GENERALIZATIONS OF SOME ZERO-SUM THEOREMS

Sukumar Das Adhikari
Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211 019, INDIA
adhikari@mri.ernet.in

Chantal David
Department of Mathematics, Concordia University, 1455 de Maisonneuve West, Montréal, QC, Canada, H3G 1M8
cdavid@mathstat.concordia.ca

Jorge Jiménez Urroz
Universitat Politecnica de Catalunya, Campus Nord, C3, C/ Jordi Girona, 1-3. 08034 Barcelona, Spain
jjimenez@ma4.upc.edu

Received: 6/27/08, Revised: 10/2/08, Accepted: 11/2/08, Published: 12/3/08

Abstract

For a finite abelian group G and a finite subset $A \subseteq \mathbb{Z}$, the Davenport constant of G with weight A, denoted by $D_A(G)$, is defined to be the smallest positive integer k such that for any sequence $(x_1, \dots, x_k)$ of k elements in G there exists a non-empty subsequence $(x_{j_1}, \dots, x_{j_r})$ and $a_1, \dots, a_r \in A$ such that $\sum_{i=1}^{r} a_i \ x_{j_i} = 0$. To avoid trivial cases, one assumes that the weight set A does not contain 0 and it is non-empty. Similarly, for any such A and an abelian group G with $|G| = n$, the constant $E_A(G)$ is the smallest positive integer k such that for any sequence $(x_1, \dots, x_k)$ of k elements in G there exists $x_{j_1}, \dots, x_{j_n}$ such that $\sum_{i=1}^{n} a_i \ x_{j_i} = 0$, with $a_i \in A$. In the present paper, we consider the problem of determining $E_A(n)$ and $D_A(n)$ where A is the set of squares in the group of units in the cyclic group $\mathbb{Z}/n\mathbb{Z}$.

1. Introduction

For a finite abelian group G, the Davenport constant $D(G)$ is the smallest positive integer k such that any sequence of k elements in G has a non-empty subsequence whose sum is zero. For a finite abelian group G, with cardinality $|G| = n$, another combinatorial invariant

The second author was partially supported by a NSERC Discovery Grant. The last author was partially supported by Secretaría de Estado de Universidades e Investigación del Ministerio de Educación y Ciencia of Spain, DGICYT Grants MTM2006-15038-C02-02 and TSI2006-02731.

$E(G)$ is defined to be the smallest positive integer k such that any sequence of k elements in G has a subsequence of length n whose sum is zero. These two constants were being studied independently before the following result of Gao [11]:

$$E(G) = D(G) + n - 1. \tag{1}$$

Generalizations of these constants with weights were considered in [5] and [6] for the particular group $\mathbb{Z}/n\mathbb{Z}$. Later, in [4], the following generalizations of both $E(G)$ and $D(G)$ for an arbitrary finite abelian group G of order n were introduced. One may look into [2] for an elaborate account of this theme.

For a finite abelian group G and a finite subset $A \subseteq \mathbb{Z}$, the Davenport constant of G with weight A, denoted by $D_A(G)$, is defined to be the smallest positive integer k such that for any sequence $(x_1, \ldots, x_k)$ of k elements in G there exists a non-empty subsequence $(x_{j_1}, \ldots, x_{j_r})$ and $a_1, \ldots, a_r \in A$ such that

$$\sum_{i=1}^{r} a_i \, x_{j_i} = 0.$$

To avoid trivial cases, one assumes that the weight set A does not contain 0 and it is non-empty. Further, if $|G| = n$, one can assume that $A \subseteq \{1, 2, \ldots, n-1\}$.

Similarly, for any such A and an abelian group G with $|G| = n$, the constant $E_A(G)$ is the smallest positive integer k such that for any sequence $(x_1, \ldots, x_k)$ of k elements in G there exists $x_{j_1}, \ldots, x_{j_n}$ such that

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

with $a_i \in A$.

Taking $A = \{1\}$, we retrieve the classical constants $D(G)$ and $E(G)$. A result similar to the above result (1) of Gao is expected to hold for the generalized constants with weights. In many special cases this relation has been established (see [3], [4], [5], [12], [13], [15]).

One of the few general results known in this direction is the following one due to Adhikari and Chen [4]; one notes that it does not include the result (1) of Gao which corresponds to the case $|A| = 1$.

