Sets with small differences and big sums in finite groups

Rafał ZDUŃCZYK

Abstract. We are looking for subsets of additive groups of residues modulo $p \in \mathbb{N}$ such that the cardinality of algebraic sum modulo p of the set with itself exceeds the cardinality of the corresponding difference. Several questions, like how big the gap between those cardinalities may be, are considered.

Keywords: MSTD (More Sums Than Differences), sumset, difference set, modular arithmetic, computer aided search.

2010 Mathematics Subject Classification: 11P83, 11E57, 11B13.

1. Preliminaries

In 1972 authors of [2] considered subsets of additive groups of integers modulo p for which the sums are smaller than the differences and cited various contexts in which the problem of finding such sets had been evoken. Since then several papers in that spirit have appeared. Here we respond to the need of solving the opposite problem, i.e. finding sets with sums bigger in cardinality than the corresponding differences. Cf. [1] for applications and more bibliographical references.

Let for $A, B \subset \mathbb{R}$, $A \pm B := \{x \pm y : x \in A, y \in B\}$. For any set A, its cardinality will be denoted by $\# A$. To avoid ambiguity, agree that the ellipsis '$\dots$' in $m, \dots, n$, abbreviates an arithmetic progression of length $n - m + 1$ with first term m and common difference equal to 1. By $[a, b]$ we will denote closed interval both on the real line and restricted to integers. We make no distinction in notation, which we hope to be clear from the context. Furthermore, for a 'punched' interval, we will write $[\![\overrightarrow{m, n}]\!] := \left\{m + 2j : j = 0, \dots, \left\lfloor \frac{n-m}{2} \right\rfloor\right\}$. Let $\mathbb{Z}_p := \{0, \dots, p-1\}$, where $p \in \mathbb{N}$, $p \geqslant 2$. We are interested in subsets of $\mathbb{Z}_p$ for which the inequality

R. Zduńczyk
Faculty of Mathematics and Computer Science, University of Łódź, 22 Banacha str., 90-238 Łódź, Poland, e-mail: rafal@math.uni.lodz.pl

R. Wituła, B. Bajorska-Harapińska, E. Hetmaniok, D. Słota, T. Trawiński (eds.), *Selected Problems on Experimental Mathematics*. Wydawnictwo Politechniki Śląskiej, Gliwice 2017, pp. 149–166.

$$\#((A+A) \bmod p) > \#((A-A) \bmod p) \tag{1}$$

holds. Although it is an easy check that for small p, say $p \leqslant 7$, such sets do not exist, the computational complexity of the problem increases exponentially with p. The Matlab solution used for the purpose of the hereby publication is presented and explained in Appendix. By searching over all subsets of $\mathbb{Z}_p$ one can find that for $p \in \{1, \ldots, 11\} \cup \{13\}$ there are no such sets. Surprisingly they appear at $p = 12$.

Fact 1.1. *For any set A of the following form*

$$\begin{array}{ccc}
\{0,1,3,4,5,8\}, & \{0,1,2,5,9,10\}, & \{0,1,4,8,9,11\}, \\
\{0,3,4,5,7,8\}, & \{2,5,6,7,9,10\}, & \{0,4,7,8,9,11\}, \\
\{0,1,2,4,5,9\}, & \{0,1,5,8,9,10\}, & \{1,2,3,6,10,11\}, \\
\{1,2,4,5,6,9\}, & \{1,5,6,8,9,10\}, & \{0,2,3,7,10,11\}, \\
\{1,4,5,6,8,9\}, & \{0,2,3,4,7,11\}, & \{0,3,7,8,10,11\}, \\
\{0,4,5,7,8,9\}, & \{2,3,4,6,7,11\}, & \{3,6,7,8,10,11\}, \\
\{1,2,3,5,6,10\}, & \{0,1,3,4,8,11\}, & \{1,2,6,9,10,11\}, \\
\{2,3,5,6,7,10\}, & \{3,4,6,7,8,11\}, & \{2,6,7,9,10,11\},
\end{array}$$

we have:

$$(A+A) \bmod 12 = \mathbb{Z}_{12}, \qquad (A-A) \bmod 12 = \mathbb{Z}_{12} \backslash \{6\},$$

and each set from the list can be described in terms of any other as $(\pm A + k) \bmod p$, where $k \in \mathbb{Z}$. Moreover, the list is complete—no other set satisfies (1) in $\mathbb{Z}_{12}$.

The following general observation needs no proof.

Property 1.2. *If $B = (\pm A + k) \bmod p$, $A \subset \mathbb{Z}_p$, $k \in \mathbb{Z}$, then*

$$\#((B+B) \bmod p) = \#((A+A) \bmod p), \qquad \#((B-B) \bmod p) = \#((A-A) \bmod p).$$

Similarly, it can be easily seen that the structure of sets satisfying (1) is restricted, no such set, nor its shift, can be symmetric. For if $A = B + k$, $B = -B$, then

$$A + A = B + k + B + k = B + k - (B + k) + 2k = A - A + 2k$$

and so A does not satisfy (1). Nevertheless, as it will be shown in Fact 2.2, a set satisfying (1) can be its own non-trivial shift.

We define an equivalence relation in $\mathbb{Z}_p$ by saying that

$$A \sim B \qquad \text{when} \qquad B = (\pm A + k) \bmod p, \qquad \text{for some } k \in \mathbb{Z},$$

The equivalence classes of the relation will be referred to as orbits. For $A \in \mathbb{Z}_p$ its orbit will be denoted by $\operatorname{orb} A$. Thus, by finding a set with property (1) we get for free $2p$ such sets—as we will see—not necessarily distinct, yet sharing some properties, including the cardinality and structure. Let for $p, k \in \mathbb{N}$, $D_p(k)$ denote the collection of subsets of $\mathbb{Z}_p$ such that

$$\#((A+A) \bmod p) - \#((A-A) \bmod p) = k,$$

and $d_p(k)$ the collection of the corresponding orbits. Finally, let $D_p := \bigcup_{k>0} D_p(k)$ and $d_p = \bigcup_{k>0} d_p(k)$. By Fact 1.1 we see that

- $\# D_{12}(1) = 24$, $\# d_{12}(1) = 1$,
- $(A+A) \bmod 12 = \mathbb{Z}_{12}$ for each $A \in D_{12}$,
- $D_{12}(k) = \varnothing$, for $k > 1$,
- $\# A = 6$ for each $A \in D_{12}$.

Hence natural questions rise.

