isibang/ms/2010/3
April 5th, 2010
http://www.isibang.ac.in/~statmath/eprints

Zero-sum problems with subgroup weights

S. D. Adhikari, A. A. Ambily and B. Sury

Indian Statistical Institute, Bangalore Centre
8th Mile Mysore Road, Bangalore, 560059 India

Zero-sum problems with subgroup weights

S. D. Adhikari[1], A. A. Ambily[2] & B. Sury[3] *

[1] Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211019, India (email : adhikari@mri.ernet.in)
[2] Statistics & Mathematics Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560059, India (email : ambily@isibang.ac.in)
[3] Statistics & Mathematics Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560059, India (email : sury@isibang.ac.in)

Abstract

In this note, we generalize some theorems on zero-sums with weights from [1], [4] and [5] in two directions. In particular, we consider $\mathbb{Z}_p^d$ for a general d and subgroups of $\mathbf{Z}_p^*$ as weights.

Mathematics Subject Classification 2001 : 11B13
Keywords : Cauchy-Davenport theorem, Chevalley-Warning theorem, Zero-sum problems

1 Davenport and Harborth constants for subgroup weights

For a finite abelian group G and any non-empty $A \subset \mathbb{Z}$, the *Davenport constant of G with weight A*, denoted by $D_A(G)$, is defined (see [2], [3] and [5] for instance) to be the least natural number k such that for any sequence $(x_1, \ldots, x_k)$ of k (not necessarily distinct) elements in G, there exists a non-empty subsequence $(x_{j_1}, \ldots, x_{j_l})$ and $a_1, \ldots, a_l \in A$ such that $\sum_{i=1}^{l} a_i x_{j_i} = 0$. Clearly, if G is of order n, one may consider A to be a non-empty subset of $\{0, 1, \ldots, n-1\}$ and we avoid the trivial case $0 \in A$.

*Corresponding author

For natural numbers n and d, considering the additive group $G = (\mathbb{Z}/n\mathbb{Z})^d$, for a subset $A \subset \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$, we shall use the symbol $D_A(n,d)$ to denote $D_A(G)$ in this case; for the case $d = 1$, the notation $D_A(n)$ has been used (see [2], [4], [5], for instance) for $D_A(n,1)$.

Similarly, for $A \subseteq \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$, the constant $f_A(n,d)$ is defined (see [1]) to be the smallest positive integer k such that for any sequence $(\mathbf{x_1}, \cdots, \mathbf{x_k})$ of k (not necessarily distinct) elements of $(\mathbb{Z}/n\mathbb{Z})^d$, there exists a subsequence $(\mathbf{x_{j_1}}, \cdots, \mathbf{x_{j_n}})$ of length n and $a_1, \cdots, a_n \in A$ such that

$$\sum_{i=1}^{n} a_i \mathbf{x_{j_i}} = \mathbf{0},$$

where $\mathbf{0}$ is the zero element of the group $(\mathbb{Z}/n\mathbb{Z})^d$. When $d = 1$, this was denoted by $E_A(n)$ in [2] and [4]. The conjectured relation $E_A(n) = D_A(n) + n - 1$, between the constants $E_A(n)$ and $D_A(n)$, has been proved by Yuan and Zeng ([14]); and the related general conjecture has also been established by Grynkiewicz, Marchan and Ordaz ([7]) recently.

These constants are respectively the analogues of the Davenport constant (see [10], for instance) and some constant considered by Harborth [8] and others ([6], [9], [12], [13]). We shall be mainly interested in the numbers $D_U(p,d)$ and $f_U(p,d)$, where $n = p$, a prime and U a subgroup of $\mathbb{Z}_p^*$. Here, and henceforth, for a positive integer n, we shall write $\mathbb{Z}_n$, and $\mathbb{Z}_n^*$ in place of $\mathbb{Z}/n\mathbb{Z}$, and $\{a \leq n : (a,n) = 1\}$ respectively, for simplicity.