Theorem A. *Let G be a finite abelian group of order n and $A = \{a_1, \ldots, a_r\}$ be a finite subset of $\mathbb{Z}$ with $r \geq 2$. If* $\gcd(a_2 - a_1, \ldots, a_r - a_1, n) = 1$, *then*

$$E_A(G) = D_A(G) + n - 1.$$

When G is the cyclic group $\mathbb{Z}/n\mathbb{Z}$, we denote $E_A(G)$ and $D_A(G)$ by $E_A(n)$ and $D_A(n)$ respectively. Exact values for $D_A(n)$ and $E_A(n)$ have been found in some cases (see [3],[5], [6], [12], [13]). For instance, it has been proved in [6] that $D_A(p) = 3$ and $E_A(p) = p + 2$, for all primes p when A is the set of quadratic residues modulo p. In the present paper we consider its natural generalization, that is, the problem of determining $E_A(n)$ and $D_A(n)$ where A is the set of squares in the group of units in the cyclic group $\mathbb{Z}/n\mathbb{Z}$ for a general integer n. In the rest of the paper, we will denote this set as $R_n = \{x^2 : x \in (\mathbb{Z}/n\mathbb{Z})^*\}$. When it is obvious from the context, we shall simply write R in place of R_n. Also, $\omega(n)$ will denote the number of distinct prime factors of n and $\Omega(n)$ the number of prime factors counting multiplicity; clearly, for a square-free integer n one has $\omega(n) = \Omega(n)$. We prove the following results. For a general integer we have:

Theorem 1. *Let n be an integer. Then*

$$\begin{aligned} \text{(i)} \quad D_R(n) &\geq 2\Omega(n) + 1, \textit{ and} \\ \text{(ii)} \quad E_R(n) &\geq n + 2\Omega(n). \end{aligned}$$

When restricting to square-free integers we can say much more.

Theorem 2. *Let n be a square-free integer, coprime to 6. Then*

$$\begin{aligned} \text{(i)} \quad D_R(n) &= 2\omega(n) + 1, \textit{ and} \\ \text{(ii)} \quad E_R(n) &= n + 2\omega(n). \end{aligned}$$

As it will be observed from Part (ii) of Theorem 4 below, when the prime 3 is involved, the constants $D_R(n)$ and $E_R(n)$ may be strictly greater than the values given in the above theorem. In this case we can prove the following:

Theorem 3. *Let n be any square-free odd integer such that $3 \mid n$. Then*

$$\begin{aligned} \text{(i)}\, D_R(n) &\leq 6\omega(n) - 3, \textit{ and} \\ \text{(ii)}\, E_R(n) &\leq n + 6\omega(n) - 4. \end{aligned}$$

However, we have the following precise result.

Theorem 4. *We have*

$$\begin{aligned} &\text{(i)} \quad D_R(3p) = 5 \textit{ for primes } p \geq 7, \textit{ and} \\ &\text{(ii)} \quad D_R(15) = 6. \end{aligned}$$

When the prime 2 is involved we have the following results.

Theorem 5. *Let n be any square-free even integer such that $3 \nmid n$. Then*

$$\begin{aligned} \text{(i)}\, D_R(n) &\leq 4\omega(n) - 2, \textit{ and} \\ \text{(ii)}\, E_R(n) &\leq n + 4\omega(n) - 3. \end{aligned}$$

Theorem 6. *Let n be any square-free integer which is a multiple of 6. Then*

$$\begin{aligned} \text{(i)}\, D_R(n) &\leq 6\omega(n) - 6, \textit{ and} \\ \text{(ii)}\, E_R(n) &\leq n + 6\omega(n) - 7. \end{aligned}$$

In the non-square-free case, we have the following result.

Theorem 7. *Let $n = p^r$, for $p > 3$ prime. Then,*

$$\begin{array}{lrcl} \text{(i)} & D_R(n) & = & 2\Omega(n) + 1, \textit{ and} \\ \text{(ii)} & E_R(n) & = & n + 2\Omega(n). \end{array}$$

Finally, we dedicate Section 3 to investigate other sets of weights. Among other remarks, we are able to prove the following result. As usual, we write $\lceil x \rceil$ for the smallest integer larger than or equal to x.