Question 1.3. *Is it possible that $\# D_p(k) \neq 2p \cdot \# d_p(k)$? How are these numbers related to p?*

Question 1.4. *Is it possible that $(A+A) \bmod p \neq \mathbb{Z}_p$ for $A \in D_p$?*

Question 1.5. *For which p would $D_p(k)$ be non-empty for $k > 1$?*

Question 1.6. *How can sizes of sets in $D_p(k)$ vary?*

Here is a sample of what computer aided calculations reveal.

Fact 1.7. *$\# D_{14} = 28$, $D_{14} = D_{14}(1)$, $\# d_{14}(1) = 1$ and for each $A \in D_{14}$ one has $(A+A) \bmod 14 = \mathbb{Z}_{14}$, $(A-A) \bmod 14 = \mathbb{Z}_{14} \backslash \{7\}$. The complete list of D_{14} follows:*

$$\begin{array}{cccc}
\{0,1,3,4,5,6,9\}, & \{0,5,6,8,9,10,11\}, & \{0,2,3,4,5,8,13\}, & \{0,1,3,4,9,12,13\}, \\
\{0,3,4,5,6,8,9\}, & \{1,2,3,4,6,7,12\}, & \{2,3,4,5,7,8,13\}, & \{0,1,4,9,10,12,13\}, \\
\{1,2,4,5,6,7,10\}, & \{3,4,6,7,8,9,12\}, & \{0,1,2,4,5,10,13\}, & \{4,7,8,9,10,12,13\}, \\
\{1,4,5,6,7,9,10\}, & \{0,1,2,3,6,11,12\}, & \{4,5,7,8,9,10,13\}, & \{0,2,3,8,11,12,13\}, \\
\{0,1,2,3,5,6,11\}, & \{3,6,7,8,9,11,12\}, & \{0,1,2,5,10,11,13\}, & \{0,3,8,9,11,12,13\}, \\
\{2,3,5,6,7,8,11\}, & \{0,1,6,9,10,11,12\}, & \{0,5,8,9,10,11,13\}, & \{1,2,7,10,11,12,13\}, \\
\{2,5,6,7,8,10,11\}, & \{1,6,7,9,10,11,12\}, & \{1,2,3,4,7,12,13\}, & \{2,7,8,10,11,12,13\}.
\end{array}$$

2. Surviving patterns

The similarities of structures between sets from D_{14} and from D_{12} suggest the existence of certain patterns preserved with increasing p, at least for even p. Indeed, we have

Fact 2.1. *Let $p = 2n$, $n \geqslant 6$. The conditions*

$$A + A = \mathbb{Z}_p, \qquad A - A = \mathbb{Z}_p \backslash \{\tfrac{p}{2}\}, \tag{2}$$

hold for each of the following sets (the order of which mocks that from Fact 1.1)

$$\{0,1\} \cup [3, n-1] \cup \{n+2\}, \tag{3}$$
$$\{0\} \cup [3, n-1] \cup \{n+1, n+2\},$$
$$[0, n-4] \cup \{n-2, n-1, 2n-3\},$$
$$\left.\begin{array}{l}\{n-5, n-4\} \cup [n-2, 2n-6] \cup \{2n-3\},\\ \{1,2\} \cup [4, n] \cup \{n+3\},\end{array}\right\} \tag{4}$$
$$\left.\begin{array}{l}\{n-5\} \cup [n-2, 2n-6] \cup \{2n-4, 2n-3\},\\ \{1\} \cup [4, n] \cup \{n+2, n+3\},\end{array}\right\} \tag{5}$$
$$\{0, n-2, n-1\} \cup [n+1, 2n-3],$$
$$[1, n-3] \cup \{n-1, n, 2n-2\},$$
$$\{n-4, n-3\} \cup [n-1, 2n-5] \cup \{2n-2\},$$
$$[0, n-4] \cup \{n-1, 2n-3, 2n-2\},$$
$$\{n-4\} \cup [n-1, 2n-5] \cup \{2n-3, 2n-2\},$$
$$\{0, 1, n-1\} \cup [n+2, 2n-2],$$
$$\{1, n-1, n\} \cup [n+2, 2n-2],$$
$$\{0\} \cup [2, n-2] \cup \{n+1, 2n-1\},$$
$$[2, n-2] \cup \{n, n+1, 2n-1\},$$
$$[0, n-5] \cup \{n-3, n-2, 2n-4, 2n-1\},$$
$$\{n-3, n-2\} \cup [n, 2n-4] \cup \{2n-1\},$$
$$\left.\begin{array}{l}\left[0, \left\lceil \frac{n}{2} \right\rceil - 2\right] \cup \{n-2\} \cup \left[n + \left\lceil \frac{n}{2} \right\rceil - 1, 2n-3\right] \cup \{2n-1\},\\ [1, n-3] \cup \{n, 2n-2, 2n-1\},\end{array}\right\} \tag{6}$$
$$\left.\begin{array}{l}\{0, n-2\} \cup [n+1, 2n-3] \cup \{2n-1\},\\ \{0, 1, 3, 4, n+2\} \cup [n+5, 2n-1],\end{array}\right\} \tag{7}$$
$$\left.\begin{array}{ll}\{1, 2, 3, n\} \cup [n+4, 2n-1], & n \neq 7,\\ \{0, 1, 4, n+2, n+3\} \cup [n+5, 2n-1], & \end{array}\right\} \tag{8}$$
$$\{0, 2, 3, n+1\} \cup [n+4, 2n-1],$$
$$\{0, 3, n+1, n+2\} \cup [n+4, 2n-1],$$
$$\{n-3\} \cup [n, 2n-4] \cup \{2n-2, 2n-1\},$$
$$\{1, 2, n\} \cup [n+3, 2n-1],$$
$$\{2, n, n+1\} \cup [n+3, 2n-1].$$

Note that however for $p = 2n = 12$ the sets (4)–(8) mutually coincide, for $n > 6$ they differ. Assertion (2) for each of the mentioned sets can be easily verified by a direct computation. We will show it for set (3), leaving the remaining proofs to the reader. We have

$$\begin{aligned}&\big((\{0,1\}\cup[3,n-1]\cup\{n+2\})+\\&+(\{0,1\}\cup[3,n-1]\cup\{n+2\})\big) \bmod 2n=\\&=\{0,1,2\}\cup[3,n]\cup\{n+2,n+3\}\cup[6,2n-2]\cup[n+5,2n+1] \bmod 2n=\mathbb{Z}_{2n},\end{aligned}$$

provided that $n \geqslant 5$ (so that one can glue together $[3,n]$ and $[6,2n-2]$) and $2n+2 \geqslant n+4$, which means $n \geqslant 6$ (in order to glue together $[6,2n-2]$ and $[n+5,2n+1]$). Now, for the difference, we have

$$\begin{aligned}&\big((\{0,1\}\cup[3,n-1]\cup\{n+2\})+\\&-(\{0,1\}\cup[3,n-1]\cup\{n+2\})\big) \bmod 2n=\\&=([2-n,n-2]\cup[3,n-1]\cup[1-n,-3]) \bmod 2n=\mathbb{Z}_{2n}\backslash\{n\}.\end{aligned}$$

The cardinalities of the considered classes of sets are listed below. Even and odd p are listed separately.