We shall often use the following simple observation :
If $U \leq \mathbb{Z}_p^*$ is a subgroup, then

$$U = Ker(x \mapsto x^{|U|}) = Im(x \mapsto x^{(p-1)/|U|}).$$

Proposition 1.

(i) *For any subgroup $U \leq \mathbb{Z}_p^*$, we have*
$d(D_U(p,1) - 1) < D_U(p,d) \leq \frac{d(p-1)}{|U|} + 1.$
Equality holds on the right if $U = \mathbb{Z}_p^*$, the subgroup $\{1\}$ or the set of quadratic residues.
Also, in general $D_U(p,d) = \frac{d(p-1)}{|U|} + 1$ if $D_U(p,1) = \frac{p-1}{|U|} + 1$.

(ii) *For any subgroup* $U \leq \mathbb{Z}_n^*$, *we have* $D_U(n,d) \geq d(l-1)+1$, *where* l *is the least natural number for which* U *has a zero-sequence of length* l. *In particular, if* $n = p$, *a prime, then* $D_U(p,d) = \frac{d(p-1)}{|U|}+1$ *if* $l > \frac{p-1}{|U|}$.

(iii) *If* p *is odd and* $U \leq \mathbb{Z}_p^*$ *contains* $1, -1$ *(in particular, if* $\frac{p-1}{|U|}$ *is odd), then* $D_U(p,d) \leq \log_2(p^d+1)$.

Proof of (i).
The inequality $d(D_U(p,1)-1) < D_U(p,d)$ is evident. For the other inequality, write $D = \frac{d(p-1)}{|U|}+1$ for simplicity of notation. Let $\mathbf{a_1}, \cdots, \mathbf{a_D} \in (\mathbb{Z}/p\mathbb{Z})^d$ be arbitrary. Write $\mathbf{a_i} = (a_{i1}, \cdots, a_{id})$ for all $i \leq D$. Consider the D polynomials

$$\sum_{i=1}^{D} a_{ij} X_i^{(p-1)/|U|}\ ,\ j \leq d.$$

The sum of the degrees of these homogeneous polynomials is $d(p-1)/|U|$ which is less than D. By the Chevalley-Warning theorem, there is a solution $X_i = x_i \in \mathbb{Z}_p$ with not all x_i zero. Writing $I = \{i : x_i \neq 0\}$, and $u_i = x_i^{(p-1)/|U|}$ for $i \in I$, we have $u_i \in U$ as observed above. So, we have

$$\sum_{i \in I} u_i \mathbf{a_i} = \mathbf{0} \in (\mathbb{Z}/p\mathbb{Z})^d,$$

which means that $D(U,p,d) \leq D = \frac{d(p-1)}{|U|}+1$.

To prove the equalities asserted, use these inequalities and the following zero-sum free sequences. The sequence $(1,0,\cdots,0), (0,1,\cdots,0), \cdots, (0,0,\cdots,1)$ shows $D_U(p,d) > d$, when $U = \mathbb{Z}_p^*$. For the case $U = \{1\}$, we can consider the sequence comprising of each of

$$(1,0,\cdots,0), (0,1,\cdots,0), \cdots, (0,\cdots,0,1)$$

repeated $p-1$ times. Finally, if U is the set of quadratic residues, then write $\mathbb{Z}_p^* = U \sqcup \alpha U$. Then, the sequence of $2d$ elements

$$(1,0,\cdots,0), (-\alpha,0,\cdots,0), (0,1,\cdots,0), (0,-\alpha,0,\cdots,0),$$

$$\cdots\cdots, (0,\cdots,0,1), (0,\cdots,0,-\alpha)$$

of $(\mathbb{Z}/p\mathbb{Z})^d$ can have no zero-subsequence. Thus, $D_U(p,d) > 2d$. This proves (i).

Proof of (ii).