Theorem 8. *Let n, r be positive integers, $1 \leq r < n$ and consider the subset $A = \{1, \ldots, r\}$ of $\mathbb{Z}/n\mathbb{Z}$. Then,*

$$\begin{array}{lrcl} \text{(i)} & D_A(n) & = & \left\lceil \frac{n}{r} \right\rceil, \textit{ and} \\ \text{(ii)} & E_A(n) & = & n - 1 + D_A(n). \end{array}$$

This theorem also generalizes a result in [6], where the case n prime was proved.

2. Proofs of Theorems

Proof of Theorem 1. We start by proving (i). Let $n = \prod_{i=1}^{\omega(n)} p_i^{\alpha_i}$, and consider the sequence of $2\Omega(n)$ elements given by $x_{i,j} = np_i^{j-\alpha_i}$ for $i = 1, \ldots, \omega(n)$, $j = 0, \ldots, \alpha_i - 1$, and $y_{i,j} = -v_i x_{i,j}$, for $i = 1, \ldots, \omega(n)$, $j = 0, \ldots, \alpha_i - 1$, and $v_i \notin R_{p_i}$. Suppose there exist $s_{i,j}, t_{i,j} \in R_n \cup \{0\}$ such that

$$\sum s_{i,j} x_{i,j} + t_{i,j} y_{i,j} = 0.$$

For any i, p_i divides every element of the sequence except $x_{i,0}$, $y_{i,0}$, which implies that

$$s_{i,0} x_{i,0} + t_{i,0} y_{i,0} \equiv 0 \pmod{p_i},$$

and hence $s_{i,0} = t_{i,0} = 0$. Now, by an easy induction procedure, we obtain that $s_{i,j} = t_{i,j} = 0$, for all i, j and we obtain (i).

In order to prove (ii) we just have to note that, if we append a sequence of $n-1$ zeroes to a sequence of length $D_R(n) - 1$ with no zero sum (which exists by the definition of $D_R(n)$), then the resulting sequence will have no subsequence of length n which sums up to zero and hence

$$E_R(n) \geq D_R(n) + n - 1. \tag{2}$$

This proves the theorem. □

For the rest of the theorems we shall need the following version of the Cauchy-Davenport Theorem (see [7], [9]; one can also find it in [14] for instance).

Theorem B (Cauchy-Davenport). *If p is a prime and $A_1, A_2, \ldots, A_h$ are non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$, then*

$$|A_1 + A_2 + \ldots + A_h| \geq min\left(p, \sum_{i=1}^{h} |A_i| - (h-1)\right).$$

We shall also need the following generalization of the above result in the case $h = 2$ (see [8] and [14]).

Theorem C (Chowla). *Let n be a natural number, and let A and B be two nonempty subsets of $\mathbb{Z}/n\mathbb{Z}$, such that $0 \in B$ and $A + B \neq \mathbb{Z}/n\mathbb{Z}$. If $(x, n) = 1$, for all $x \in B \setminus \{0\}$, then $|A + B| \geq |A| + |B| - 1$.*

Lemma 9. *If $p \geq 7$ is a prime and $x_1, \ldots, x_k$ are elements of $\mathbb{Z}/p\mathbb{Z}$ with at least three of them being non-zero, then there exist $a_i \in R_p$, $i = 1, \ldots, k$, such that $\sum_{i=1}^{k} a_i\ x_i = 0$.*

Proof. Without loss of generality, let x_1, x_2, x_3 be units. By Theorem B,

$$|x_1R_p + x_2R_p + x_3R_p| \geq min\left(p, \frac{3(p-1)}{2} - 2\right) = p.$$

Therefore, one can write $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 = -(x_4 + x_5 + \ldots + x_k)$, where $\alpha_i \in R_p$. □

We also have the following lemma, the proof of which is similar to the proof of Lemma 9.

Lemma 10. *If $x_1, \ldots, x_k$ are elements of $\mathbb{Z}/5\mathbb{Z}$ with at least four of them being non-zero, then there exists $a_i \in R_5$, $i = 1, \ldots, k$, such that $\sum_{i=1}^{k} a_i\ x_{j_i} = 0$.*

Theorem 2 will be an easy corollary of Propositions 11 and 12 below. As it can be seen, the bulk of the work goes towards the proof of Proposition 12.