$p=2n$	$\# D_p$	$\# d_p$	$\# D_p(2)$	$\# d_p(2)$	$\# D_p(3)$	$\# d_p(3)$
$\leqslant 10$	0	0	0	0	0	0
12	24	1	0	0	0	0
14	28	1	0	0	0	0
16	384	12	0	0	0	0
18	792	22	0	0	0	0
20	5440	136	80	2	0	0
22	15224	346	660	15	0	0
24	70632	1472	1176	25	0	0
26	218192	4196	9360	180	0	0
28	922348	16471	38780	693	336	6
30	2669760	44497	127320	2123	2220	37

$p=2n+1$	$\# D_p$	$\# d_p$	$\# D_p(2)$	$\# d_p(2)$	$\# D_p(3)$	$\# d_p(3)$
$\leqslant 13$	0	0	0	0	0	0
15	60	2	0	0	0	0
17	272	8	0	0	0	0
19	1026	27	0	0	0	0
21	4746	113	630	15	0	0
23	15686	341	1012	22	0	0
25	56000	1120	7500	150	0	0
27	184194	3411	25272	468	0	0
29	656096	11312	103124	1778	0	0

Note that for $p=24$ and 28 the equality $\# D_p = 2p \cdot \# d_p$ fails. The culprit in $\mathbb{Z}_{24}$ is

$$\begin{aligned}A&=\{0,1,3,4,5,8,12,13,15,16,17,20\}=\\&=\{0,1,3,4,5,8\}\cup(12+\{0,1,3,4,5,8\})\in D_{24}(2)\end{aligned}$$

and its $\operatorname{orb} A$ with cardinality 24, unlike all the other orbits each consisting of 48 different sets. In $\mathbb{Z}_{28}$ the situation is similar. Indeed, we have

$$\# D_{24} = 70632 = 1471 \cdot 48 + 24 \qquad \text{and} \qquad \# D_{28} = 922348 = 16470 \cdot 56 + 28.$$

This should come as no surprise, in the light of the following observation.

Fact 2.2. *Let $A \in D_p$ for some $p \geqslant 12$ and*

$$B = \bigcup_{j=0}^{k-1} (A + jp), \qquad k > 1.$$

Then $B \in D_{kp}$ and $\# \operatorname{orb} B \leqslant 2p$.

Proof. That $\# \operatorname{orb} B \leqslant 2p$ is obvious, as $(B + jp) \bmod kp = B$. We have $A + A \subset \mathbb{Z}_{2p}$ and hence $A + A = A_1 \cup A_2$, where $A_1 \subset \mathbb{Z}_p$, $A_2 \subset \mathbb{Z}_p + p$. Since $A \subset \mathbb{Z}_p$, we have $A + jp \subset \mathbb{Z}_p + jp$ and so $B \subset \mathbb{Z}_{kp}$. Furthermore

$$\begin{aligned}
(B + B) \bmod kp &= \bigcup_{j=0}^{2(k-1)} (A + A + jp) \bmod kp = \\
&\overset{*}{=} \bigcup_{j=0}^{k-1} (A + A + jp) \bmod kp = \\
&= \bigcup_{j=0}^{k-1} ((A_1 \cup A_2) + jp) \bmod kp = \\
&= \bigcup_{j=0}^{k-1} ((A_1 + jp) \cup (A_2 + jp)) \bmod kp = \\
&= A_1 \cup \bigcup_{j=0}^{k-2} \Big((A_2 + jp) \cup (A_1 + (j+1)p) \Big) \cup \\
&\qquad \cup (A_2 + (k-1)p) \bmod kp = \\
&= A_1 \cup (A_2 - p) \cup \bigcup_{j=0}^{k-2} \Big((A_2 + jp) \cup (A_1 + (j+1)p) \Big) = \\
&= \bigcup_{j=0}^{k-1} ((A + A) \bmod p + jp),
\end{aligned}$$

the equality '$*$' being a consequence of $(A + A + (k+j)p) \bmod kp = A + A + jp$ for $j \in \mathbb{Z}$. Since $(A + A) \bmod p \subset \mathbb{Z}_p$,

$$\#((B + B) \bmod kp) = k\, \#((A + A) \bmod p).$$

Finally

$$B - B = \bigcup_{j=0}^{k-1} (jp + A - A),$$

hence $\#((B - B) \bmod kp) \leqslant k\, \#((A - A) \bmod p)$. $\square$

Thus, Question 1.3 can be answered as follows: $\# D_p$ can be smaller than $2p \cdot \# d_p$, since for large p there are sets in D_p with relatively small orbits.

Fact 2.3. *If $A \in D_p(k)$, and $m \in \mathbb{N}$, then $mA \in D_{mp}(mk)$.*

Proof. We have $m((A \pm A) \bmod p) = (m(A \pm A)) \bmod mp = (mA \pm mA) \bmod mp$. □

Example 2.4. For the set $A = \{0, 6, 8, 10, 14, 16\} = 2 \cdot \{0, 3, 4, 5, 7, 8\} \subset \mathbb{Z}_{24}$ we have

$$\#((A + A) \bmod 24) = 12 \qquad \text{and} \qquad \#((A - A) \bmod 24) = 10.$$