Consider the sequence of length $\frac{d(p-1)}{|U|}$ in $(\mathbb{Z}/p\mathbb{Z})^d$ comprising of each of

$$(1,0,\cdots,0),(0,1,\cdots,0),\cdots,(0,\cdots,0,1)$$

repeated $\frac{p-1}{|U|}$ times. If it has a subsequence, say $\mathbf{a_1},\cdots,\mathbf{a_k}$ and elements $u_1,\cdots,u_k$ in U such that $\sum_{i=1}^k u_i\mathbf{a_i} = \mathbf{0} \in (\mathbb{Z}/p\mathbb{Z})^d$, then looking at each co-ordinate, we have $\min\{l : U$ has a zero-sequence of length $l\} \leq \frac{p-1}{|U|}$, a contradiction of the hypothesis. Thus (ii) is proved.

Proof of (iii).

Note firstly that if $(p-1)/|U|$ is odd, then $1,-1 \in U$ by the observation in the beginning. Write $D = \lceil \log_2(p^d+1) \rceil$ and consider any sequence $a_1,\cdots,a_D$ of length D in $(\mathbb{Z}/p\mathbb{Z})^d$. For each of the 2^D-1 nonempty subsets J of $\{1,2,\cdots,D\}$, look at the sum $\sum_{j\in J} a_j \in (\mathbb{Z}/p\mathbb{Z})^d$. Note $2^D-1 \geq p^d$. If these 2^D-1 sums are all distinct elements of $(\mathbb{Z}/p\mathbb{Z})^d$, then they must be the various elements of this group and one of them is zero. If these sums are not distinct, there exist two subsets $J_1 \neq J_2$ of $\{1,2,\cdots,D\}$ such that $\sum_{j\in J_1} a_j = \sum_{i\in J_2} a_i$. Cancelling off all the terms corresponding to $J_1 \cap J_2$, we have a nonempty subset J_0 and $\epsilon_j \in \{1,-1\}$ such that $\sum_{j\in J_0} \epsilon_j a_j = 0 \in (\mathbb{Z}/p\mathbb{Z})^d$. This completes the proof.

Remarks.

(i) If $U \neq \mathbb{Z}_p^*$ is a subgroup of $\mathbb{Z}_p^*$ such that $-1 \in U$, then $\{1,-1\}$ is a zero-sum in U of length 2 and hence $\min\{l : U$ has a zero-sequence of length $l\} = 2$ and the condition in (ii) of the proposition is not satisfied for the subgroup U of $\mathbb{Z}_p^*$. For instance, if $p \equiv 1 \pmod 4$ and U is the set of quadratic residues mod p, then we are in this situation.

(ii) The bound $D_U(p,d) \leq \frac{d(p-1)}{|U|} + 1$ may not be tight in general. For example, if U is a subgroup of $\mathbb{Z}_p^*$ of index 3, for $p = 7, 13, 19$, we have $D_U(p,1) < 4$.

(iii) The value of $D_U(p,d)$ for the case $U = \{1\}$ is well known. In fact, this case corresponds to the classical Davenport constant and the value is known for all finite abelian p -groups (Olson [10]). We shall be using the result in the particular case in the next proposition.

Proposition 2.
Let $A = \{1, 2, \cdots, r\}$, *where* r *is an integer such that* $1 < r < p$. *We have*

(i) $D_A(p,d) \leq \left\lceil \frac{d(p-1)+1}{r} \right\rceil$, *where for a real number* x, $\lceil x \rceil$ *denotes the smallest integer* $\geq x$,

(ii) *We have*

$$D_A(p,d) > \left[\frac{p}{r}\right] d.$$

Proof of (i).
Write $D = \left\lceil \frac{d(p-1)+1}{r} \right\rceil$. Let $S = \mathbf{a_1}, \cdots, \mathbf{a_D} \in (\mathbb{Z}/p\mathbb{Z})^d$ be arbitrary.