Proposition 11. *Let $n = p_1 \ldots p_r$, $r \geq 1$ be a square-free integer all of whose prime factors are greater than or equal to 7. Let $m \geq 3r$ and $(x_1, \ldots, x_{m+2r})$ be a sequence of elements of $\mathbb{Z}/n\mathbb{Z}$. Then there exists a subsequence $(x_{i_1}, \ldots, x_{i_m})$ and $a_1, \ldots, a_m \in R_n$ such that $\sum_{j=1}^{m} a_j\ x_{i_j} = 0$.*

Proposition 12. *Let $n = p_1 \ldots p_r$, $r \geq 1$ be a square-free integer where $p_1 = 5$ and $p_i \geq 7$, for all $i \geq 2$. Let $m \geq 3r + 1$ and $(x_1, \ldots, x_{m+2r})$ be a sequence of $m + 2r$ elements in $\mathbb{Z}/n\mathbb{Z}$. Then there exists a subsequence $(x_{i_1}, \ldots, x_{i_m})$ and $a_1, \ldots, a_m \in R_n$ such that $\sum_{j=1}^{m} a_j\ x_{i_j} = 0$.*

We observe that in the above propositions, the results would be true if the given sequence has more than $m + 2r$ elements, say $t + m + 2r$ elements, with $t \geq 1$, without considering the extra t elements.

Proof of Proposition 11. We proceed by induction on r. When $r = 1$, we have $n = p$, a prime. By Lemma 9, given any sequence $(x_1, \ldots, x_{m+2})$ of elements modulo p with at least three non-zero elements, there are $a_i \in R_p$ for $i = 1, \ldots, m$ such that $\sum_{i=1}^{m} a_i\ x_i = 0$. Otherwise, at most two elements of the sequence are units which implies that at least m elements say $x_{j_1}, \ldots, x_{j_m}$ are divisible by p and hence $\sum_{i=1}^{m} a_i \ x_{j_i} = 0$ for any choice of $a_i \in R_p$ for each $i = 1, \ldots, m$. This establishes the case with $r = 1$.

Suppose now that $r \geq 2$ and the result is true for any square-free odd integer with a number of prime factors not exceeding $r - 1$ provided all its prime factors are ≥ 7. Suppose we are given a sequence $(x_1, \ldots, x_{m+2r})$ of $m + 2r$ elements of $\mathbb{Z}/n\mathbb{Z}$.

Suppose that, for each prime $p \mid n$, the sequence contains three elements coprime to p. Then, without loss of generality, let $S = (x_1, \ldots, x_t)$ be a subsequence of $t \leq 3r \leq m$ elements such that S has three units corresponding to each prime.

Then, by Lemma 9, for each prime p_i, we have $\sum_{j=1}^{m} a_j^{(i)} \ x_j \equiv 0 \pmod{p_i}$, with some $a_j^{(i)} \in R_{p_i}$. The result now follows by the Chinese Remainder Theorem.

If, on the other hand, the sequence does not contain three elements coprime to every prime p_i, there is a prime p_l such that the sequence does not contain more than two elements coprime to it. We remove those elements and consider a subsequence of $m+2(r-1)$ elements all whose elements are 0 in $\mathbb{Z}/p_l\mathbb{Z}$. By the induction hypothesis, there is a subsequence $(x_{i_1}, \ldots, x_{i_m})$ such that $\sum_{j=1}^{m} a_j^{(i)} \ x_{i_j} \equiv 0 \pmod{p_i}$, for some $a_j^{(i)} \in R_{p_i}$, for all $i \neq l$. However,

$$\sum_{j=1}^{m} a_j^{(l)} \ x_{i_j} \equiv 0 \pmod{p_l},$$

where $a_j^{(l)} = 1$, for all $j = 1, \ldots, m$. Once again, we are through via the Chinese Remainder Theorem. □

Proof of Proposition 12. We consider four cases.

`Case 0.` When $n = 5$. In this case, $r = 1$ and we are given a sequence $(x_1, \ldots, x_{m+2})$ of elements modulo 5, where $m \geq 4$. If there are at least four non-zero elements of $\mathbb{Z}/5\mathbb{Z}$ in the given sequence, the result is true by Lemma 10. If there are not more than two non-zero elements, then the sequence has at least m multiples of 5 and the result follows for these elements and any choice of $a_i \in R_5$.