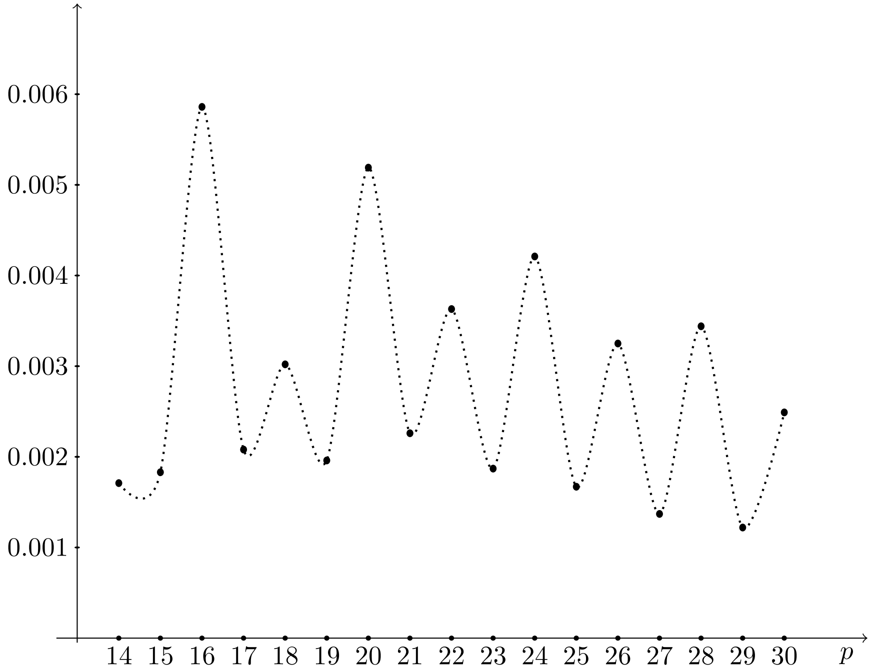

Fig. 1. $(\# D_p)/2^p$ against p

Figures 1 and 2 exhibit how $\# D_p$ is related to 2^p and to $\# D_{p-2}$, respectively. What can be observed is the cardinality of D_p stabilising in the interval $[0.001, 0.005]$ of the entire $\mathbb{Z}_p$ and the evident gap between p odd and even. In comparison of sizes of D_p and D_{p-2} repeating peaks are observed for multiples of 4.

3. Odd p

Fact 3.1. *By the symmetry of the difference* $\bmod p$*, no set in $D_{2n+1}(2m+1)$ can give* $(A + A) \bmod (2n+1) = \mathbb{Z}_{2n+1}$.

By this, Question 1.4 is answered affirmatively.

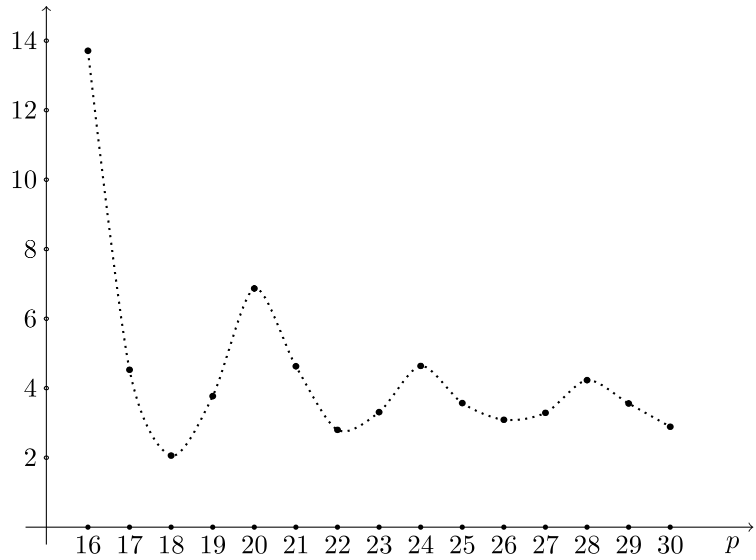

Fig. 2. $(\# D_p)/(\# D_{p-2})$ against p

Example 3.2. Let $B = \{0, 1, 3, 4, 5, 8\}$ and $C = \{0, 1, 2, 6, 8, 10\}$. We have

$$\begin{aligned} \operatorname{orb} B \cap \operatorname{orb} C &= \varnothing, \\ D_{15} = D_{15}(1) = \operatorname{orb} B &\cup \operatorname{orb} C, \end{aligned}$$

$$(B+B) \bmod 15 = \mathbb{Z}_{15} \backslash \{14\}, \quad (B-B) \bmod 15 = \mathbb{Z}_{15} \backslash \{6, 9\},$$
$$(C+C) \bmod 15 = \mathbb{Z}_{15} \backslash \{13\}, \quad (C-C) \bmod 15 = \mathbb{Z}_{15} \backslash \{3, 12\}.$$

Fact 3.3. *The sets B and C from the example above again fall into patterns which survive in D_p increasing $p = 2n+1$. Namely, for the following subsets of $\mathbb{Z}_{2n+1}$, $n > 6$,*

$$B := \{0, 1\} \cup [3, n-2] \cup \{n+1\}, \qquad C := \{0, 1, 2\} \cup [\![\overrightarrow{6, 2n-4}]\!],$$

one has

$$\begin{aligned} (B+B) \bmod (2n+1) &= \mathbb{Z}_{2n+1} \backslash \{2n\}, \\ (B-B) \bmod (2n+1) &= \mathbb{Z}_{2n+1} \backslash \{n-1, n+1\}, \\ (C+C) \bmod (2n+1) &= \mathbb{Z}_{2n+1} \backslash \{2n-1\}, \\ (C-C) \bmod (2n+1) &= \mathbb{Z}_{2n+1} \backslash \{3, 2n-2\}. \end{aligned}$$

By this and Fact 2.1 we have

Corollary 3.4. *There is a surviving pattern which works for both even and odd p, namely:*

$$\{0, 1\} \cup [3, n-1] \cup \{n+2\} \in D_{2n}(1) \cap D_{2n+3}(1).$$

Fact 3.5. *In $\mathbb{Z}_{17}$ we have $D_{17} = \bigcup_{j=1}^{8} \operatorname{orb} A_j$, where*

$$
\begin{aligned}
A_1 &= \{0,1,3,4,5,6,9\}, & A_5 &= \{0,3,4,5,7,8,12\},\\
A_2 &= \{0,1,4,5,6,7,11\}, & A_6 &= \{0,1,2,6,8,10,12\},\\
A_3 &= \{0,1,3,6,8,9,11\}, & A_7 &= \{0,1,4,5,8,11,12\},\\
A_4 &= \{0,1,2,4,8,10,11\}, & A_8 &= \{0,2,4,6,9,11,14\}.
\end{aligned}
$$

