Distribution of the exponents of primitive circulant matrices in the first four boxes of $\mathbb{Z}_n$.

M.I. Bueno,*

Department of Mathematics and The College of Creative Studies
University of California, Santa Barbara, USA;
mbueno@math.ucsb.edu

K. Y. Fang †

Department of Mathematics
Northwestern University, Evanston, Il, USA;
kuanyingfang2011@u.northwestern.edu

S. Fuller‡

Department of mathematics
Pennsylvania State University, USA;
saf5132@psu.edu

S. Furtado,§

Faculdade de Economia do Porto
Rua Dr. Roberto Frias 4200-464 Porto, Portugal;
sbf@fep.up.pt

Submitted: Dec. 2010; Accepted: ; Published: XX
Mathematics Subject Classification: 11P70, 05C25, 05C50

Abstract

In this paper we consider the problem of describing the possible exponents of n-by-n Boolean primitive circulant matrices. It is well known that this set is a subset of $[1, n-1]$ and not all integers in $[1, n-1]$ are attainable exponents. In the literature, some attention has been paid to the gaps in the set of exponents. The first three gaps have been proven, that is, the integers in the intervals $[\lfloor n/2 \rfloor + 1, n-$

*Supported by Dirección General de Investigación (Ministerio de Ciencia y Tecnología) of Spain under grant MTM2009-09281 and NSF grant DMS-0852065.

†Work done at the UCSB Summer Research Program for Undergraduates 2010 supported by NSF Grant DMS-0852065.

‡Work done at the UCSB Summer Research Program for Undergraduates 2010 supported by NSF Grant DMS-0852065.

§This work was done within the activities of Centro de Estruturas Lineares e Combinatorias da Universidade de Lisboa.

2], $[\lfloor n/3\rfloor+2, \lfloor n/2\rfloor-2]$ and $[\lfloor n/4\rfloor+3, \lfloor n/3\rfloor-2]$ are not attainable exponents. Here we study the distribution of exponents in between those gaps by giving the exact exponents attained there by primitive circulant matrices. We also study the distribution of exponents in between the third gap and our conjectured fourth gap. It is interesting to point out that the exponents attained in between the (i-1)th and the ith gap depend on the value of n mod i.

1 Introduction

A Boolean matrix is a matrix over the binary Boolean algebra $\{0,1\}$. An n-by-n Boolean matrix C is said to be circulant if each row of C (except the first one) is obtained from the preceding row by shifting the elements cyclically 1 column to the right. In other words, the entries of a circulant matrix $C=(c_{ij})$ are related in the manner: $c_{i+1,j}=c_{i,j-1}$, where $0\le i\le n-2$, $0\le j\le n-1$, and the subscripts are computed modulo n. The first row of C is called the generating vector. Here and throughout we number the rows and columns of an n-by-n matrix from 0 to $n-1$.

The set of all n-by-n Boolean circulant matrices forms a multiplicative commutative semigroup C_n with $|C_n|=2^n$ [5, 9]. In 1974, K. H. Kim-Buttler and J.R. Krabill [7], and S. Schwarz [10] investigated this semigroup thoroughly.

An n-by-n Boolean matrix C is said to be primitive if there exists a positive integer k such that $C^k=J$, where J is the n-by-n matrix whose entries are all ones and the product is computed in the algebra $\{0,1\}$. The smallest such k is called the exponent of C, and we denote it by $\exp(C)$. Let us denote $E_n=\{exp(C): C\in C_n,\ C \text{ is primitive}\}$.

In [1] we stated the following question: Given a positive integer n, what is the set E_n?

The previous question can easily be restated in terms of circulant graphs or bases for finite cyclic groups, as we explain next.

Let C be a Boolean primitive circulant matrix and let S be the set of positions corresponding to the nonzero entries in the generating vector of C (where the columns are counted starting with zero). C is the adjacency matrix of the circulant digraph $Cay(\mathbb{Z}_n, S)$. The vertex set of this graph is $\mathbb{Z}_n$ and there is an arc from u to u+a (mod n) for every $u\in\mathbb{Z}_n$ and every $a\in S$. A digraph D is called primitive if there exists a positive integer k such that for each ordered pair a,b of vertices there is a directed walk from a to b of length k in D. The smallest such integer k is called the exponent of the primitive digraph D. Thus, a circulant digraph G is primitive if and only if its adjacency matrix is. Moreover, if they are primitive, they have the same exponent. Therefore, finding the set E_n is equivalent to finding the possible exponents of circulant digraphs of order n.

Let n be a positive integer and let S be a nonempty subset of the additive group $\mathbb{Z}_n$. For a positive integer k we denote by kS the set given by

$$kS=\{s_1+\cdots+s_k \text{ mod n}: s_i\in S\}\subset\mathbb{Z}_n.$$

The set kS is called the k-fold sumset of S.

The set S is said to be a basis for $\mathbb{Z}_n$ if there exists a positive integer k such that $kS=\mathbb{Z}_n$. The smallest such k is called the order of S, denoted by $order(S)$. It is well known that the set $S = \{s_0, s_1, ..., s_r\} \subset \mathbb{Z}_n$ is a basis if and only if $gcd(s_1 - s_0, ..., s_r - s_0, n) = 1$. In [1] we proved that, given a matrix C in C_n, if S is the set of positions corresponding to the nonzero entries in the generating vector of C, then C is primitive if and only if S is a basis for $\mathbb{Z}_n$. Moreover, if C is primitive, then $\exp(C) = order(S)$. Therefore, finding the set E_n is equivalent to finding the possible orders of bases for the cyclic group $\mathbb{Z}_n$. This question is quite interesting by itself.

The problem we study in this paper has applications in different areas. In particular, circulant matrices appear as transition matrices in Markov processes [3]. Also, the problem stated in terms of bases for $\mathbb{Z}_n$ has applications in Coding Theory and Quantum information [8].

In the literature, the problem of computing all possible exponents attained by circulant primitive matrices or, equivalently, by circulant digraphs, has been considered. In particular, the following results were obtained. Here and throughout, $[a, b]$ denotes the set of positive integers in the real interval $[a, b]$. If $a > b$ then $[a, b] = \emptyset$.

Lemma 1. *[4, 11] If C is a primitive circulant matrix, then its exponent is either $n-1$, $\lfloor n/2 \rfloor$, $\lfloor n/2 \rfloor - 1$ or does not exceed $\lfloor n/3 \rfloor + 1$. Moreover, $exp(C) = n - 1$ if and only if the number of nonzero entries in the generating vector of C is exactly 2.*

Lemma 2. *[6] For every $n \geq 3$, $[\lfloor n/4 \rfloor + 3, \lfloor n/3 \rfloor - 2] \cap E_n = \emptyset$.*

All these results can be immediately translated into results about the possible orders of bases for a finite cyclic group.

Note that the only primitive matrix in C_2 is J_2, so $E_2 = \{1\}$. From now on, we assume that $n \geq 3$. In [1] we presented a conjecture concerning the possible exponents attained by n-by-n Boolean primitive circulant matrices which we restate here in a more precise way. We start with a definition.

Definition 3. *Let j be a positive integer. We call the j^{th} box of $\mathbb{Z}_n$, and denote it by B_j, the set of positive integers*

$$\left[\left\lfloor \frac{n}{j} \right\rfloor - 1, \left\lfloor \frac{n}{j} \right\rfloor + j - 2\right].$$

Conjecture 4. *If $C \subseteq C_n$ is primitive, then*

$$exp(C) \in [1, \lfloor \sqrt{n} \rfloor] \cup \bigcup_{j=1}^{\lfloor \sqrt{n} \rfloor} B_j.$$

In a recent preprint [6], it was proven that if $C \in C_n$ is primitive and its exponent is greater than k for some positive integer k, then there exists d_k such that the exponent of C is within d_k of n/l for some integer $l \in [1, k]$. Notice that the result we present in Conjecture 4 produces gaps in the set of exponents which are larger than the ones encountered in [6]. In fact, we showed in [2] that the gaps in our conjecture should be maximal. However, as stated in [6], we remain far from a complete characterization of the possible exponents of $n \times n$ primitive circulant matrices.

All the results in this paper are given in terms of bases for $\mathbb{Z}_n$ since the equivalent formulation of the problem in these terms resulted more fruitful than the original statement of the problem in terms of circulant matrices. Lemmas 1 and 2 show the gaps between the first and second box, between the second and third box, and between the third and fourth box when these boxes do not overlap. Here we study the distribution of orders of bases in the first three boxes by showing what orders are attained and which ones are not. We also study the order of bases in the fourth box by giving orders that are attained and we conjecture that those are, in fact, the exact orders in that box. In addition, we also prove that all integers in $[1, \lfloor\sqrt{n}\rfloor]$ are attained by bases of $\mathbb{Z}_n$.

This paper is organized as follows. In Section 2 we state our main results and prove them in Section 4. In section 3 we state and prove several auxiliary results concerning the order of bases for $\mathbb{Z}_n$, which will be used to prove our main theorems. The order of several bases for $\mathbb{Z}_n$ with cardinality at most 4 that are relevant to our proofs is studied in the appendix.

2 Main Results

In this section, we give the exact orders attained by bases for $\mathbb{Z}_n$ in the first three boxes of $\mathbb{Z}_n$. We also give orders attained in the fourth box. Notice that the results for the first and second box were already known [4, 11] but we include them for completeness. Finally, we state that all integers up to $\lfloor\sqrt{n}\rfloor$ are in E_n.

The result for the first box is an immediate consequence of Lemma 1.

Theorem 5. *[4] For all n,*

$$B_1 \subseteq E_n.$$

The next theorems are our main results and will be proved in Section 4. In our first two results we assume a lower bound n_0 for n, which is the smallest value of n for which the theorem holds for all $n > n_0$. The possible orders in E_n, with $n < n_0$, appear in Tables 1 and 2. We observe that, for any n for which the box under study does not overlap with adjacent boxes, the theorem holds. We also notice that, though we have a lower bound for n in our results, when $n \equiv 0$ mod j, $j = 2, 3, 4$, B_j is a subset of E_n, for all n.

Theorem 6. *Let $n \geq 17$ be a positive integer.*

- *If n is even, then $B_2 \subseteq E_n$.*
- *If n is odd, then $B_2 \cap E_n = \left\lfloor \frac{n}{2} \right\rfloor$.*

Theorem 7. *Let $n \geq 45$ be a positive integer.*

- *If $n \equiv 0$ (mod 3), then $B_3 \subseteq E_n$.*
- *If $n \equiv 1$ (mod 3), then $B_3 \cap E_n = \left\{ \left\lfloor \frac{n}{3} \right\rfloor + 1, \left\lfloor \frac{n}{3} \right\rfloor \right\}$.*

- *If* $n \equiv 2 \pmod 3$, *then* $B_3 \cap E_n = \left\{ \left\lfloor \frac{n}{3} \right\rfloor + 1 \right\}$.

Theorem 8. *Let* $n \geq 16$ *be a positive integer.*

- *If* $n \equiv 0 \pmod 4$, *then* $B_4 \subseteq E_n$.
- *If* $n \equiv 1 \pmod 4$, *then* $\left\{ \left\lfloor \frac{n}{4} \right\rfloor + 2, \left\lfloor \frac{n}{4} \right\rfloor + 1, \left\lfloor \frac{n}{4} \right\rfloor \right\} \subseteq E_n$.
- *If* $n \equiv 2 \pmod 4$ *or* $n = 3$ *mod(4), then* $\left\{ \left\lfloor \frac{n}{4} \right\rfloor + 2, \left\lfloor \frac{n}{4} \right\rfloor + 1 \right\} \subseteq E_n$.

Though we do not prove it, we conjecture that $\lfloor n/4 \rfloor - 1 \notin E_n$ when $n \equiv 1 \pmod 4$ and $\lfloor n/4 \rfloor - 1, \lfloor n/4 \rfloor \notin E_n$ when $n \equiv 2, 3 \pmod 4$.

n	E_n	n	E_n	n	E_n
2	1	23	1...8,11,22	44	1...13, 15, 21, 22, 43
3	1,2	24	1...9, 11, 12, 23	45	1...16, 22, 44
4	1,2,3	25	1...9, 12, 24	46	1...13, 15, 16, 22, 23, 45
5	1, 2, 4	26	1...9,12, 13, 25	47	1...13, 16, 23, 46
6	1, 2, 3, 5	27	1...10,13,26	48	1...17, 23, 24, 47
7	1,2,3,6	28	1...10, 13, 14, 27	49	1...14, 16, 17, 24, 48
8	1...4,7	29	1...10, 14, 28	50	1...14, 17, 24, 25, 49
9	1...4,8	30	1...11, 14, 15, 29	51	1...14, 16, 17, 18, 25, 50
10	1...5,9	31	1...11, 15, 30	52	1...15, 17, 18, 25, 26, 51
11	1...5, 10	32	1...11, 15, 16, 31	53	1...15, 18, 26, 52
12	1...6, 11	33	1...12, 16, 32	54	1...15, 19, 26, 27, 53
13	1...6, 12	34	1...12, 16, 17, 33	55	1...15, 19, 27, 54
14	1...7, 13	35	1...10, 12, 17, 34	56	1...16, 19, 27, 28, 55
15	1...7,14	36	1...13, 17, 18, 35	57	1...16, 19, 20, 28, 56
16	1...8,15	37	1...13, 18, 36	58	1...16, 20, 28, 29, 57
17	1...6,8,16	38	1...11, 13, 18, 19, 37	59	1...16, 20, 29, 58
18	1...9, 17	39	1...14, 19, 38	60	1...17, 19,20,21, 29, 30, 59
19	1...7, 9,18	40	1...14, 19, 20, 39	61	1...17, 20, 21, 30, 60
20	1...7, 9,10,19	41	1...12, 14, 20, 40	62	1...17, 21, 30, 31, 61
21	1...8,10,20	42	1...14, 15, 20, 21, 41	63	1...17, 20, 21, 22, 31, 62
22	1...8, 10, 11, 21	43	1...12, 14, 15, 21, 42	64	1...18, 21, 22, 31, 32, 63

Table 1: Orders of bases for $\mathbb{Z}_n$

In Tables 1 and 2 we give the exact orders attained by bases for $\mathbb{Z}_n$ with $n = 2, 3, 4, ..., 104$. As the numerical experiments show, for each n there is a number of consecutive orders that can be attained by bases of $\mathbb{Z}_n$. Though we just prove Theorem 9, according to our numerical experiments, we conjecture that at least all consecutive integers up to $2\sqrt{n} - 2$ are attained orders.

Theorem 9. *Let n be a positive integer. Then,* $[1, \lfloor\sqrt{n}\rfloor] \subseteq E_n$.

Though this result is referred in [6], it seems that the paper where its proof is said to be is not available.

n	E_n	n	E_n
65	1,...,14,16,17,18,22,32,64	85	1,...,18,20,21,22,23,28,29,42,84
66	1,...,18, 21,22,23,32,33,65	86	1,...,18,20,21,22,23,29,42,43,85
67	1,...,18, 22, 23, 33, 66	87	1,...,18,20,22,23,28,29,30,43,86
68	1,...,19,23,33,34,67	88	1,...,24,29,30,43,44,87
69	1,...,19,22,23,24,34,68	89	1,...,20,22,23,24,30,44,88
70	1,...,15, 17,18,19,23,24,34,35,69	90	1,...19,21,22,23,24,29,30,31,44,45,89
71	1,...,19, 24, 35, 70	91	1,...,21,23,24,30,31,45,90
72	1,...,20, 23,24,25,35,36,71	92	1,...19,21,22,23,24,25,31,45,46,91
73	1,...,20, 24, 25, 36, 72	93	1,...,21,23,24,25,30,31,32,46,92
74	1,...,20, 25, 36, 37, 73	94	1,...,21,23,24,25,31,32,46,47,93
75	1,...,16, 18,19,20,24,25,26,37,74	95	1,...,20,22,24,25,32,47,94
76	1,...,21,25,26,37,38,75	96	1,...,26,31,32,33,47,48,95
77	1,...,16,18,19,20,21,26,38,76	97	1,...,18,20,22,24,25,26,32,33,48
78	1,...,21,25,26,27,38,39,77	98	1,...,22,24,25,26,33,48,49,97
79	1,...,18, 20,21,26,27,39,78	99	1,...,22, 25,26,32, 33,34, 49, 98
80	1,...,17,19,20,21,22,27,39,40,79	100	1,...,21, 23, 24, 25, 26, 27, 33, 34, 49, 50, 99
81	1,...,22,26,27,28,40,80	101	1,...,23, 25, 26, 27, 34, 50,100
82	1,...,17,19,20,21,22,27,28,40,41,81	102	1,...,21,23,25,26,27,33,34,35,50,51,101
83	1,...,19,21,22,28,41,82	103	1,...,19, 21, 22, 23, 26, 27, 34, 35, 51, 102
84	1,...,23,27,28,29,41,42,83	104	1,...,19, 21,22,23,25,26,27,28,35,51,52,103

Table 2: Orders of bases for $\mathbb{Z}_n$

3 Order of Bases for $\mathbb{Z}_n$

Computing the order of bases for $\mathbb{Z}_n$ is, in general, a challenging task. In this section we introduce some results relative to the order of bases of $\mathbb{Z}_n$ that will be helpful when proving our main results.

To start with, let us notice that the order of a basis S is invariant under shifts and multiplication by a unit of $\mathbb{Z}_n$, that is, for $a \in \mathbb{Z}_n$ and b a unit of $\mathbb{Z}_n$

$$order(S) = order(S + a), \quad \text{and} \quad order(S) = order(b * S) \tag{1}$$

where $b * S = \{\text{bs mod n} : s \in S\}$. In particular, this result implies that the set of orders attained by bases of $\mathbb{Z}_n$ is the same as the set of orders attained by bases of $\mathbb{Z}_n$ containing 0.

We now state some known results about the order of a basis for $\mathbb{Z}_n$. The following lemma gives an upper bound on the cardinality of a basis when a lower bound on its order is known.

Lemma 10. *[8] Let $n \in \mathbb{N}$ and $\rho \in [2, n-1]$. Let S be a basis for $\mathbb{Z}_n$ such that $order(S) \geq \rho$. Then,*

$$|S| \leq max\left\{\frac{n}{d}\left(\left\lfloor\frac{d-2}{\rho-1}\right\rfloor+1\right) : d|n, d \geq \rho+1\right\}.$$

In particular, for each fixed $k \in \mathbb{N}$, if $order(S) \geq \frac{n}{k}$ and $n >> 0$, then $|S| \leq 2k$.

The next lemma gives an upper and a lower bound on the order of some bases for $\mathbb{Z}_n$ with cardinality 3.

Lemma 11. *[2] Let $2 \leq b \leq n-1$. Then,*

$$\left\lfloor\frac{n}{b}\right\rfloor \leq order(\{0,1,b\}) \leq \left\lfloor\frac{n}{b}\right\rfloor + b - 2.$$

Lemma 12. *Let $1 \leq r < b \leq n-1$. Then,*

$$order(\{0,1,2,...,r,b\}) \leq \left\lfloor\frac{n}{b}\right\rfloor + \left\lceil\frac{b-2}{r}\right\rceil.$$

Proof. Let $S = \{0,1,2,...,r,b\}$. It can be shown by induction on k that, for $k \geq 1$,

$$kS = \bigcup_{i=0}^{k}[l_{i,k}, u_{i,k}],$$

where $l_{i,k} = ib$ and $u_{i,k} = ib + (k-i)r$. Let $n = bm + t$, with $0 \leq t < b$. We have $\max\limits_{i=1,\ldots,m} = l_{i,m} - u_{i-1,m} = b - r$ and $u_{m,m} = mb$. Also note that, if $x \in kS$, then $\{x, \ldots, x + k'r\} \in (k+k')S$. Then,

$$order(S) \leq m + \max\left\{\left\lceil\frac{b-r-1}{r}\right\rceil, \left\lceil\frac{t-1}{r}\right\rceil\right\} \leq m + \left\lceil\frac{b-2}{r}\right\rceil$$

which proves the result. □

We now give the exact order of some particular bases for $\mathbb{Z}_n$ that will be needed later. The next lemma shows, in particular, that the largest element of the jth box, $j \leq \sqrt{n}$, belongs to E_n for all n.

Lemma 13. *[1] For $j \in \{1, 2, \ldots, \lfloor\sqrt{n}\rfloor\}$,*

$$order\{0,1,j\}) = \left\lfloor\frac{n}{j}\right\rfloor + j - 2.$$

Lemma 14. *[2] Let $2 \leq j \leq \sqrt{n}$ be a positive integer. Then,*

$$order\left(\left\{0, 1, \left\lfloor \frac{n}{j} \right\rfloor + 1\right\}\right) = \left\lfloor \frac{n}{j} \right\rfloor + j - 2.$$

Lemma 15. *[1] Let $2 \leq r \leq n-1$ and $t = n - r\lfloor n/r \rfloor$. Then,*

$$order(\{0, 1, 2, ..., r-1, r\}) = \begin{cases} \lfloor n/r \rfloor, & \text{if } t \leq 1 \\ \lfloor n/r \rfloor + 1, & \text{if } t > 1 \end{cases}.$$

Lemma 16. *Let $2 \leq r \leq n-2$. Then,*

$$order(\{0, 1, 2, ..., r-1, r+1\}) = \left\lfloor \frac{n}{r+1} \right\rfloor + 1.$$

Proof. Let $S = \{0, 1, 2, ..., r-1, r+1\}$. It can be shown by induction on k that, for $k \geq 1$, $kS = [0, \cdots, k(r+1)-2] \cup \{k(r+1)\}$. Thus, $order(S) = k$ if and only if k is the minimum integer such that $k(r+1) - 2 \geq n-1$, which implies the result. □

Lemma 17. *Suppose that m is a divisor of n and let $1 \leq q < m \leq n$. Then,*

$$order\left(\bigcup_{i=0}^{q}(i + \langle m \rangle)\right) = \left\lceil \frac{m-1}{q} \right\rceil.$$

Proof. Let S be the basis in the statement. Note that $kS = \bigcup_{i=0}^{kq}(i + \langle m \rangle)$. Therefore, the order of S equals the minimum k such that $kq \geq m-1$ and the result follows. □

As a consequence of the previous result, we obtain that, if j is a divisor of n, the smallest element of the jth box is an element of E_n, as $order\left(\langle n/j \rangle \cup (1 + \langle n/j \rangle)\right) = n/j - 1$.

Using canonical projections we can bound the order of some bases in a convenient way. Given $\mathbb{Z}_n$ and a proper divisor m of n, we denote by ϕ the canonical quotient map $\phi : \mathbb{Z}_n \to \mathbb{Z}_{n/m}$. We denote by $order_n(S)$ the order of the basis S as a subset of $\mathbb{Z}_n$.

Lemma 18. *Let m be a proper divisor of n. If S is a basis for $\mathbb{Z}_n$ that contains zero and an element of order m, then $\phi(S)$ is a basis for $\mathbb{Z}_{n/m}$ and*

$$order_{n/m}(\phi(S)) \leq order_n(S) \leq order_{n/m}(\phi(S)) + m - 1.$$

Proof. First, we show, by induction on k, that $\phi(kS) = k\phi(S)$ for all $k \geq 1$. Clearly the equality holds for $k = 1$. Since ϕ is a group homomorphism, we get

$$\phi((k+1)S) = \phi(kS + S) = \phi(kS) + \phi(S) = k\phi(S) + \phi(S) = (k+1)\phi(S). \qquad (2)$$

Let $order_n(S) = q$. As $qS = \mathbb{Z}_n$, the first inequality follows because

$$q\phi(S) = \phi(qS) = \phi(\mathbb{Z}_n) = \mathbb{Z}_{n/m}$$

as ϕ is surjective.

Now we prove the second inequality. Let s be an element of order m in S. Then $s \in \langle n/m \rangle$, that is, $s = b_0\, n/m$ for some $b_0 \in \{1, \ldots, m-1\}$. Let $order_{n/m}(\phi(S)) = t$. Then, since $\phi(tS) = t\phi(S) = \mathbb{Z}_{n/m}$,

$$\left\{0, b_0\frac{n}{m}, 1+b_1\frac{n}{m}, 2+b_2\frac{n}{m}, \ldots, \frac{n}{m}-1+b_{\frac{n}{m}-1}\frac{n}{m}\right\} \subseteq tS$$

for some $b_i \in \{0,1,...,m-1\}$, $1 \leq i \leq n/m-1$. Since $ls \in (m-1)\,S$ for all $l \in \{0,1,...,m-1\}$, then $i+b_i\,n/m+ls \in (m-1)\,S+tS$, for all l and all i. But this shows that $\mathbb{Z}_n \subseteq (m-1+t)\,S$, so that $order_n(S) \leq m-1+t$. Note that

$$\mathbb{Z}_n = \bigcup_{\substack{1\leq i\leq n/m-1\\ 0\leq l\leq m-1}} \left\{i+b_i\frac{n}{m}+ls\right\}.$$

□

The next corollaries are immediate consequences of the previous lemma and Lemma 1.

Corollary 19. *Suppose m is a proper divisor of n and S is a basis for $\mathbb{Z}_n$ that contains zero and an element of order m. Then,*

$$order(S) \leq \frac{n}{m}+m-2.$$

Corollary 20. *Let S be a basis for $\mathbb{Z}_n$ and assume that S contains zero and an element of order 2. Then,*

$$order(S) \leq \left\lfloor\frac{n}{4}\right\rfloor+1 \quad or \quad order(S) \geq \left\lfloor\frac{n}{2}\right\rfloor-1.$$

Corollary 21. *Let S be a basis for $\mathbb{Z}_n$ and assume that S contains zero and an element of order 3. Then,*

$$order(S) \leq \left\lfloor\frac{n}{6}\right\rfloor+2 \quad or \quad order(S) \geq \left\lfloor\frac{n}{3}\right\rfloor-1.$$

The next lemma allows us to prove Corollary 23, which is a key result in the proof of our main theorems.

Lemma 22. *Let $j \geq 2$ be an integer and assume that $b \in I_j = \left[\left\lfloor\frac{n}{j+1}\right\rfloor+2, \left\lfloor\frac{n}{j}\right\rfloor-1\right]$. Then,*

$$order(\{0,1,b\}) \leq \left\lfloor\frac{n}{j+2}\right\rfloor+j.$$

Proof. Let $S=\{0,1,b\}$. First we observe that $j+1<(j+1)b-n<b$. To see this, suppose that $b=\left\lfloor\frac{n}{j+1}\right\rfloor+i \in I_j$. Then $n=(j+1)(b-i)+r$, with $0 \leq r < j+1$ which implies $b(j+1)-n=(j+1)i-r$. On the other hand, since $j+1>r$ and $i \geq 2$, we get that $(j+1)i-r > 2(j+1)-(j+1)=(j+1)$. Thus the inequality on the left follows. The inequality on the right is true because $bj < \lfloor n/j \rfloor\, j \leq n$. We now divide the proof into three cases.

Case 1: Assume b is even and $(j+1)b - n = b/2$. This implies that $(2j+1)b/2 = n$ and, therefore, b is not a divisor of n. Since $(2j+1)b = 2n$, then b is an element of $\mathbb{Z}_n$ of order $2j+1$. Then,

$$order(S) \le \frac{n}{2j+1} + 2j - 1 \le \left\lfloor \frac{n}{j+2} \right\rfloor + j.$$

The first inequality follows from Corollary 19. In order to prove the second inequality, notice that, since $j+1 < b/2$ and $b/2$ is an integer, then $b/2 = j+2+k$ for some nonnegative integer k. Thus,

$$\left\lfloor \frac{n}{j+2} \right\rfloor + j = \left\lfloor \frac{(2j+1)(j+2+k)}{j+2} \right\rfloor + j = 3j + 1 + \left\lfloor \frac{(2j+1)k}{j+2} \right\rfloor$$

$$\ge 3j + 1 + k = \frac{b}{2} + 2j - 1 = \frac{n}{2j+1} + 2j - 1.$$

Case 2: Assume $(j+1)b - n < b/2$. Let $k = j+1$ and $p = (j+1)b - n$. Clearly, $[0,k] \cup \{p\} \cup [b, b+k-1] \subseteq kS$. It can be shown by induction on q that

$$\bigcup_{i=0}^{q} [ip, ip + (q-i)k] \cup [b, b+qk-1] \subset qkS \tag{3}$$

and

$$\bigcup_{i=0}^{q-1} [ip + (k-1)b, ip + (k-1)b + (q-(i+1))k] \subset (qk-1)S. \tag{4}$$

Now assume that q is the largest integer such that $qp < b$, that is, $q = \lfloor b/p \rfloor$ and let $l = \max\{b - pq, p - k\}$. Note that $q \ge 2$. Also, the gaps between consecutive intervals in the unions in (3) and (4) have at most l-1 elements. Thus, we have

$$[0, b+j] \cup [jb, jb + (q-1)p + l] \subseteq (qk + l - 1)S.$$

Since $[0, ib+j] \subseteq (qk+l-1+i-1)S$, for all $i \ge 1$, we get $[0, jb+j] \subseteq (qk+l-1+j-1)S$. Thus, $[0, jb + (q-1)p + l + j - 1] \subseteq (qk + l - 1 + (j-1))S$. We now show that

$$jb + (q-1)p + l + j - 1 \ge n - 1,$$

or, equivalently,

$$(q-1)p + l + j \ge n - jb, \tag{5}$$

which implies

$$order(S) \le qk + max\{b - pq, p - k\} + j - 2. \tag{6}$$

In fact, since $n - jb = b - p$, (5) is equivalent to $j + l \ge b - qp$, which is true because of the definition of l.

Let $b = pq + r$, $0 \le r < p$ and $q_1 = \lfloor rk/p \rfloor$. We proceed by proving that

$$max\{b - pq, p - k\} \le q_1 + p - k \tag{7}$$

which implies
$$order(S) \leq \left\lfloor \frac{bk}{p} \right\rfloor + p - k + j - 2. \tag{8}$$
Since $q_1 \geq 0$, the case $p - k \geq b - pq$ is clear. Consider the case $r = b - pq > p - k$. Let $f = p - r$. Then, $1 \leq f < k$ and
$$q_1 = \left\lfloor \frac{rk}{p} \right\rfloor = \left\lfloor \frac{(p-f)k}{p} \right\rfloor = k - \left\lceil \frac{fk}{p} \right\rceil \geq k - f,$$
where the last inequality follows because $k = j + 1 < (j+1)b - n = p$. So
$$q_1 + p - k \geq k - f + p - k = p - f = r$$
and (7) follows. Taking into account (8), to complete the proof it is sufficient to show that
$$\left\lfloor \frac{bk}{p} \right\rfloor + p - k + j - 2 \leq \left\lfloor \frac{n}{j+2} \right\rfloor + j. \tag{9}$$
Let g be the function given by
$$g(b) = \frac{bk}{p} + p - 3 = \frac{n}{p} + p - 2.$$
It is enough to show that
$$g(b) \leq \frac{n}{j+2} + j.$$
A calculation shows that $g(b) \leq \frac{n}{j+2} + j$ if and only if $p \in \left[j+2, \frac{n}{j+2} \right]$ or equivalently, if and only if
$$b \in \left[\frac{n+j+2}{j+1}, \frac{n + \frac{n}{j+2}}{j+1} \right].$$
By hypothesis, $b < \frac{2n}{2j+1}$, and it is easy to see that $\frac{2n}{2j+1} \leq \frac{n+\frac{n}{j+2}}{j+1}$. Also,
$$\left\lceil \frac{n+j+2}{j+1} \right\rceil = \left\lceil \frac{n+1}{j+1} \right\rceil + 1 \leq \left\lfloor \frac{n}{j+1} \right\rfloor + 2 \leq b.$$
Thus, (9) follows.

Case 3: Assume $(j+1)b - n > b/2$. Note that $j = \lfloor n/b \rfloor$. Let $n = jb + r_3$, $0 \leq r_3 < b$. Thus, $(j+1)b - n = b - r_3$. Clearly, $[0, j+1] \cup \{b - r_3\} \cup [b, b+j] \cup [jb, jb+1] \subseteq (j+1)S$. It can be shown by induction on j that
$$[0, qj+1] \cup \bigcup_{i=0}^{q-1} [b - (q-i)r_3, b - (q-i)r_3 + ij] \cup [b, b+qj] \subset (qj+1)S \tag{10}$$

Denote by q the largest integer such that $qj+2 \leq b-qr_3$, that is, $q = \left\lfloor \frac{b-2}{j+r_3} \right\rfloor$. Let $l = max\{r_3, b-q(j+r_3)-1\}$. Note that any gaps between consecutive intervals in the union (10) have at most $l-1$ elements. Since $[jb, jb+(q-1)j+1] \subset (qj+1)S$, we have

$$[0, b+qj+l-1] \cup [jb, jb+(q-1)j+1+l-1] \subset (qj+1+l-1)S,$$

which implies

$$[0, jb+(q-1)j+1+l-1+j-1] \subset (qj+1+l-1+j-1)S.$$

As

$$jb+(q-1)j+1+l+j-2 = jb+qj+l-1 \geq jb+r_3-1 = n-1,$$

it follows that

$$order(S) \leq qj + max\{r_3, b-q(j+r_3)-1\} + j - 1. \tag{11}$$

Now we show that

$$qj+l+j-1 \leq \left\lfloor \frac{j(b-1)}{j+r_3} \right\rfloor + j + r_3 - 1 \leq \left\lfloor \frac{n}{j+2} \right\rfloor + j. \tag{12}$$

To see the first inequality in (12), it is enough to note that, by definition of q, $q(j+r_3) < b-1$ and $b-1 \leq (q+1)(j+r_3)$. To see the second inequality in (12), let h be the function given by

$$h(b) = \frac{j(b-1)}{j+r_3} + j + r_3 - 1 = \frac{n}{j+n-jb} + j + n - jb - 2.$$

Then, we see that

$$h(b) \leq \frac{n}{j+2} + (j+2) - 2 \text{ if and only if } j+n-jb \in \left[j+2, \frac{n}{j+2}\right].$$

Moreover, for $j+n-jb = \left\lfloor \frac{n}{j+2} \right\rfloor + 1$, we get

$$\lfloor h(b) \rfloor = \left\lfloor \frac{n}{j+2} \right\rfloor + j,$$

since by Theorem 5.7 in [2], and taking into account that $j < \sqrt{n}$,

$$\left\lfloor \frac{n}{\left\lfloor \frac{n}{j+2} \right\rfloor + 1} \right\rfloor = j+1.$$

Therefore, if $j+n-jb \in \left[j+2, \frac{n}{j+2}+1\right]$, or equivalently, if

$$b \in \left[\frac{n+j-1-\frac{n}{j+2}}{j}, \frac{n-2}{j}\right] \tag{13}$$

then the second inequality in (12) holds. We finish the proof by showing that any b satisfying our assumptions is such that (13) holds. Note that, as $(j+1)b - n > \frac{b}{2}$, we have $2n/(2j+1) < b \leq \lfloor n/j \rfloor - 1$. Thus, because $j \geq 2$, it follows that $b \leq \frac{n}{j} - 1 \leq \frac{n-2}{j}$. If $|I_j| \geq 2$, we claim that

$$\frac{n + j - 1 - \frac{n}{j+2}}{j} \leq \frac{2n}{2j+1} < b. \tag{14}$$

Note that if the first inequality would not hold then $n \leq 2j^2 + 5j + 1$, and, for $n = 2j^2 + 5j + 1 - s$ with $0 \leq s \leq 2j^2 + 5j + 1$,

$$\left\lfloor \frac{n}{j+1} \right\rfloor + 2 = 2j + 4 + \left\lfloor \frac{j-1-s}{j+1} \right\rfloor \geq 2j + 4 + \left\lfloor \frac{1-s}{j} \right\rfloor = \left\lfloor \frac{n}{j} \right\rfloor - 1,$$

a contradiction since $|I_j| \geq 2$.

If $|I_j| = 1$, then $b = \left\lfloor \frac{n}{j} \right\rfloor - 1$. If (14) holds, we are done. Otherwise, we claim that

$$\frac{n + j - 1 - \frac{n}{j+2}}{j} \leq b = \left\lfloor \frac{n}{j} \right\rfloor - 1.$$

To see this, let $n = \left\lfloor \frac{n}{j} \right\rfloor j + t$, with $0 \leq t < j$, and assume that

$$\frac{2n}{2j+1} < \left\lfloor \frac{n}{j} \right\rfloor - 1 < \frac{n + j - 1 - \frac{n}{j+2}}{j} \tag{15}$$

in order to get a contradiction. Multiplying (15) by j, we get

$$2j^2 + j + (2j+1)t < n < 2j^2 + 3j - 2 + t(j+2). \tag{16}$$

which implies $t < 2$. If $t = 0$, then $2j^2 + j < n < 2j^2 + 3j - 2$. Therefore, $n = j(2j+2) = 2j(j+1)$ and

$$\left\lfloor \frac{n}{j} \right\rfloor - 1 < \left\lfloor \frac{n}{j+1} \right\rfloor + 2, \tag{17}$$

which contradicts our assumption. The case $t = 1$ cannot occur as, by (16), $j(2j+3)+1 < n < j(2j+4)$. □

Corollary 23. *Let $n \geq 16$. Suppose that $2 \leq b \leq \lfloor n/2 \rfloor + 1$.*

i) If either $b \notin \left\{2, 3, \left\lfloor \frac{n}{3} \right\rfloor, \left\lfloor \frac{n}{3} \right\rfloor + 1, \left\lfloor \frac{n}{2} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor + 1\right\}$, or $b = \left\lfloor \frac{n}{3} \right\rfloor$ and $n \neq 0 \bmod 3$ then

$$order(\{0, 1, b\}) \leq \left\lfloor \frac{n}{4} \right\rfloor + 2.$$

ii) If either $b \in \{3, \left\lfloor \frac{n}{3} \right\rfloor + 1\}$*, or* $b = \left\lfloor \frac{n}{3} \right\rfloor$ *and* $n \equiv 0 \bmod 3$*, or* $b = \left\lfloor \frac{n}{2} \right\rfloor$ *with* n *odd, then*

$$order(\{0,1,b\}) = \left\lfloor \frac{n}{3} \right\rfloor + 1.$$

iii) If either $b \in \{2, \left\lfloor \frac{n}{2} \right\rfloor + 1\}$*, or* $b = \left\lfloor \frac{n}{2} \right\rfloor$ *and* n *is even, then*

$$order(\{0,1,b\}) = \left\lfloor \frac{n}{2} \right\rfloor .$$

Proof. By Lemma 22, if $b \in \left[\left\lfloor \frac{n}{4} \right\rfloor + 2, \left\lfloor \frac{n}{3} \right\rfloor - 1\right] \cup \left[\left\lfloor \frac{n}{3} \right\rfloor + 2, \left\lfloor \frac{n}{2} \right\rfloor - 1\right]$, then $order(\{0,1,b\}) \leq \left\lfloor \frac{n}{4} \right\rfloor + 2$. By Lemma 11, if $4 \leq b \leq n/4$, then $order(\{0,1,b\}) \leq \left\lfloor \frac{n}{4} \right\rfloor + 2$. By Lemma 14, $order\{0,1,\left\lfloor \frac{n}{4} \right\rfloor + 1\} = \left\lfloor \frac{n}{4} \right\rfloor + 2$. If $b = \left\lfloor \frac{n}{3} \right\rfloor$ and $n \not\equiv 0 \bmod 3$ then

$$order(\{0,1,b\}) = \begin{cases} order(1 + 3 * \{0,1,b\}) = order(\{0,1,4\}), & \text{if } n \equiv 1 \mod 3 \\ order(2 + 3 * \{0,1,b\}) = order(\{0,2,5\}), & \text{if } n \equiv 2 \mod 3 \end{cases},$$

and the result follows from Lemmas 26 and 27. Thus, i) follows. If $b \in \{3, \lfloor n/3 \rfloor + 1\}$ the result follows from Lemmas 14 and 16. If n is odd, then $order(\{0,1,\lfloor n/2 \rfloor\}) = order(1 + 2 * \{0,1,b\}) = \{0,1,3\}$ and the result follows from Lemma 16. If $n \equiv 0 \bmod 3$ and $b = n/3$, then, for $k \geq 1$, $kS = [0,k] \cup [n/3, n/3 + k - 1] \cup [2n/3, 2n/3 + k - 2]$ (in $\mathbb{Z}$). The order of S is the smallest positive integer k such that $k - 2 + 2n/3 \geq n - 1$, that is, $k = 1 + n/3$, completing the proof of ii). To prove iii), note that, if n is even and $b = n/2$, then, for $k \geq 1$, $kS = [0,k] \cup [n/2, n/2 + k - 1]$ (in $\mathbb{Z}$). Thus, the order of S is the smallest positive integer k such that $k - 1 + n/2 \geq n - 1$, that is, $order(S) = n/2$. If $b \in \{2, \lfloor n/2 \rfloor + 1\}$, the result follows from Lemmas 14 and 15. □

4 Proofs of the Main Results

In this section we prove our main results. To prove the first three results, we initially show that certain orders in each box are attained by giving examples of bases with such orders. Then, regarding the first two theorems, we prove that the remaining orders are not attained.

4.1 Proof of Theorem 6

In the next table, we give examples of bases attaining the orders in the second box according to Theorem 6. The results follow from Lemmas 15 and 17.

Second Box for $\mathbb{Z}_n$		
$n \equiv 0 \bmod 2$	$n \equiv 1 \bmod 2$	$Order(S)$
$S = \langle n/2 \rangle \cup (1 + \langle n/2 \rangle)$	—	$\lfloor n/2 \rfloor - 1$
$S = \{0,1,2\}$	$S = \{0,1,2\}$	$\lfloor n/2 \rfloor$

We now assume that $n \geq 17$ and n is odd, and show that there is no basis $S \subseteq \mathbb{Z}_n$ such that $order(S) = \lfloor n/2 \rfloor - 1$.

Assume that $S \subset \mathbb{Z}_n$ is a basis such that $order(S) = \lfloor n/2 \rfloor - 1$. By Lemma 10, $|S| \leq 3$. Note that, by definition of basis, $|S| \geq 2$ and, by Lemma 1, $|S| \neq 2$ if $order(S) \neq n-1$. Thus $|S| = 3$. Suppose $S = \{0, a, b\}$ where $a, b \in \mathbb{Z}_n$. If a had order $m \neq n$, then $3 \leq m < \lfloor n/2 \rfloor$, since n is odd. By Corollary 19, this would imply that $order(S) \leq m + n/m - 2 < \lfloor n/2 \rfloor - 1$, as $n \geq 17$. Therefore, a must have order n. Then, S has the same order as $a^{-1}S = \{0, 1, c\}$ for some $c \in \mathbb{Z}_n$. If $c > \lfloor n/2 \rfloor + 1$, then S has the same order as $1 - a^{-1}S = \{0, 1, d\}$ with $d \leq \lfloor n/2 \rfloor + 1$. Thus, we can assume that $c \leq \lfloor n/2 \rfloor + 1$. Now using Corollary 23, we get $order(S) \neq \lfloor n/2 \rfloor - 1$, a contradiction.

4.2 Proof of Theorem 7

The next table gives examples of bases attaining the conjectured orders in the third box according to Theorem 7. The results follow from Lemmas 15, 16, and 17.

Third Box for $\mathbb{Z}_n$			
$n \equiv 0$ mod 3	$n \equiv 1$ mod 3	$n \equiv 2$ mod 3	$Order(S)$
$S = \langle n/3 \rangle \cup (1 + \langle n/3 \rangle)$	—	—	$\lfloor n/3 \rfloor - 1$
$S = \{0, 1, 2, 3\}$	$S = \{0, 1, 2, 3\}$	—	$\lfloor n/3 \rfloor$
$S = \{0, 1, 3\}$	$S = \{0, 1, 3\}$	$S = \{0, 1, 3\}$	$\lfloor n/3 \rfloor + 1$

The fact that, for $n \geq 45$, $order(S) \neq \lfloor n/3 \rfloor - 1$, if $n \equiv 1$ mod 3, and $order(S) \notin \{\lfloor n/3 \rfloor - 1, \lfloor n/3 \rfloor\}$, if $n \equiv 2$ mod 3, follows from Lemma 24. Just note that, if $order(S) \in \{\lfloor n/3 \rfloor - 1, \lfloor n/3 \rfloor\}$, then, by Lemma 10, $|S| \leq 3$ if n is odd and $|S| \leq 4$ if n is even.

We note that the statement in the next lemma is stronger than what we need to prove Theorem 7. In particular, when n is odd, the case in which $|S| = 4$ needed not to be considered. However, the techniques we used for the purpose of the proof of Theorem 7 allowed us to get this result, which in turn is useful in the proof of Corollary 25.

Lemma 24. *Let $n \geq 45$ and suppose that 3 is not a divisor of n. Let S be a basis for $\mathbb{Z}_n$. If $|S| \leq 4$, then*

$$order(S) \leq \left\lfloor \frac{n}{4} \right\rfloor + 2 \qquad or \qquad order(S) \geq \lfloor n/3 \rfloor .$$

Moreover, if $order(S) = \lfloor n/3 \rfloor$ then $n \equiv 1$ mod 3.

Proof. Without loss of generality, assume $0 \in S$. Suppose that $n \neq 0$ mod 3. Since S is a basis, $|S| > 1$. If $|S| = 2$, then $order(S) = n - 1 > \lfloor n/3 \rfloor$. Suppose that $|S| = 3$ or $|S| = 4$. If S has an element whose order is not 1, 2, n/2 nor n, then, by Corollary 19, the result follows. Suppose that the order of the elements in S is $1, 2, n/2$, or n, where 2 and $n/2$ only occur when n is even. If S has an element of order 2, then the result follows from Corollary 20. If S does not contain an element of order 2, then necessarily it contains an element of order n. Moreover, by (1), if S has an element of order n, the basis S has the same order as some basis of the form $\{0,1,a,b\}$. If $|S|=3$, then we can assume that $S=\{0,1,a\}$, wit $1<a\leq \left\lfloor \frac{n}{2} \right\rfloor +1$. In this case, the result follows from Corollary 23. If $|S|=4$, assume that $S=\{0,1,a,b\}$ with $a\leq \left\lfloor \frac{n}{2} \right\rfloor +1$. Since for $S'\subset S$, $order(S)\leq order(S')$, we have

$$order(\{0,1,a,b\})\leq \min\{order(\{0,1,a\}), order(\{0,1,b\})\}. \tag{18}$$

Let

$$A_1=\{2,3,\left\lfloor \frac{n}{3} \right\rfloor +1, \left\lfloor \frac{n}{2} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor +1\}$$

and

$$A_2=\{2,3,\left\lfloor \frac{n}{3} \right\rfloor +1, \left\lfloor \frac{n}{2} \right\rfloor, \left\lfloor \frac{n}{2} \right\rfloor +1, 1-\left\lfloor \frac{n}{2} \right\rfloor, -\left\lfloor \frac{n}{3} \right\rfloor, -2, -1\}$$

Note that $-\left\lfloor \frac{n}{2} \right\rfloor \in A_2$. Also, $1-\lfloor n/2\rfloor \equiv \lfloor n/2\rfloor +1 \bmod n$, for n even. If $a\notin A_1$ or $b\notin A_2$ then, by Corollary 23 and taking into account (18),

$$order(\{0,1,a,b\})\leq \min\{order(\{0,1,a\}), order(\{0,1,b\})\}\leq \left\lfloor \frac{n}{4} \right\rfloor +2.$$

Recall that $order(\{0,1,1-b\})=order(\{0,1,b\})$. If $a\in A_1$ and $b\in A_2$, the result follows from Lemmas 29, 30, 31, 32 and 33.

□

The following result was presented in [6]. However, the authors leave most of the details of the proof to the reader and we do not see clearly that the result follows from their proof. For that reason and for completeness we are including it in this paper.

Corollary 25. *Let S be a basis for $\mathbb{Z}_n$. