DAVENPORT CONSTANT WITH WEIGHTS AND SOME RELATED QUESTIONS

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

Purusottam Rath
Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211 019, INDIA
rath@mri.ernet.in

Received: 5/22/06, Revised: 7/5/06, Accepted: 8/12/06, Published: 10/20/06

Abstract

Let $n \in \mathbb{N}$ and let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be such that A does not contain 0 and it is non–empty. Generalizing a well known constant, $E_A(n)$ is defined to be the least $t \in \mathbb{N}$ such that for all sequences $(x_1, \ldots, x_t) \in \mathbb{Z}^t$, there exist indices $j_1, \ldots, j_n \in \mathbb{N}, 1 \leq j_1 < \cdots < j_n \leq t$, and $(\vartheta_1, \cdots, \vartheta_n) \in A^n$ with $\sum_{i=1}^{n} \vartheta_i x_{j_i} \equiv 0 \pmod{n}$. Similarly, for any such set A, we define the Davenport Constant of $\mathbb{Z}/n\mathbb{Z}$ with weight A denoted by $D_A(n)$ to be the least natural number k such that for any sequence $(x_1, \cdots, x_k) \in \mathbb{Z}^k$, there exists a non-empty subsequence $\{x_{j_1}, \cdots, x_{j_l}\}$ and $(a_1, \cdots a_l) \in A^l$ such that $\sum_{i=1}^{l} a_i x_{j_i} \equiv 0 \pmod{n}$. In the present paper, in the special case where $n = p$ is a prime, we determine the values of $D_A(p)$ and $E_A(p)$ where A is $\{1, 2, \cdots, r\}$ or the set of quadratic residues $\pmod{p}$.

1. Introduction

Here we shall be concerned with certain generalizations of two important combinatorial invariants related to zero-sum problems (for detailed accounts one may see [10], [3], [13], [9]) in finite abelian groups.

For an abelian group G, the Davenport constant $D(G)$ is defined to be the smallest natural number k such that any sequence of k elements in G has a non-empty subsequence whose sum is zero (the identity element). For an abelian group G of cardinality n, another interesting constant is the smallest natural number k such that any sequence of k elements in G has a subsequence of length n whose sum is zero; we shall denote it by $E(G)$.

The following result due to Gao [8] (see also [10], Proposition 5.7.9) connects these two invariants.

Theorem 1. *If G is a finite abelian group of order n, then $E(G) = D(G) + n - 1$.*

For the particular group $\mathbb{Z}/n\mathbb{Z}$, the following generalization of $E(G)$ was considered in [2] recently. Let $n \in \mathbb{N}$ and assume $A \subseteq \mathbb{Z}/n\mathbb{Z}$. Then $E_A(n)$ is the least $t \in \mathbb{N}$ such that for all sequences $(x_1, \ldots, x_t) \in \mathbb{Z}^t$ there exist indices $j_1, \ldots, j_n \in \mathbb{N}, 1 \le j_1 < \cdots < j_n \le t$, and $(\vartheta_1, \cdots, \vartheta_n) \in A^n$ with

$$\sum_{i=1}^{n} \vartheta_i x_{j_i} \equiv 0 \pmod{n}.$$

To avoid trivial cases, one assumes that the weight set A does not contain 0 and it is non–empty.

Similarly, for any such set $A \subset \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ of weights, we define the Davenport Constant of $\mathbb{Z}/n\mathbb{Z}$ with weight A denoted by $D_A(n)$ to be the least natural number k such that for any sequence $(x_1, \cdots, x_k) \in \mathbb{Z}^k$, there exists a non-empty subsequence $\{x_{j_1}, \cdots, x_{j_l}\}$ and $(a_1, \cdots a_l) \in A^l$ such that

$$\sum_{i=1}^{l} a_i x_{j_i} \equiv 0 \pmod{n}.$$

Thus, for the group $G = \mathbb{Z}/n\mathbb{Z}$, if we take $A = \{1\}$, then $E_A(n)$ and $D_A(n)$ are respectively $E(G)$ and $D(G)$ as defined earlier.

For several sets $A \subset \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ of weights, exact values of $E_A(n)$ and $D_A(n)$ have been determined: The case $A = \{1\}$ is classical and is covered by the well-known theorem (EGZ theorem) due to Erdős, Ginzburg and Ziv [6] (one may also see [11] or [10]) and Theorem 1 is also applicable; the case $A = \{1, -1\}$, was done in [2] where it is shown that $E_A(n) = n + [\log_2 n]$. Furthermore, by the pigeonhole principle (see [2]), $D_A(n) \le [\log_2 n] + 1$, and by considering the sequence $(1, 2, \ldots, 2^r)$, where r is defined by $2^{r+1} \le n < 2^{r+2}$, it follows that $D_A(n) \ge [\log_2 n] + 1$; the case observed in [2] shows that for $A = \{1, 2 \cdots n-1\}$ we have $E_A(n) = n + 1$. In this case, it is easy to see that $D_A(n) = 2$; lastly, settling a conjecture from [2], it was proved in [7] that for $A = (\mathbb{Z}/n\mathbb{Z})^* = \{a : (a, n) = 1\}$, $E_A(n) = n + \Omega(n)$, where $\Omega(n)$ denotes the number of prime factors of n, multiplicity included.