Note that A_1 and A_6 follow the pattern from Fact 3.3. Moreover, A_2 and A_8 can be described respectively as

$$
\begin{aligned}
D &= \{0,1\} \cup [4, n-1] \cup \{n+3\} \subset \mathbb{Z}_{2n+1},\\
F &= [\![\overrightarrow{0, 2n-10}]\!] \cup \{2n-7, 2n-5, 2n-2\} \subset \mathbb{Z}_{2n+1}, \qquad n \geqslant 8,
\end{aligned}
$$

for which

$$
\begin{aligned}
(D+D) \bmod (2n+1) &= \mathbb{Z}_{2n+1} \setminus \{3\}, & (D-D) \bmod (2n+1) &= \mathbb{Z}_{2n+1} \setminus \{n, n+1\},\\
(F+F) \bmod (2n+1) &= \mathbb{Z}_{2n+1} \setminus \{2n-7\}, & (F-F) \bmod (2n+1) &= \mathbb{Z}_{2n+1} \setminus \{1, 2n\}.
\end{aligned}
$$

Finally, A_5 and A_7 can be described respectively as

$$
\begin{aligned}
E &= \{0\} \cup \bigcup_{k=1}^{n-1} [4k-1, 4k+1] \cup \{4n-1, 4n, 4n+4\} \subset \mathbb{Z}_{8n+1}, \qquad n \geqslant 2,\\
G &= \bigcup_{k=0}^{n-3} \{4k, 4k+1\} \cup \{4n-8, 4n-5, 4n-4\} \subset \mathbb{Z}_{4n+1}, \qquad n \geqslant 4,
\end{aligned}
$$

for which

$$
\begin{aligned}
(E+E) \bmod (8n+1) &= \mathbb{Z}_{8n+1} \setminus \{1\},\\
(E-E) \bmod (8n+1) &= \mathbb{Z}_{8n+1} \setminus \{4n-2, 4n+3\},\\
(G+G) \bmod (4n+1) &= \mathbb{Z}_{4n+1} \setminus \{4n-2\},\\
(G-G) \bmod (4n+1) &\subset \mathbb{Z}_{4n+1} \setminus \{2, 4n-1\}.
\end{aligned}
$$

4. Increasing k in $D_p(k)$

Let us restate Question 1.5 as follows.

Question 4.1. *Given $k \in \mathbb{N}$ can one find $p_0 \in \mathbb{N}$ such that $D_p(k) \neq \varnothing$ for all $p \geqslant p_0$?*

So far we know that

Fact 4.2. *For each $k \geqslant 0$ and $n = 6 + 4k$ and the following set $A \subset \mathbb{Z}_{2n}$*

$$
A = \bigcup_{j=0}^{\frac{n}{4}-\frac{3}{2}} \{2+8j, 6+8j, 7+8j\} \cup [2n-3, 2n-1],
$$

the conditions

$$(A+A) \bmod 2n = \mathbb{Z}_{2n} \qquad \textit{and} \qquad (A-A) \bmod 2n = \mathbb{Z}_{2n} \setminus \bigcup_{j=0}^{\frac{n}{4}-\frac{3}{2}} \{6+8j\}$$

hold. In other words

$$\#((A-A) \bmod 2n) = 2n-k-1.$$

Hence we have

Corollary 4.3. *For $k > 0$, $d_{4+8k}(k) \neq \varnothing$.*

Fact 4.4. *For $n \geqslant 9k+1$ and the following $A \subset \mathbb{Z}_{2n+1}$*

$$A = \{4k\} \cup [n+k, n+3k] \cup [n+5k+1, 2n],$$

the conditions

$$(A+A) \bmod (2n+1) = \mathbb{Z}_{2n+1} \quad \textit{and} \quad ((A-A) \bmod (2n+1)) \cap [n-k+1, n+k] = \varnothing$$

hold. Furthermore, for $n \geqslant 9k-3$ and the following $A \subset \mathbb{Z}_{2n}$

$$A := \{4k-2\} \cup [n+k-1, n+3k-2] \cup [n+5k-2, 2n-1],$$

what follows holds.

$$(A+A) \bmod 2n = \mathbb{Z}_{2n} \qquad \textit{and} \qquad ((A-A) \bmod 2n) \cap [n-k+1, n+k-1] = \varnothing.$$

Corollary 4.5. *For each $k \in \mathbb{N}$ there is a p (namely: $p = 3+9k$) such that there exists an $A \subset \mathbb{Z}_p$ for which*

$$\#((A+A) \bmod p) = p \qquad \textit{and} \qquad ((A-A) \bmod p) \cap [a,b] = \varnothing,$$

where $\#[a,b] = k$ and $\frac{b+a}{2} = \frac{p}{2}$.

Question 4.6. *Are the numbers $8k$ and $9k$ (in $4+8k$ and $3+9k$, respectively) from the obove facts optimal?*

Question 4.7. *How does $D_p(m)$ behave between $4+8k$ and $4+8(k+1)$?*

Here is what we know about how the sizes of sets from each class may vary, cf. Question 1.6. In each case m_p stands for the minimum and M_p for the maximum of $\# A$, where $A \in D_p$, cf. list of orbit generators in the Appendix.

p	m_p	M_p	$m_p(2)$	$M_p(2)$	$m_p(3)$	$M_p(3)$
12	6	6	—	—	—	—
14	7	7	—	—	—	—
16	7	8	—	—	—	—
18	7	9	—	—	—	—
20	8	10	9	9	—	—
22	7	11	8	9	—	—
24	6	12	9	12	—	—
26	8	13	9	11	—	—
28	7	14	8	14	10	12
30	6	15	9	14	10	12

p	m_p	M_p	$m_p(2)$	$M_p(2)$	$m_p(3)$	$M_p(3)$
15	6	6	—	—	—	—
17	7	7	—	—	—	—
19	7	8	—	—	—	—
21	7	9	8	9	—	—
23	8	10	9	10	—	—
25	8	11	9	11	—	—
27	8	12	9	12	—	—
29	8	13	9	13	—	—

Let us comment on the diagram above. M_p seems to be always equal to $p/2$ for even p and $(p-3)/2$ for odd. A false impression one could have is that m_p increases with p for odd p. Actually, as Fact 2.3 shows, for $p = 45$ we can expect $m_p \leqslant 6$. On the other hand, $m_p < 6$ looks unlikely.

5. Real analysis applications

One of the applications of the hereby considerations is shown in [1], where a set from D_{12} is used to construct a compact subset of $\mathbb{R}$ (endowed with the Euclidean topology) such that

$$\operatorname{int}(X+X) \neq \varnothing \qquad \text{and} \qquad X-X \quad \text{is Lebesgue null.}$$

We will now make only a few notes akin, cf. also [3]. Let for $A \subset \mathbb{Z}$ and $p \in \mathbb{N}$, $X(A,p) = \left\{\sum_{j=1}^{\infty} a_j p^{-j} : a_j \in A\right\}$.