If there are exactly three non-zero elements of $\mathbb{Z}/5\mathbb{Z}$ in the given sequence, let them be x_1, x_2, x_3. Since $D_R(p) = 3$ for any prime p, where R is the set of quadratic residues modulo p (see Theorem 3 of [6]), we have $\sum_{i \in I} a_i x_i = 0$, for some nonempty $I \subseteq \{1, 2, 3\}$ and $a_i \in R_5$ for $i \in I$. It is clear that $|I| \geq 2$.

Taking $(x_4, \ldots, x_t)$ with $t = m + (3 - |I|)$, we have $\sum_{i \in I} a_i x_i + \sum_{i=4}^{t} a_i x_i = 0$, where $a_4 = \ldots = a_t = 1$, thus giving us an m-sum with $a_i \in R_5$. ◇

So, let us now suppose that $n > 5$, that is, we have $r \geq 2$. Let $n = 5n_1n_2$, where n_2 is the product of all primes $p|n$, $p \neq 5$ such that the sequence does not contain more than two elements coprime to p. We then remove a sequence of length $t \leq 2\omega(n_2) \leq 2r - 2$, so that each of the remaining elements are divisible by n_2.

Hence, we just have to prove the theorem for the new $N = 5n_1 = p_1 \dots p_{r_1}$, and, in this case, we have a sequence $(x_1, x_2, \dots)$ of at least $m + 2r_1$ elements containing at least three elements coprime to p for any prime $p \mid n_1$.

`Case I.` The sequence contains four units modulo 5. Without loss of generality, let $S = (x_1, \dots, x_t)$ be a subsequence of $t \leq 3r_1 + 1 \leq m$ elements such that S has three units corresponding to each prime p_i for $i = 2, \dots, r_1$, and four elements coprime to 5.

By Lemmas 9 and 10, we have $\sum_{j=1}^{m} a_j^{(i)} \ x_j \equiv 0 \,(\text{mod } p_i)$, for each prime $p_i \mid N$, with $a_j^{(i)} \in R_{p_i}$, for $j = 1, \dots, m$ and the result follows by the Chinese Remainder Theorem. $\diamond$

`Case II.` The sequence contains at most two units modulo 5. We remove the elements coprime with 5, and apply Proposition 11 to the remaining subsequence to obtain another one $x_{j_1}, \dots, x_{j_m}$ with $\sum_{i=1}^{m} a_i \ x_{j_i} \equiv 0 \,(\text{mod } n_1)$, with $a_i \in R_{n_1}$. The result now follows since every element in this subsequence is a multiple of 5. $\diamond$

`Case III.` The sequence contains exactly three units modulo 5. Let x_1, x_2, x_3 be those elements. Once again, since $D_R(p) = 3$, we have $\sum_{i \in I} a_i x_i \equiv 0 \pmod 5$, for some subset I of $\{1, 2, 3\}$ with $|I| \geq 2$ and some $a_i \in R_5$, for $i \in I$. If $|I| = 3$, we have a subsequence of length less than or equal to $3r_1$ and hence, not exceeding m, which will contain x_1, x_2, x_3 and three elements coprime to each of the remaining primes. We complete it to a subsequence of length m, say $x_1, \dots, x_m$.

Now, $\sum_{i=1}^{m} a_i \ x_i \equiv 0 \pmod 5$, where a_1, a_2, a_3 are as above and $a_4, \dots, a_m \in R_5$ are chosen arbitrarily. Applying Lemma 9, we get $\sum_{i=1}^{m} a_i^{(j)} \ x_i \equiv 0 \pmod{p_j}$, with $a_i^{(j)} \in R_{p_j}$, for all $j = 1, \dots, m$ and all prime factors p_j of n_1. The result now follows by the Chinese Remainder Theorem.

If however, $|I| = 2$, let us suppose $1 \notin I$. We remove x_1. Let $\hat{n}$ be the product of those primes $p|n_1$ such that, after removing x_1, there are only two elements coprime to p remaining. We remove all the elements which are coprime to one or more of these primes; observe that we are removing less than $2\omega(\hat{n}) + 1$ elements in the whole process. If after this, there remains at most one unit modulo 5, we remove it. So, in total, we are removing at most $2\omega(\hat{n}) + 2$ elements, and now the result follows by Proposition 11. If after this, there remain two units modulo 5, we argue as in the previous case ($|I| = 3$), but for this new sequence and integer $N/\hat{n}$, which suffices since every remaining element is a multiple of $\hat{n}$. $\diamond$

The four cases exhaust all possibilities, thereby proving the theorem. $\square$

We now prove Theorem 2 using Propositions 11 and 12.