It is not difficult to observe that

$$E_A(n) \ge D_A(n) + n - 1 \text{ for any } A \subset \mathbb{Z}/n\mathbb{Z} \setminus \{0\}. \tag{1}$$

Taking $A = (\mathbb{Z}/n\mathbb{Z})^*$, it follows from (1) and the above result that $D_A(n) \le 1 + \Omega(n)$. On the other hand, in this case, writing $n = p_1 \cdots p_s$ as a product of $s = \Omega(n)$ (not necessarily distinct) primes, the sequence $(1, p_1, p_1p_2, \ldots, p_1p_2 \cdots p_{s-1})$ gives the lower bound $D_A(n) \ge 1 + \Omega(n)$.

Thus, in all these above cases, namely when A is one of the sets appearing in the chain $\{1\} \subset \{1, -1\} \subset (\mathbb{Z}/n\mathbb{Z})^* \subset \{1, 2, \cdots, n-1\}$, one has $E_A(n) = D_A(n) + n - 1$.

In the present paper, in the special case where $n = p$ is a prime (other than 2, the trivial case), we determine the values of $D_A(p)$ and $E_A(p)$ where A is $\{1, 2, \cdots, r\}$ or the set of quadratic residues $\pmod p$. In both cases, the equality $E_A(p) = D_A(p) + p - 1$ holds.

Perhaps one would expect that for any set $A \subset \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ of weights, the equality $E_A(n) = D_A(n) + n - 1$ holds.

2. $D_A(p)$ and $E_A(p)$ for certain subsets A of $(\mathbb{Z}/p\mathbb{Z})^*$

In what follows, p will always denote an odd prime.

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

(i) $D_A(p) = \lceil \frac{p}{r} \rceil$, where for a real number x, $\lceil x \rceil$ denotes the smallest integer $\geq x$,

(ii) $E_A(p) = p - 1 + D_A(p)$.

Proof. Consider any sequence $S = (s_1, \cdots, s_{\lceil \frac{p}{r} \rceil})$ of elements of $\mathbb{Z}/p\mathbb{Z}$ of length $\lceil \frac{p}{r} \rceil$. Considering the sequence

$$S' = (\overbrace{s_1, s_1, \cdots, s_1}^{r \text{ times}}, \overbrace{s_2, s_2, \cdots, s_2}^{r \text{ times}}, \cdots, \overbrace{s_{\lceil \frac{p}{r} \rceil}, \cdots, s_{\lceil \frac{p}{r} \rceil}}^{r \text{ times}}),$$

obtained from S by repeating each element r times, and observing that the length of this sequence is $\geq p$, it follows that

$$D_A(p) \leq \left\lceil \frac{p}{r} \right\rceil. \tag{2}$$

On the other hand, considering the sequence $(\overbrace{1, 1, \cdots, 1}^{(\lceil \frac{p}{r} \rceil - 1) \text{ times}})$, for any non-empty subsequence $(s_{j_1}, \cdots, s_{j_l})$ of this sequence and $(a_1, \cdots a_l) \in A^l$,

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

Therefore,

$$D_A(p) \geq \left\lceil \frac{p}{r} \right\rceil. \tag{3}$$

From equations (2) and (3), part (i) follows.

Now, consider any sequence $S = (s_1, \cdots, s_N)$ of elements of $\mathbb{Z}/p\mathbb{Z}$ of length

$$N = p - 1 + \left\lceil \frac{p}{r} \right\rceil .$$

Case I. (The sequence S has at least p non-zero elements in it).

Let $(s_{i_1}, s_{i_2}, \cdots, s_{i_p})$ be a subsequence of S of p non-zero elements and let $A_k = \{s_{i_k}, 2s_{i_k}\}$ for $k = 1, \cdots, p$. Since $|A_k| = 2$ for all k, by the Cauchy-Davenport Theorem (see [11], Theorem 2.3) it follows that $|A_1 + A_2 + \cdots + A_p| \geq p$ and hence

$$\sum_{k=1}^{p} a_k s_{i_k} = 0, \text{ where } a_k \in \{1, 2\} \subset A.$$

Case II. (The sequence S has less than p non-zero elements in it).