Fact 5.1. *If $\{k, k+1\} \subset A \subset \mathbb{Z}_{2p}$, and $A \bmod p = \mathbb{Z}_p$ then $X(A,p)$ contains infinitely many intervals and hence has a positive interior measure.*

Proof. As we will show all intervals of the form

$$\sum_{j=1}^{n} a_j p^{-j} + p^{-n-1}[k+1, k+2],$$

where $n \in \mathbb{N}$, $a_j \in A$, $a_j < p$, are contained in $X(A,p)$. Thus, given

$$x = \sum_{j=1}^{n} a_j p^{-j} + q \cdot p^{-n-1}, \qquad \text{for some } q \in [k+1, k+2],$$

we need to find

$$\{a_m(q)\}_{m=0}^{\infty}, \qquad a_m(q) \in A, \text{ for } m \geqslant 0,$$

so that

$$q = \sum_{m=0}^{\infty} a_m(q) p^{-m}.$$

Let $q := \sum_{m=0}^{\infty} q_m p^{-m}$, where $q_m \in \{0, \ldots, p-1\}$ and $\{a_r\}_{r=1}^{\mu} := A \cap \mathbb{Z}_p$, $\{a'_s\}_{s=1}^{\nu} := A \cap (p + \mathbb{Z}_p)$. By assumption we either have $q_0 + q_1 p^{-1} = k + a'_s$ for some $s \in \{1, \ldots, \nu\}$ or $q_0 + q_1 p^{-1} = k + 1 + a_r$ for some $r \in \{1, \ldots, \mu\}$. Hence we have found candidates for $a_0(q)$ and $a_1(q)$. Note that these may need to be reduced by subtracting 1 accordingly to whther a carry will occur. The remaining digits of q can be found in either $A \cap \mathbb{Z}_p$ or $A \cap (p + \mathbb{Z}_p)$ by a similar reasoning. □

Fact 5.2. *Let $B \subset \{b, \ldots, m-1, m+2, \ldots, p+d\}$, where $m + 1 \leqslant d < p - 1$. Complement of $X(B, p)$ contains infitively many intervals.*

Proof. It can be checked that no interval of the form

$$\sum_{j=1}^{n-1} b_j p^{-j} + p^{-n}\left(m + \frac{d+1}{p-1}, m + 2 + \frac{b}{p-1}\right),$$

where $b_j \in \{b, m+2\}$, is contained in $X(B, p)$. □

Fact 5.3. *The same applies when $m > p$.*

Example 5.4. For $A = \{0, 1, 3, 4, 5, 8\} \in D_{12}$ we have what follows:

$$A + A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16\},$$
$$14, 15 \notin A + A,$$
$$(A + A) \bmod 12 = \mathbb{Z}_{12},$$

hence $X(A + A, 12)$ contains some intervals and ommits some other.

Appendix

Matlab codes

This section contains Matlab codes used for the purpose of the hereby paper. The following strategy has been applied

1. Convert the numbers $n \in \{0, \ldots, 2^p\}$ to subsets of $\mathbb{Z}_p$ by means of the binary expansion, e.g.: $11 \mapsto \{0, 1, 3\}$.

2. For each subset $A \subset \mathbb{Z}_p$, compare the sizes of Cayley tables for addition and subtraction modulo p (results of functions `sm` and `dm` respectively) and whenever

$$\#((A + A) \bmod p) > \#((A + A) \bmod p)$$

then append A to the list.

A set is appended to the list together with the corresponding difference of sizes, i.e. `sd`. For bigger p searching over 2^p subsets takes much time, therefore, the second argument of `sumdiff` is responsible for the consecutive portion of data. The portion sizes are fixed as 2^{25}, the variable k is the portion count.

```
-1 function B = dm(A,p)

 1 B=mod(bsxfun(@minus,A,A'),p);
 2 B(isnan(B))=[];
 3 B=unique(B);
 4 end
```

The function `dm(A,p)` finds $(A - A) \bmod p$ as follows

1 The Cayley table for $A - A$ is produced and reduced mod$p$.
2 Since A is a row of a matrix of a fixed width, it may contain some `NaN`s (*not-a-numbers*). Here they are deleted from $(A - A) \bmod p$.
3 The Cayley table contains repetitions. Here they are deleted.

```
-1 function B = sm(A,p)

 1 B=mod(bsxfun(@plus,A,A'),p);
 2 B(isnan(B))=[];
 3 B=unique(B);
 4 end
```

The function `sm(A,p)` does the same for the sum in place of the difference.

```
-1 function C = cat2(A,B)

 1 if size(A,2)<size(B,2)
 2     A=[A,NaN.*ones(size(A,1),size(B,2)-size(A,2))];
 3 elseif size(A,2)>size(B,2)
 4     B=[B,NaN.*ones(size(B,1),size(A,2)-size(B,2))];
 5 end
 6 C=[A;B];
 7 end
```

Vectors representing sets may have different lengths, hence the function `cat2` is defined to handle concatenation of matrices of possibly different widths. This is achieved by concatenating an appropriate number of `NaN`s to each row which is too short.

```
-1 function [A,t] = sumdiff(p,k)

 1 portion=25;
 2 A=[];
 3 for i=(k-1)*2^portion:min(k*2^portion-1,2^p-1)
 4     d2bei=find(mod(floor(i./2.^[0:log2(i)]),2))-1;
 5     sd=size(sm(d2bei,p),1)-size(dm(d2bei,p),1);
 6     if sd>0
 7         A=cat2(A,[sd,NaN,d2bei]);
 8     end
 9 end
10 end
```

The function `sumdiff(p,k)` does the crucial work.

1 The portion of $\mathbb{Z}_p$ is set.
2 The resulting matrix is initialized for future reference.
3–9 The sets fulfilling the condition

$$\#((A+A) \bmod p) > \#((A-A) \bmod p)$$

are filtered and appended to the result.
4 The variable `d2bei` holds the number as a list of non-zero powers of 2 in the binary expansion (i.e. a subset of $\mathbb{Z}_p$).
5 The number $\#((A+A) \bmod p) - \#((A-A) \bmod p)$ is found and kept as `sd`.
6–8 The current set with its `sd` (separated by a `NaN`) is appended to the result if `sd` > 0.