Proof of Theorem 2. Since trivially $n \geq 3r+1$, we can apply Propositions 11 and 12 with $m = n$ to get $E_R(n) \leq n + 2r$. Hence, by Theorem 1 and (2), $n + 2r \leq D_R(n) + n - 1 \leq E_R(n) \leq n + 2r$, which gives the result. □

Proof of Theorem 3. By the Erdős-Ginzburg-Ziv Theorem [10] (can also see [1] or [14], for instance), given any five integers there is a subsequence of three elements which sums up to $0 \pmod 3$. Therefore, given a sequence $(x_1, \ldots, x_{n+6r-4})$ of $n+6r-4$ elements of $\mathbb{Z}/n\mathbb{Z}$, we can pick up $t = p_2 \ldots p_r + 2(r-1)$ disjoint subsequences $I_1, I_2, \ldots, I_t$ one after another each of length 3 such that

$$\sum_{i \in I_j} x_i = 0 \pmod 3,$$

for $i = 1, 2, \ldots, t$. Now, considering the sequence $(y_1, \ldots, y_t)$ where $y_j = \sum_{i \in I_j} x_i$, by Theorem 2 there exists a subsequence $(y_{i_1}, \ldots, y_{i_l})$ with $l = p_2 \ldots p_r$ such that

$$\sum_{j=1}^{l} a_j y_{i_j} = 0 \pmod l,$$

with $a_j \in R_l$.

Since $y_j = \sum_{i \in I_j} x_i$, where $|I_j| = 3$ for each j, by the Chinese Remainder Theorem we get the result since $n = 3l$. From here we deduce the upper bound for $E_R(n)$ and, hence, the upper bound for $D_R(n)$ follows from the inequality $n - 1 + D_R(n) \leq E_R(n)$. □

Proof of Theorem 4. (i) It is interesting to observe that in the case when $n = 3p$, for $p \geq 7$ prime, we again reach the identity of Theorem 2, $D_R(n) = 2r + 1 = 5$. Indeed, given a sequence $\{x_1, \ldots, x_5\}$, (in all the arguments we will assume that none of these elements is zero modulo $3p$), with at most two units modulo p, or at most two units modulo 3, then removing those elements, the result is true since $D_R(q) = 3$ for any prime q. Now suppose the sequence has at least three units modulo p and three units modulo 3. The interesting case is when the sequence has precisely three units modulo p. So suppose $p|(x_4, x_5)$, and hence, are coprime with 3. If $x_4 \equiv -x_5 \pmod 3$ then $x_4 + x_5 = 0 \pmod{3p}$. Otherwise, since there are at least three units modulo 3, we can assume that $(x_3, 3p) = 1$. Then, for some $\{b_4, b_5\} \subseteq \{0, 1\}$ we have $x_1 + x_2 + x_3 \equiv -(b_4 x_4 + b_5 x_5) \pmod 3$. We fix those b_i. On the other hand, there exist squares $a_i \in (\mathbb{Z}/p\mathbb{Z})^*$ for $i = 1, 2, 3$, such that $\sum_{i=1}^{3} a_i x_i \equiv -(b_4 x_4 + b_5 x_5) \equiv 0 \pmod p$. We just have to apply the Chinese Remainder Theorem to get the result.

When the sequence has five units modulo p, the result is trivial by Lemma 9, since by the Erdős-Ginzburg-Ziv Theorem, the sum of three of them will be a multiple of 3. If the sequence has exactly four units modulo p then suppose $p|x_5$ and $3 \nmid x_4 x_5$. Then, as before, we will choose $\{b_4, b_5\} \subseteq \{0, 1\}$ so that $\sum_{i=1}^{3} a_i x_i \equiv -(b_4 x_4 + b_5 x_5) \equiv 0 \pmod{3p}$. In this way we get $D_R(3p) \leq 5$, and we get the identity by Theorem 1. (It is important to note that Theorem A does not apply because the only square modulo 3 is 1, so $a^2 - b^2$ will always be a multiple of 3.)