Considering the sequence

$$S' = (\overbrace{\mathbf{a_1}, \mathbf{a_1}, \cdots, \mathbf{a_1}}^{r \text{ times}}, \overbrace{\mathbf{a_2}, \mathbf{a_2}, \cdots, \mathbf{a_2}}^{r \text{ times}}, \cdots, \overbrace{\mathbf{a_D}, \mathbf{a_D}, \cdots, \mathbf{a_D}}^{r \text{ times}}),$$

obtained from S by repeating each element r times, and observing that the length of this sequence is $\geq d(p-1)+1$ and from Part (i) of Proposition 1, $D_U(p,d) = d(p-1)+1$ when U is the subgroup $\{1\}$, the result follows.

Proof of (ii).
Considering the sequence comprising of each of

$$(1, 0, \cdots, 0), (0, 1, \cdots, 0), \cdots, (0, \cdots, 0, 1)$$

repeated $\left[\frac{p}{r}\right]$ times, let $(t_1, t_2, \cdots, t_d)$ be a sum of some of the elements of this sequence with weights a_i from the set $A = \{1, 2, \cdots, r\}$. If $(0, \cdots, 0, 1, 0, \cdots, 0)$ with 1 at the i-th place is involved in the sum, then we have $0 < t_i \leq \left[\frac{p}{r}\right] r < p$, and the result follows.

Remarks.

(i) If r divides $(p-1)$, then from Part (i) we have

$$D_A(p,d) \leq \left\lceil \frac{d(p-1)+1}{r} \right\rceil = \frac{(p-1)d}{r} + 1.$$

On the other hand, from Part (ii) we have

$$D_A(p,d) > \left[\frac{p}{r}\right] d = \frac{(p-1)d}{r},$$

thus obtaining the exact value of $D_A(p,d)$ in this case.

(ii) Since the value of the classical Davenport constant is known for all finite abelian p -groups (Olson [10]) and for all finite abelian groups of rank 2 (Olson [11]) it is clear that results similar to the above proposition can be obtained for groups of the form $(\mathbb{Z}/p^k\mathbb{Z})^d$ and $(\mathbb{Z}/n\mathbb{Z})^2$, for positive integers k and n.

The following proposition generalizes some results in [5] and some in [4].

Proposition 3.

(i) *For* $U = \mathbb{Z}_p^*$, $f_U(p, d) = p + d$, *if* $d < p$. *In particular,* $f_U(p, p-1) = 2p - 1$.

(ii) $f_U(p, d) \leq \frac{d(p-1)}{|U|} + p$ *if* $d < \frac{p|U|}{p-1}$. *In particular,* $f_U(p, |U|) \leq 2p - 1$. *Moreover, if* U *is the group of quadratic residues, then for* $d \leq (p-1)/2$, *we have* $f_U(p, d) = p + 2d$.

(iii) $f_U(p, 1) \geq p - 1 + D_U(p, 1)$ *for any subgroup* U *of* $\mathbf{Z}_p^*$. *Further, the equality* $f_U(p, 1) = p - 1 + D_U(p, 1)$ *holds when* $D_U(p, 1) = 1 + \frac{p-1}{|U|}$.

Proof of (i).

Let $\mathbf{a_1}, \cdots, \mathbf{a_{p+d}} \in (\mathbb{Z}/p\mathbb{Z})^d$ be arbitrary. Write $\mathbf{a_i} = (a_{i1}, \cdots, a_{id})$ for all $i \leq p + d$. Considering the $d + 1$ polynomials

$$\sum_{i=1}^{p+d} a_{ij} X_i \ , \ j \leq d$$

and

$$\sum_{i=1}^{p+d} X_i^{p-1}$$

it follows by the Chevalley-Warning theorem that there is a nontrivial solution $X_i = x_i \in \mathbb{Z}_p$ because the sum of the degrees is $d + p - 1 < p + d$. If $I = \{i : x_i \neq 0\}$ we have $|I| = p$ because $p + d < 2p$. Therefore,