Finally, the function `sdnew` finds the generators of orbits in a given list of sets. An optional argument is a list of the possibly already found generators:

```
function [B,t] = sdnew(A,p,C)

B=[];
if isnan(A(1,2)); A=A(:,3:end); end;
A=A(A(:,1)==0,:);
if nargin<3
    C=[];
    B(1,:)=A(1,:);
    j0=2;
else
    B=C;
    j0=1;
end
B(isnan(B))=-1;
for j=j0:size(A,1)
    flag=1;
    A1=sort(mod(bsxfun(@plus,A(j,:),[0:p-1]'),p),2);
    A2=sort(mod(bsxfun(@plus,-A(j,:),[0:p-1]'),p),2);
```

```
17         A1(isnan(A1))=-1;
18         A2(isnan(A2))=-1;
19         if any(ismember(A1,B,'rows')) ||...
20                     any(ismember(A2,B,'rows'))
21             flag=0;
22         end
23         if flag
24             B=cat2(B,A(j,:));
25         end
26 end
27 if ~isequal(C,[])
28         B(1:size(C,1),:)=[];
29 end
30 B(B==-1)=NaN;
31 end
```

1 The output matrix B is initialized.

2 The input optionally carries now irrelevant information about the difference between the sizes of sum and differerence. This is stored in the first column and separated from the current set with a `NaN` in the second column. Both are now cancelled.

3 Only the sets containing 0 are relevant. Any set not containing 0 has in its orbit a set that does contain 0.

4–11 If the third argument is dropped, the sets in the input will be compared to the first set and then possibly to other flagged as orbit generators. The first set doesn't need to be compared with itself, hence the comparison starts with `j0=2`. Otherwise, ie. when there is a list of so far found generators (an optional `C`), all the input must be checked and compared with `C`.

12,17,18 The crucial work here is done by the `ismember` function which does not handle `NaN`s properly, hence the `NaN`s are changed into -1's.

13–26 Input sets are one by one compared to the already chosen orbit generators and if none of the shifts nor its opposite mod p of the current set is found, the current set is appended to the list of generators.

14 Each set is by default flagged as the orbit generator.

15–16 All the shifts mod p and the opposites mod p are calculated.

19–22 If any of the shifts or its opposite is found on the list of the already found generators, it is flagged off.

23–25 The current set, if flagged, is appended to the list of generators.

27–29 The output is planned as the list of generators filtered from the input only. Hence the optional list of generators (the third argument of the function) is removed from the output.

30 The `NaN`s return (cf. 12,17,18).

List of the orbit generators

Finally, let us list orbit generators for small p.

$$D_{12}: \{0,1,3,4,5,8\},$$
$$D_{14}: \{0,1,3,4,5,6,9\},$$
$$D_{15}: \begin{cases} \{0,1,3,4,5,8\}, \\ \{0,1,2,6,8,10\} \end{cases}$$
$$D_{17}: \begin{cases} \{0,1,3,4,5,6,9\}, \\ \{0,1,4,5,6,7,11\}, \\ \{0,1,3,6,8,9,11\}, \\ \{0,1,2,4,8,10,11\}, \\ \{0,3,4,5,7,8,12\}, \\ \{0,1,2,6,8,10,12\}, \\ \{0,1,4,5,8,11,12\}, \\ \{0,2,4,6,9,11,14\}, \end{cases}$$
$$D_{16}: \begin{cases} \{0,1,3,4,5,6,10\}, \\ \{0,1,3,4,5,7,10\}, \\ \{0,1,3,5,6,7,10\}, \\ \{0,1,3,4,5,6,7,10\}, \\ \{0,1,2,4,5,7,11\}, \\ \{0,1,2,4,6,7,11\}, \\ \{0,1,2,4,5,6,7,11\}, \\ \{0,1,3,4,5,8,12\}, \\ \{0,2,5,6,7,9,12\}, \\ \{0,2,3,5,6,7,9,12\}, \\ \{0,1,3,5,6,7,10,12\}, \\ \{0,1,4,5,8,11,12\}, \end{cases}$$
$$D_{18}: \begin{cases} \{0,1,3,4,5,6,7,11\}, \\ \{0,1,3,4,5,6,8,11\}, \\ \{0,1,3,4,6,7,8,11\}, \\ \{0,1,3,5,6,7,8,11\}, \\ \{0,1,3,4,5,6,7,8,11\}, \\ \{0,1,3,5,6,7,12\}, \\ \{0,1,2,4,5,7,8,12\}, \\ \{0,1,2,5,6,7,8,12\}, \\ \{0,1,2,4,5,6,7,8,12\}, \\ \{0,2,3,5,6,7,10,13\}, \\ \{0,1,2,7,8,10,13\}, \\ \{0,2,3,6,7,8,10,13\}, \\ \{0,2,5,6,7,8,10,13\}, \\ \{0,2,3,5,6,7,8,10,13\}, \\ \{0,1,5,6,7,8,11,13\}, \\ \{0,1,3,5,6,7,8,11,13\}, \\ \{0,1,2,5,6,8,12,13\}, \\ \{0,1,4,7,8,12,13\}, \\ \{0,1,2,5,6,7,8,12,13\}, \\ \{0,1,4,6,7,8,11,14\}, \\ \{0,1,3,4,6,7,8,11,14\}, \\ \{0,1,4,6,7,8,11,12,14\}, \end{cases}$$
$$D_{20}(2): \begin{cases} \{0,1,3,4,5,8,12,13,16\}, \\ \{01,4,5,8,9,12,15,16\}, \end{cases}$$
$$D_{19}: \begin{cases} \{0,1,3,5,6,7,10\}, \\ \{0,1,3,4,5,6,7,10\}, \\ \{0,1,3,5,6,9,11\}, \\ \{0,1,4,5,6,7,8,12\}, \\ \{0,1,2,4,5,9,12\}, \\ \{0,2,3,5,6,7,9,12\}, \\ \{0,1,2,5,6,8,13\}, \\ \{0,1,2,5,6,7,8,13\}, \\ \{0,1,2,3,8,10,13\}, \\ \{0,1,3,4,7,11,13\}, \\ \{0,1,3,4,7,10,11,13\}, \\ \{0,1,2,3,8,10,11,13\}, \\ \{0,1,3,7,9,10,11,13\}, \\ \{0,1,3,4,5,6,9,14\}, \\ \{0,1,3,5,6,9,11,14\}, \\ \{0,1,2,3,8,9,11,14\}, \\ \{0,1,6,7,10,11,14\}, \\ \{0,1,2,6,10,12,14\}, \\ \{0,1,2,6,8,10,12,14\}, \\ \{0,2,3,4,7,11,12,14\}, \\ \{0,1,4,5,8,9,13,14\}, \\ \{0,1,3,4,5,8,12,15\}, \\ \{0,2,5,8,10,12,15\}, \\ \{0,1,2,6,7,11,13,15\}, \\ \{0,1,4,5,8,11,14,15\}, \\ \{0,2,4,6,8,11,13,16\}, \\ \{0,2,4,6,9,11,13,16\}, \end{cases}$$