(ii) To get the lower bound $D_R(15) \geq 6$, we observe that the sequence obtained by repeating 1 five times does not contain any subsequence whose sum is zero with coefficients squares of units modulo 15. We just have to note that such a subsequence, to be a multiple of 3, would have exactly three elements. On the other hand, we can assume the squares modulo 5 to be ± 1. Then, the sum of any three elements would be $-3 \leq \sum a_i \leq 3$, and the only way to be a multiple of 5 is that it is 0, which needs an even number of ± 1.

In order to get the upper bound, let $x_1, \ldots, x_6$ be elements modulo 15. We assume that none is zero. If at least three are zero modulo 5, let them be x_1, x_2, x_3. Now, some non-empty subsum of them is zero modulo 3 (since the classical Davenport constant $D(\mathbb{Z}/3\mathbb{Z}) = 3$). From now on, we assume that at least four of them are non-zero modulo 5.

Let us assume that the elements x_1, x_2, x_3, x_4 are non-zero modulo 5. If there is $I \subseteq \{5, 6\}$ (I can be empty), such that $\sum_{i \in J} x_i \equiv 0 \pmod 3$, where $J = \{1, \ldots, 4\} \cup I$, then we are through by Lemma 10.

So, assume that there is no such I. In particular, $\sum_{i=1}^{4} x_i \not\equiv 0 \pmod 3$. We may then assume, without loss of generality (considering the sequence $-x_1, \ldots, -x_6$, if necessary), that

$$\sum_{i=1}^{4} x_i \equiv 1 \pmod 3.$$

By our assumption, neither of x_5 and x_6 can be -1 modulo 3. Also, both of them can not be 1 modulo 3. Therefore, one of them, say x_6, is 0 modulo 3. Then x_6 is non-zero modulo 5. If one among the elements $x_1, \ldots, x_4$ is 1 modulo 3, we replace it by x_6 and we are through by Lemma 10. If none of them is 1 modulo 3, the only possibility is that two of them are -1 modulo 3 and the other two are 0 modulo 3. We replace the pair of elements -1 modulo 3 by x_6. Since we have three elements each of which is 0 modulo 3, some of them will sum up to 0 modulo 5, since $D_R(5) = 3$. □

Proofs of Theorems 5 and 6. The proof of Theorem 5 relies on the trivial observation that given any three integers, there is a subsequence of two elements which sums up to $0 \pmod 2$. Similarly, for the proof of Theorem 6, one has to observe that by the Erdős-Ginzburg-Ziv Theorem, given any eleven integers, there is a subsequence of six elements which sums up to $0 \pmod 6$. Then, one has to follow the arguments as in the proof of Theorem 3. □

Proof of Theorem 7. Observe that, by Theorem A, we just have to prove $D_R(n) = 2r + 1$ since $\{1, 4\} \subseteq R$. By Theorem 1, it remains to establish the upper bound $D_R(n) \leq 2r + 1$. Let $S = (x_1, \ldots, x_{2r+1})$ be a sequence of elements of $\mathbb{Z}/p^r\mathbb{Z}$. We note that three of the integers in S will be divisible by the same power of p. So, without loss of generality, we can suppose that $\{y_1, y_2, y_3\} \subseteq (\mathbb{Z}/p^r\mathbb{Z})^*$ where $y_i = x_i/p^\alpha$ for some $0 \leq \alpha \leq r - 1$. Then, by Theorem C we see that

$$|Ry_1 + Ry_2 \cup 0 + Ry_3 \cup 0| \geq min\{n, 3|R|\} = n,$$

since $|R| = \frac{n}{2}(1 - \frac{1}{p})$, and $\frac{3}{2}n(1 - \frac{1}{p}) > n$ for any $p > 3$, and the result follows. Observe that $Ry \cup 0$ satisfies the conditions of Theorem C for any $y \in (\mathbb{Z}/p^r\mathbb{Z})^*$. This concludes the proof of the theorem. □

3. Other Weights

In this section we include some zero-sum results concerning different sets of weights. We start with the remark that Theorems 1, 2, 3, 4 and 7 remain true if we replace the set R_n by the set $S_n = \{a \in (\mathbb{Z}/n\mathbb{Z})^*, \left(\frac{a}{n}\right) = 1\}$, where $\left(\frac{a}{n}\right)$ is the Jacobi symbol. Indeed, R_n is a subset of S_n, which gives the upper bound. For the lower bound, we just have to use the similar counterexample as in the proof of Theorem 1, but with $v_i \notin S_{p_i}$ instead. On the other hand, it is interesting to observe that, $|S_n| = \varphi(n)/2$ whereas, in general, R_n gets much smaller when n is composite.

We now proceed to prove Theorem 8, where one considers a completely different set of weights.

Proof of Theorem 8. For the proof of the first part we use the argument in [6]. Given a sequence $S = (s_1, \ldots, s_{\lceil \frac{n}{r} \rceil})$ we consider the sequence

$$S' = (s_1, \ldots, s_1, s_2, \ldots, s_2, \ldots, s_{\lceil \frac{n}{r} \rceil}, \ldots, s_{\lceil \frac{n}{r} \rceil}),$$

where each element is repeated r times. Then $|S'| \geq n$, and noting that $D_{\{1\}}(n) \leq n$, we obtain

$$D_A(n) \leq \left\lceil \frac{n}{r} \right\rceil.$$

On the other hand, let us consider the sequence of $\lceil \frac{n}{r} \rceil - 1$ elements all equal to 1. Then, for any nonempty subsequence, $(s_{j_1}, \ldots, s_{j_l})$ and $a_i \in A$, $i = 1, \ldots, l$ we have

$$0 < \sum_{i=1}^{l} a_i s_{j_i} < rl \leq n - 1,$$

which gives us the lower bound,

$$D_A(n) \geq \left\lceil \frac{n}{r} \right\rceil,$$

and hence part (i) follows.

Since the Erdős-Ginzburg-Ziv Theorem takes care of the second part of the theorem for the case $r = 1$, we can assume that $r > 1$. Now, noting that $\{1, 2\} \subseteq A$, part (ii) is a consequence of Theorem A. □

Acknowledgment. This work was done while the first and the last authors were visiting the Centre de Recherches Mathématiques (CRM) in Montreal, and they wish to thank this institute for its hospitality. We would like to thank the referee for a very careful reading of the earlier manuscript and giving numerous suggestions to improve the presentation and also for providing the proof of the upper bound (the proof given here is slightly modified) of part (ii) of Theorem 4.

References

[1] Sukumar Das Adhikari, *Aspects of combinatorics and combinatorial number theory*, Narosa Publishing House, New Delhi, 2002.

[2] S. D. Adhikari, R. Balasubramanian and P. Rath, *Some combinatorial group invariants and their generalizations with weights*, Additive combinatorics, (Eds. Granville, Nathanson, Solymosi), 327–335, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007.

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

[4] 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).

[5] S. D. Adhikari, Y. G. Chen, J. B. Friedlander, S. V. Konyagin and F. Pappalardi, *Contributions to zero-sum problems*, Discrete Math. 306, no. 1, 1-10 (2006).

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

[7] A. L. Cauchy, *Recherches sur les nombres*, J. Ecôle Polytech. 9, 99–123 (1813).

[8] Chowla, *A theorem on the addition of residue classes: Application to the number F(k) in Waring's problem*, Proc. Indian Acad. Sci. 2, 242-243 (1935).

[9] H. Davenport, *On the addition of residue classes*, J. London Math. Soc. 22, 100–101 (1947).

[10] P. Erdős, A. Ginzburg, A. Ziv, *Theorem in the additive number theory*, Bull. Res. Council Israel 10 (F) 41-43 (1961).

[11] W. D. Gao, *A combinatorial problem on finite abelian groups*, J. Number Theory 58 , no. 1, 100-103 (1996).

[12] Simon Griffiths, *The Erdős-Ginzburg-Ziv theorem with units*, Discrete Math. 308, no. 23, 5473-5484 (2008).

[13] Florian Luca, *A generalization of a classical zero-sum problem*, Discrete Math. 307, no. 13, 1672-1678 (2007).

[14] Melvyn B. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics, 165. Springer-Verlag, New York, 1996.

[15] R. Thangadurai, *A variant of Davenport's constant*, Proc. Indian Acad. Sci. Math. Sci. 117 no. 2, 147–158 (2007).