In this case, at least $\lceil \frac{p}{r} \rceil$ elements of the sequence are equal to zero. We reorder the sequence in such a way that $s_1 = s_2 = \cdots = s_t = 0$ and the remaining elements are non-zero. We have $N - t < p$. Let $B = \{r_1, \ldots, r_l\} \subseteq \{t + 1, t + 2, \cdots, N\}$ be maximal with respect to the property that there exist $a_1, \cdots, a_l \in \{1, 2, \cdots, r\}$ with

$$\sum_{j=1}^{l} a_j s_{r_j} = 0.$$

Now we claim that $l + t \geq p$. Indeed, if this were not the case then the set $C = \{t + 1, \cdots, N\} \setminus \{r_1, \cdots, r_l\}$ would contain $N - t - l \geq \lceil \frac{p}{r} \rceil$ elements. Hence by part (i), there would exist a non–empty $B' \subset C$ and $a_j \in \{1, 2, \cdots, r\}$ for each $j \in B'$ such that

$$\sum_{j \in B'} a_j s_j = 0.$$

Now, $B \cup B'$ would contradict the maximality of B. Hence $l + t \geq p$. Therefore, appending the sequence B to $(s_1, s_2, \cdots, s_{p-l}) = (0, 0, \cdots, 0)$, we get a sequence of length p with desired property.

From Cases (I) and (II), and part (i), $E_A(p) \leq p - 1 + \lceil \frac{p}{r} \rceil = p - 1 + D_A(p)$, and hence from equation (1), part (ii) follows.

Theorem 3. *Let A be the set of quadratic residues* (mod p). *That is, A consists of all the squares in $(\mathbb{Z}/p\mathbb{Z})^*$. We have*

(i) $D_A(p) = 3,$

(ii) $E_A(p) = p + 2.$

Proof. Given any sequence $S = (s_1, \cdots, s_{p+2})$ of elements of $\mathbb{Z}/p\mathbb{Z}$ of length $p+2$, we consider the following system of equations in $(p+2)$ variables over the finite field $\mathbb{F}_p$:

$$\sum_{i=1}^{p+2} s_i x_i^2 = 0, \quad \sum_{i=1}^{p+2} x_i^{p-1} = 0.$$

By Chevalley - Warning Theorem (see [12] or [1], for instance), there is a nontrivial solution $(y_1, \cdots, y_{p+2})$ of the above system. Writing $I = \{i : y_i \neq 0\}$, from the first equation it follows that $\sum_{i \in I} a_i s_i = 0$ where a_i's belong to the set of squares in $(\mathbb{Z}/p\mathbb{Z})^*$. By Fermat's little theorem, from the second equation we have $|I| = p$. Hence

$$E_A(p) \leq p + 2. \tag{4}$$

From (1), we have $E_A(p) \geq D_A(p) + p - 1$, and hence by (4),

$$D_A(p) \leq E_A(p) - p + 1 \leq 3. \tag{5}$$

On the other hand, considering a sequence $v_1, -v_2$, where v_1 is a quadratic residue and v_2 a quadratic non-residue $\pmod p$, for two elements $a_1, a_2 \in A$, $a_1 v_1 + a_2(-v_2) = 0$ implies $a_1 v_1 = a_2 v_2$, – an absurdity, since $a_1 v_1$ is a quadratic residue and $a_2 v_2$ a non-residue.

Therefore, $D_A(p) \geq 3$ and this together with (5) proves part (i) of the theorem.

Again, since $E_A(p) \geq D_A(p) + p - 1$, by part (i), $E_A(p) \geq p + 2$, which, together with (4) gives part (ii) of the theorem.

Remarks. First, we note that the values of $D_A(p)$ and $E_A(p)$ remain unchanged if one replaces A by $cA = \{ca | a \in A\}$ for any $c \in (\mathbb{Z}/p\mathbb{Z})^*$. Hence, in particular, the statement of Theorem 3 holds with A as the set of quadratic non-residues $\pmod p$.

Finally, in Theorem 2, if $A \subset \{1, 2, \cdots, r\}$, where r is an integer such that $1 < r < p$, then also the lower bound (3) for $D_A(p)$ (and hence a corresponding lower bound for $E_A(p)$, namely $E_A(p) \geq p - 1 + \lceil \frac{p}{r} \rceil$, obtained by (1)) holds. However, taking $A = \{1, p-1\}$, for instance, this may not be a good lower bound in general. It is interesting to note the difference in the values of the constant $D_A(p)$ (from Theorem 2 and the result in [2] quoted in the introduction) corresponding to the weight sets $\{1, 2\}$ and $\{1, -1\}$ having the same cardinality.

Acknowledgement. We thank the referee whose suggestions helped us improve the presentation of the paper.

References

[1] S. D. Adhikari, *Aspects of combinatorics and combinatorial number theory*, Narosa, New Delhi, 2002.

[2] 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).

[3] Y. Caro, *Zero-sum problems – A survey*, Discrete Math. **152**, 93–113 (1996).

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

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

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

[7] Florian Luca, *A generalization of a classical zero-sum problem*, Preprint.

[8] W. D. Gao, *A combinatorial problem on finite abelian groups*, J. Number Theory, **58**, 100–103 (1996).

[9] W. D. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: A survey*, to appear.

[10] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations*, Chapman & Hall, CRC (2006).

[11] Melvyn B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.

[12] J. -P. Serre, *A course in Arithmetic*, Springer, 1973.

[13] R. Thangadurai, *Interplay between four conjectures on certain zero-sum problems*, Expo. Math. **20**, no. 3, 215–228 (2002).