$$D_{21}(2):\begin{cases}\{0,1,3,5,6,7,10,12\},\\ \{0,1,2,5,6,8,9,14\},\\ \{0,1,2,5,6,7,8,9,14\},\\ \{0,1,3,4,6,7,8,11,14\},\\ \{0,1,2,3,8,9,11,14\},\\ \{0,1,3,4,7,11,13,15\},\\ \{0,1,2,4,8,11,12,14,15\},\\ \{0,2,5,6,7,9,11,12,16\},\\ \{0,1,2,3,8,9,11,14,16\},\\ \{0,1,2,6,7,8,12,14,16\},\\ \{0,2,3,4,7,11,12,14,16\},\\ \{0,1,4,5,9,12,15,16\},\\ \{0,1,4,5,8,9,12,15,16\},\\ \{0,2,5,7,9,12,15,17\},\\ \{0,2,4,6,8,11,13,15,18\},\end{cases}$$

$$D_{22}(2):\begin{cases}\{0,1,3,5,6,7,9,14\},\\ \{0,1,3,5,6,7,8,9,14\},\\ \{0,1,3,4,5,8,13,15\},\\ \{0,1,3,4,5,8,12,13,15\},\\ \{0,2,3,5,7,8,9,11,16\},\\ \{0,3,5,6,7,10,12,16\},\\ \{0,1,3,5,6,7,10,12,16\},\\ \{0,3,5,6,7,9,10,12,16\},\\ \{0,1,2,3,8,10,13,16\},\\ \{0,1,2,3,8,10,11,13,16\},\\ \{0,1,2,3,8,10,13,15,16\},\\ \{0,2,5,9,10,12,13,14,17\},\\ \{0,1,4,7,8,12,16,17\},\\ \{0,1,4,7,8,11,12,16,17\},\\ \{0,1,4,5,9,10,13,16,17\},\end{cases}$$

$$D_{23}(2):\begin{cases}\{0,1,3,5,6,7,8,11,13\},\\ \{0,1,2,5,6,7,9,10,15\},\\ \{0,1,2,5,6,7,8,9,10,15\},\\ \{0,1,3,4,7,8,9,12,15\},\\ \{0,1,3,4,6,7,8,9,12,15\},\\ \{0,1,2,3,5,6,11,14,15\},\\ \{0,2,3,4,7,11,12,14,16\},\\ \{0,1,2,4,5,9,12,13,14,16\},\\ \{0,1,2,6,7,8,13,15,17\},\\ \{0,1,3,4,7,11,13,15,17\},\\ \{0,1,6,7,9,12,14,15,17\},\\ \{0,1,3,4,7,11,13,14,15,17\},\\ \{0,1,3,5,6,7,8,11,13,18\},\\ \{0,1,2,5,7,11,12,14,18\},\\ \{0,1,3,4,5,6,9,14,15,18\},\\ \{0,1,4,7,10,11,14,15,18\},\\ \{0,1,2,6,7,8,12,14,16,18\},\\ \{0,1,2,7,8,10,13,15,16,18\},\\ \{0,2,3,7,9,12,13,14,16,19\},\\ \{0,2,4,7,10,12,14,17,19\},\\ \{0,1,4,5,8,9,12,15,18,19\},\\ \{0,2,4,6,8,10,13,15,17,20\},\end{cases}$$

$$D_{24}(2):\begin{cases}\{0,1,3,4,6,7,8,11,14\},\\ \{0,1,3,5,6,7,8,9,10,15\},\\ \{0,2,3,4,7,11,12,14,16\},\\ \{0,1,2,4,5,9,12,13,14,16\},\\ \{0,1,3,4,5,8,13,15,17\},\\ \{0,1,3,4,5,8,12,13,15,17\},\\ \{0,1,2,4,5,9,12,14,16,17\},\\ \{0,1,2,4,9,12,13,14,16,17\},\\ \{0,1,2,4,5,9,12,13,14,16,17\},\\ \{0,1,2,3,8,10,11,13,16,18\},\\ \{0,1,2,7,8,10,13,15,16,18\},\\ \{0,1,2,4,8,11,14,15,17,18\},\\ \{0,1,3,4,5,6,9,14,15,19\},\\ \{0,2,3,4,7,11,12,14,16,19\},\\ \{0,2,4,7,11,12,14,15,16,19\},\\ \{0,2,3,4,7,11,12,14,15,16,19\},\\ \{0,1,2,3,8,9,11,14,17,19\},\\ \{0,1,2,6,10,11,15,17,19\},\\ \{0,1,2,3,8,9,11,14,16,17,19\},\\ \{0,1,4,5,7,8,9,12,13,16,20\},\\ \{0,1,3,4,5,8,12,13,15,17,20\},\\ \{0,1,3,4,5,8,12,13,16,17,20\},\\ \{0,1,3,4,5,8,12,13,15,16,17,20\},\\ \{0,1,4,5,8,9,12,13,16,19,20\},\\ \{0,2,4,6,8,11,13,15,18,21\}.\end{cases}$$

$$D_{28}(3):\begin{cases}\{0,2,3,5,7,9,10,11,13,20\},\\ \{0,1,3,6,11,12,13,18,19,21\},\\ \{0,1,3,5,6,7,10,12,16,22\},\\ \{0,1,4,5,7,8,9,12,13,16,20,24\},\\ \{0,1,3,4,5,8,12,13,16,20,21,24\},\\ \{0,1,4,5,8,11,12,16,17,20,21,24\},\end{cases}$$

Bibliography

1. Bartoszewicz A., Filipczak M.: *Remarks on sets with small differences and large sums* (to appear).
2. Jackson T.H., Williamson J.H., Woodal D.R.: *Difference-covers that are not k-sum-covers.* Proc. Camb. Phil. Soc. **72**, no. 3 (1972), 425–438.
3. Nitecki Z.: *Cantorval and subsum sets of null sequences.* Math. Amer. Monthly **122**, no. 9 (2015), 862–870.