$$\sum_{i \in I} x_i \mathbf{a_i} = \mathbf{0} \in (\mathbb{Z}/p\mathbb{Z})^d.$$

The fact that $f_U(p,d) > p+d-1$ follows by considering the following p-zerosum-free sequence of length $d+p-1$:

$$\underbrace{(0,\cdots,0),\cdots,(0,\cdots,0)}_{p-1 \text{ times}},(1,0,\cdots,0),(0,1,\cdots,0),\cdots,(0,0,\cdots,1).$$

Proof of (ii).
This has a similar proof. Let $\mathbf{a_1},\cdots,\mathbf{a_{2p-1}} \in (\mathbb{Z}/p\mathbb{Z})^d$ be arbitrary. Let $d < \frac{p|U|}{p-1}$. Write $\mathbf{a_i} = (a_{i1},\cdots,a_{id})$ for $i = 1,2,\cdots,2p-1$. Considering the $d+1$ polynomials

$$\sum_{i=1}^{t} a_{ij} X_i^{(p-1)/|U|} \ , \ j \leq d$$

and

$$\sum_{i=1}^{t} X_i^{p-1},$$

with

$$t = \frac{d(p-1)}{|U|} + p,$$

the proof follows as before.
To see that $f_U(p,d) > p+d-1$ when U is the group of quadratic residues and $d \leq (p-1)/2$, consider the sequence $(0,\cdots,0)$ repeated $p-1$ times, along with the d elements $(1,0,\cdots,0),(0,1,\cdots,0),\cdots(0,0,\cdots,1)$ and the d elements $(-t,0,\cdots,0),(0,-t,\cdots,0),\cdots(0,0,\cdots,-t)$ where $\mathbf{Z}_p^* = U \sqcup tU$. Clearly, it has no zero-sum of length p with weights from U.
Proof of (iii).
Clearly, a sequence of length $D_U(p,1)-1$ which has no zero-sum subsequence with weights in U can be augmented with the sequence $(0,\cdots,0)$ repeated $p-1$ times and the combined sequence cannot contain a zero-sum subsequence of length p. This proves the inequality $f_U(p,1) \geq p-1+D_U(p,1)$. Since the inequality $f_U(p,1) \leq p + \frac{p-1}{|U|}$ was proved in (ii) above, one has the equality $f_U(p,1) \leq p + \frac{p-1}{|U|}$ whenever one has $D_U(p,1) \leq 1 + \frac{p-1}{|U|}$.

Remarks.
Similar to what we observed in the case of $D_U(p,d)$, one has that equality may not hold in (ii) of the above proposition, in general. For instance $f_U(7,2) < 13$ when U is the subgroup of cubic residues.

The other method which is often useful in deducing results on zero-sums, is to use the Cauchy-Davenport theorem which states :
If $A_1, \cdots, A_h$ are non-empty subsets of $\mathbf{Z}_p$, then

$$|A_1 + \cdots + A_h| \geq min\Big(p, \sum_{i=1}^{h} |A_i| - h + 1\Big).$$

Using this, one has, for $a_1, \cdots, a_r \in \mathbf{Z}_p^*$ and for a subset A of $\mathbf{Z}_p$, that

$$|a_1 A + \cdots + a_r A| \geq min(p, r|A| - r + 1).$$

In [4], it was shown that when $n = p_1 p_2 \cdots p_k$ is square-free and coprime to 6, then $f_U(n, 1) = n + 2k$. For prime n, this is a consequence of (ii) of proposition 3 above - in fact, an inductive argument can be used to deduce this result for general square-free n. Now, we prove a generalization of proposition 11 from [4] where subgroups more general than the subgroup of squares are treated; this is the following :

Proposition 4.
(i) *Let $n = p_1 p_2 \cdots p_k$ be odd and, square-free and, let $U_i \leq \mathbf{Z}_{p_i}^*$ be nontrivial subgroups. Consider the subgroup $U \leq \mathbf{Z}_n^*$ mapping isomorphically onto $U_1 \times U_2 \cdots \times U_k$ under the isomorphism $\mathbf{Z}_n^* \to \mathbf{Z}_{p_1}^* \times \cdots \times \mathbf{Z}_{p_k}^*$ given by the Chinese remainder theorem. Suppose $r \geq max\ \{\frac{p_i - 1}{|U_i| - 1} : i \leq k\}$. Further, let $m \geq rk$ and let $a_1, \cdots, a_{m+(r-1)k}$ be a sequence in $\mathbf{Z}_n$. Then, there exists a subsequence $a_{i_1}, \cdots, a_{i_m}$ and elements $u_1, \cdots, u_m \in U$ such that $\sum_j u_j a_{i_j} = 0 \in \mathbf{Z}_n$.*
(ii) *With n, U as above, $f_U(n, 1) \leq n + k(\max_i b_i - 1)$ where $b_i = \left\lceil \frac{p_i - 1}{|U_i| - 1} \right\rceil$.*
Proof.
For the first part we proceed by induction on the number k of prime factors of n.

If $k = 1$, write $n = p$. If there are less than r elements among $a_1, \cdots, a_{m+r-1}$ which are non-zero in $\mathbf{Z}_p$, then at least m of them are zero. Hence, taking m such a_i's and arbitrary units $u_1, \cdots, u_m$ the corresponding sum is zero. If, on the other hand, at least r among the a_i's (say, $a_1, \cdots, a_r$) are in $\mathbf{Z}_p^*$, then the above observation based on the Cauchy-Davenport theorem shows that

$$|a_1 U + \cdots + a_r U| \geq min(p, r|U| - r + 1).$$

Now, $p \leq r|U| - r + 1$ since it is given that $r \geq \frac{p-1}{|U|-1}$.

Hence, $a_1U + \cdots + a_rU = \mathbf{Z}_p$. So, there are $u_1, \cdots, u_r \in U$ such that

$$a_1u_1 + \cdots + a_ru_r = -(a_{r+1} + \cdots + a_m).$$

Thus, the choice $u_{r+1} = \cdots = u_m = 1$ gives $\sum_{i=1}^{m} u_ia_i = 0$. Thus, the case $k = 1$ follows.

Assume that $k \geq 2$ and that the result holds for smaller k.

Consider any sequence $a_1, \cdots, a_{m+(r-1)k}$ in $\mathbf{Z}_n$.

Suppose first that, for each $i \leq k$, at least r among the a_i's are units modulo p_i. So, there is $t \leq rk \leq m$ such that among $a_1, \cdots, a_t$ there are at least r units in $\mathbf{Z}_{p_i}$ for each $i \leq k$. Then, we have solutions of $\sum_{j=1}^{m} a_ju_j^{(i)} \equiv 0 \mod p_i$ for $i = 1, \cdots, k$ and $u_j^{(i)} \in U_i$ for each $j \leq m$. As U is a subgroup of $\mathbf{Z}_n^*$ corresponding to the product $U_1 \times U_2 \cdots \times U_k$ by the Chinese remainder theorem, the group U contains elements $u_1, \cdots, u_m$ such that $u_j \equiv u_j^{(i)} \mod p_i$ for $i = 1, \cdots, k$. Therefore, $\sum_{j=1}^{m} u_ja_j \equiv 0 \mod n$. We are done in this case.

Now, consider the case when the sequence of a_i's contain less than r units mod p_i for some p_i, say p_1. Removing them, we have a sequence of $m+(r-1)k-(r-1) = m+(r-1)(k-1)$ elements which are all $\equiv 0 \mod p_1$. By induction hypothesis, the case $k-1$ implies that there is a subsequence $a_{s_1}, \cdots, a_{s_m}$ of this and elements $u_1^{(i)}, \cdots, u_m^{(i)} \in U_i$ for each $i \geq 2$ such that $\sum_{j=1}^{m} u_j^{(i)}a_{s_j} \equiv 0 \mod p_i$ for every $i \geq 2$. Since a_{s_j}'s are all 0 mod p_1, it follows that $\sum_{j=1}^{m} a_{s_j} \equiv 0 \mod p_1$. Choosing elements $u_1, \cdots, u_m \in U$ by the Chinese remainder theorem, we have $\sum_{j=1}^{m} u_ja_{s_j} \equiv 0 \mod p_i$ for all $i \geq 1$. Thus, we have $\sum_{j=1}^{m} u_ja_{s_j} \equiv 0 \mod n = p_1p_2\cdots p_k$. This completes the proof.

Taking $m = n$, (ii) follows from (i); one simply uses the observation that $n \geq kr$.

Remarks.
As has been remarked following Proposition 3, the upper bounds in the above proposition may not be tight. In fact, it can be checked that $f_U(13, 1) \leq 15$ where U is the subgroup consisting of cubes.

Finally, we partially generalize the result $f_{\{1,-1\}}(n, 2) = 2n - 1$ proved in [1] for odd n. The following Proposition treats the problem for more general subgroups and for general d. We obtain only an upper bound.

Proposition 5.
Let U be a subset of $\mathbb{Z}_n^*$ closed under multiplication. Suppose that for each

prime p dividing n, the set $\{u \bmod p : u \in U\}$ is a subgroup of $\mathbb{Z}_p^*$ of order at least d. Then,

$$f_U(n,d) \leq 2n-1.$$

Further, equality holds when $U = \{1,-1\}$, $d=2$ and n is odd.

Proof.

This will be proved by induction on the number of prime factors of n (counted with multiplicity). The prime case is covered by Proposition 3. Write $n = \prod_{i=1}^{k} p_i^{l_i}$. Start with a sequence $\mathbf{a_1}, \cdots, \mathbf{a_{2n-1}}$ of length $2n-1$ in $\mathbb{Z}_n^d$. Look at the subsequence $\mathbf{a_1}, \cdots, \mathbf{a_{2p_1-1}}$. Since $\{u \text{ mod } p : u \in U\}$ is a subgroup of $\mathbb{Z}_p^*$ of order at least d, Proposition 3(ii) gives a p_1-subsequence, say $\mathbf{a_1}, \cdots, \mathbf{a_{p_1}}$ and elements $u'_1, \cdots, u'_{p_1} \in \{u \text{ mod } p_1 : u \in U\}$ such that $\sum_{i=1}^{p_1} \mathbf{a_i} u'_i = 0$ in $(\mathbb{Z}_{p_1})^d$. This means that $\sum_{i=1}^{p_1} \mathbf{a_i} u_i = p_1 \mathbf{b_1}$ for some tuple $\mathbf{b_1}$. Keeping away this p_1-subsequence and working with the rest, we get another p_1-sequence. We may, in this manner choose $2m-1$ such subsequences (where $n = mp_1$) and corresponding elements in U such that

$$\sum_{i=jp_1+1}^{(j+1)p_1} \mathbf{a_i} u_i = p\mathbf{b_{j+1}} \;\; \forall\ 0 \leq j \leq 2m-2.$$

Then, by induction hypothesis, one has elements $v_1, \cdots, v_m$ in U and a m-subsequence, say, $\mathbf{b_1}, \cdots, \mathbf{b_m}$ so that $\sum_{j=1}^{m} \mathbf{b_j} v_j = m\mathbf{b_0}$ for some d-tuple $\mathbf{b_0}$. Since U is closed under multiplication modulo n, we will have then a pm-subsequence of the original sequence and elements of U such that the sum is 0 mod n. The equality $f_U(n,2) = 2n-1$ when $U = \{1,-1\}$ and n is odd is clear from considering the sequence $(1,0)$ repeated $n-1$ times along with the sequence $(0,1)$ repeated $n-1$ times as well.

Remarks.

(i) There are many examples of U satisfying the hypothesis of the above theorem apart from $U = \{1,-1\}$ which was considered in [1]. For instance, the whole of $\mathbb{Z}_n^*$ is one such. More generally, if $n = p_1 p_2 \cdots p_r$ is square-free, then for any subgroups $U_i \leq \mathbb{Z}_{p_i}^*$, the Chinese remainder theorem gives us a subgroup U of $\mathbb{Z}_n^*$ isomorphic to the product of the U_i's.

(ii) Using the above method, one can also prove the following result about the Davenport constant. If $n = \prod_{i=1}^{k} p_i^{l_i}$ is the prime factorization of n, then

$$D_{U(n,r)}(n,d) \leq \prod_{i=1}^{k} D_{U(p_i,r)}(p_i,d)^{l_i} \leq \prod_{i=1}^{k} \{\frac{d(p_i-1)}{(p_i-1,r)}+1\}^{l_i}.$$

Here, we have denoted by $\mathbb{Z}_n^*$, the group of units of $\mathbb{Z}/n\mathbb{Z}$ and, for $r \geq 1$, write $U(n,r) = \{u^r : u \in \mathbb{Z}_n^*\}$. Note that $|U(p_i,r)| = \frac{p_i-1}{(p_i-1,r)}$.

Acknowledgement.
We are indebted to the referee for pointing out a small gap in the earlier version of proposition 1 (iii).

References

[1] S.D.Adhikari, R.Balasubramanian, F.Pappalardi & P.Rath - *Some zero-sum constants with weights*, Proc. Indian Acad.Sci.. (Math.Sci.) **118**, No. 2, 183–188 (2008).

[2] S.D. Adhikari and Y. G. Chen, *Davenport constant with weights and some related questions II.*, J. Combin. Theory Ser. A **115**, No. 1, 178–184 (2008).

[3] S. D. Adhikari, Y. G. Chen, J. B. Friedlander, S. V. Konyagin and F. Pappalardi, *Contributions to zero–sum problems*, Discrete Math. **306**, 1–10 (2006).

[4] S.D.Adhikari, C.David & J.J.Urroz, *Generalizations of some zero-sum theorems*, Integers, Electronic Journal of Combinatorial Number Theory **8**, A 52, (2008).

[5] Sukumar Das Adhikari and Purusottam Rath, *Davenport constant with weights and some related questions*, Integers **6**, A30, (2006).

[6] N. Alon and M. Dubiner, *A lattice point problem and additive number theory*, Combinatorica **15**, 301–309 (1995).

[7] D. J. Grynkiewicz, L. E. Marchan and O. Ordaz, *A weighted generalization of two theorems of Gao*, Priprint.

[8] H. Harborth, *Ein Extremalproblem für Gitterpunkte*, J. Reine Angew. Math. **262/263**, 356–360 (1973).

[9] A. Kemnitz, *On a lattice point problem*, Ars Combin., **16b**, 151–160 (1983).

[10] J. E. Olson, *A combinatorial problem in finite abelian groups, I*, J. Number Theory, **1**, 8–10 (1969).

[11] J. E. Olson, *A combinatorial problem in finite abelian groups, II*, J. Number Theory, **1**, 195–199 (1969).

[12] Christian Reiher, *On Kemnitz's conjecture concerning lattice-points in the plane*, Ramanujan J., **13**, No. 1-3, 333–337 (2007).

[13] L. Rónyai, *On a conjecture of Kemnitz*, Combinatorica, **20** (4), 569–573 (2000).

[14] Pingzhi Yuan and Xiangneng Zeng, *Davenport constant with weights*, Preprint.