big| \Big\{ (a_1, \ldots, a_l) \in A_1 \times \ldots \times A_l \mid g = a_1 + \ldots + a_l \Big\} \Big|$$

denote the number of representations of g as a sum of elements of $A_1, \ldots, A_l$. 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 $|A + B| \ge |A| + |B| - \mathsf r_{A,B}(g)$.

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

2. Preliminaries

Let $\mathbb{N}$ denote the set of integers and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $a, b \in \mathbb{Z}$ we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$. All abelian groups will be written additively, and for $n \in \mathbb{N}$ 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 $n_1, \ldots, n_r \in \mathbb{N}$ such that $G \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$ where either $r = n_1 = 1$ or $1 < n_1 \mid \ldots \mid n_r$. Then $n_r = \exp(G)$ is the *exponent* of G, and we set $\mathsf{d}^*(G) = \sum_{i=1}^r (n_i - 1)$. 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 $p \in \mathbb{N}$. An s-tuple $(e_1, \ldots, e_s)$ of elements of G is called a *basis* of G, if $G = \langle e_1 \rangle \oplus \ldots \oplus \langle e_s \rangle$. For every $g \in G$, $\operatorname{ord}(g) \in \mathbb{N}$ 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 in G*, and it will be written in the form

$$S = \prod_{i=1}^{l} g_i = g_1 \cdot \ldots \cdot g_l = \prod_{g \in G} g^{\mathsf{v}_g(S)} \qquad \text{where all} \quad \mathsf{v}_g(S) \in \mathbb{N}_0 \,.$$

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

- $|S| = l = \sum_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0$ the *length* of S,
- $\sigma(S) = \sum_{i=1}^l g_i = \sum_{g \in G} \mathsf{v}_g(S) g \in G$ the *sum* of S, and by
- $\Sigma(S) = \{\sum_{i \in I} g_i \mid \emptyset \ne I \subset [1, l]\} \subset G$ the set of sums of non-empty subsequences of S.

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

$$\mathsf{N}_g^k(S) = \Big| \Big\{ I \subset [1, l] \;\Big|\; \sum_{i \in I} g_i = g \text{ and } |I| = k \Big\} \Big|$$

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

$$\mathsf{N}_g(S) = \sum_{k \ge 0} \mathsf{N}_g^k(S), \quad \text{and} \quad \mathsf{N}_g^+(S) = \sum_{k \ge 0} \mathsf{N}_g^{2k}(S) \quad \text{resp.} \quad \mathsf{N}_g^-(S) = \sum_{k \ge 0} \mathsf{N}_g^{2k+1}(S)$$

denote the number of subsequences T of S having sum $\sigma(T) = g$ and even (resp. odd) length.

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

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

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

$$\varepsilon \colon R[G] \to R, \quad \text{defined by} \quad \varepsilon \Big(\sum_{g \in G} a_g X^g \Big) = \sum_{g \in G} a_g$$

is an epimorphism of R-algebras. Its kernel $\operatorname{Ker}(\varepsilon) = I_G$ is called the *augmentation ideal*, and $\{1 - X^g \mid 0 \ne g \in G\}$ 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 $k \in \mathbb{N}_0$.*

1. *If $g \in G$, then*
$$(1 - X^g)^{k\operatorname{ord}(g)} \in p^k R[G]\,.$$
2. *If $(e_1, \ldots, e_r)$ is a basis of G and $m_1, \ldots, m_r \in \mathbb{N}_0$ with $m_1 + \ldots + m_r > k\exp(G) + \mathsf{d}^*(G)$, then*
$$\prod_{i=1}^{r} (1 - X^{e_i})^{m_i} \in p^{k+1} R[G]\,.$$

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

2. Let $(e_1, \ldots, e_r)$ be a basis of G with $\operatorname{ord}(e_i) = n_i$ for every $i \in [1, r]$ and suppose that $n_1 \le \ldots \le n_r$. Furthermore, let $m_1, \ldots, m_r \in \mathbb{N}_0$ such that $m_1 + \ldots + m_r > k\exp(G) + \mathsf{d}^*(G)$. 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
$$\sum_{i=1}^{r} (k_i n_i + t_i) > k\exp(G) + \mathsf{d}^*(G) = kn_r + \sum_{i=1}^{r} (n_i - 1)$$
whence
$$\sum_{i=1}^{r} k_i n_r \ge \sum_{i=1}^{r} k_i n_i \ge kn_r + 1 \quad \text{and} \quad \sum_{i=1}^{r} k_i \ge k + 1\,.$$
By 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
$$\prod_{i=1}^{r} (1 - X^{e_i})^{m_i} \in p^{k_1 + \ldots + k_r} R[G] \subset p^{k+1} R[G]\,.$$
$\square$

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 $k, l \in \mathbb{N}_0$ such that $l > k\exp(G) + \mathsf{d}^*(G)$. Then*
$$\Big(I_G + pR[G]\Big)^l \subset p^{k+1} R[G]\,.$$
In particular, if $g_1, \ldots, g_l \in G$, 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 $f_1 \cdot \ldots \cdot f_l \in p^{k+1}R[G]$.

Let $(e_1, \ldots, e_r)$ be a basis of G with $\mathrm{ord}(e_i) = n_i$ 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

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

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

$$\prod_{i=1}^l (1 - X^{g_i}) = \prod_{i=1}^l \sum_{\nu=1}^r (1 - X^{e_\nu}) f_{i,\nu} = \sum_{\substack{\boldsymbol{m} \in [0,l]^r \\ m_1 + \ldots + m_r = l}} f_{\boldsymbol{m}} (1 - X^{e_1})^{m_1} \cdot \ldots \cdot (1 - X^{e_r})^{m_r}$$

where all $f_{\boldsymbol{m}} \in R[G]$ and $\boldsymbol{m} = (m_1, \ldots, m_r)$. Since $m_1 + \ldots + m_r = l > k \exp(G) + \mathsf{d}^*(G)$, 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 $l - s > (k-s)\exp(G) + \mathsf{d}^*(G)$ whence 1. implies that

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

Therefore we obtain that

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

□

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

$$\mathsf{N}_0(S) = \mathsf{N}_g(S) \qquad \textit{for every} \quad g \in \Sigma(S) \,.$$

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

$$\{I_1, \ldots, I_t\} = \Big\{ I \subset [1,l] \mid \sum_{i \in I} g_i = 0 \Big\} \quad \text{and} \quad \{J_1, \ldots, J_s\} = \Big\{ J \subset [1,l] \mid \sum_{j \in J} g_j = g \Big\} \,.$$

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

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

and

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

This implies that

$$\mathsf{N}_0(S) = t = |\{J_1 \triangle I_\nu \mid \nu \in [1,t]\}| \le \mathsf{N}_g(S) = s = |\{J_1 \triangle J_\mu \mid \mu \in [1,s]\}| \le \mathsf{N}_0(S) \,.$$

□

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

1. By Proposition 3.2 (with $R = \mathbb{Z}$) we obtain that

$$\prod_{i=1}^{l}(1 - X^{g_i}) = \sum_{g \in G}\Big(\mathsf{N}_g^+(S) - \mathsf{N}_g^-(S)\Big)X^g \in p^{k+1}\mathbb{Z}[G]$$

whence the assertion follows.

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

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

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 $\mathbb{Z}[G \oplus C]$ is (isomorphic to) the group ring of $G \oplus C$ over the polynomial ring $\mathbb{Z}[T]$, so

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

We consider the element

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

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

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

Proof of the Assertion: We have

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

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

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

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

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

$$m\exp(G) + j \ge (k + w)\exp(G) \ge k\exp(G) + \mathsf{d}^*(G) + 1$$

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

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

Therefore we finally obtain that

$$\sum_{i=0}^{m}\mathsf{N}_g^{(m-i)\exp(G)+j}(S)(-1)^{i\exp(G)}\binom{l - \big((m-i)\exp(G) + j\big)}{i\exp(G)} \;\equiv\; 0 \mod p^k\,.$$

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

□

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

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

If we set $f = \sum_{g \in G} c_g X^g$, then clearly c_g equals the representation number $\mathsf{r}_{A_1,\ldots,A_l}(g)$ whence the assertion follows. □

Acknowledgement. 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, vol. 60, Coll. Math. Soc. J. Bolyai, 1992, pp. 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, Paul Erdős is Eighty, J. Bolyai Math. Soc., 1993, pp. 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 Univ. of Chicago Press, 1984.
[8] D.J. Grynkiewicz, *On a conjecture of Hamidoune for subsequence sums*, Integers.
[9] Y. ould Hamidoune, *Subsequence sums*, Comb. Probab. Comput. **12** (2003), 413 – 425.
[10] M. Kisin, *The number of zero sums modulo m in a sequence of length n*, Mathematika **41** (1994), 149 – 163.
[11] I. Koutis, *Dimensionality restrictions on sums over $\mathbb{Z}_p^d$*, –.
[12] J.E. Olson, *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8 – 10.
[13] V. Ponomarenko, *Minimal zero sequences of finite cyclic groups*, Integers **4** (2004), Paper A24, 6p.
[14] C. Reiher, *On Kemnitz' conjecture concerning lattics points in the plane*, Ramanujan J., to appear.
[15] W.A. Schmid, *On zero-sum subsequences in finite abelian groups*, Integers **1** (2001), Paper A01, 8p.

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
E-mail address: wdgao_1963@yahoo.com.cn

Institut für Mathematik, Karl-FranzensUniversität, Heinrichstrasse 36, 8010 Graz, Austria
E-mail address: alfred.geroldinger@uni-graz.at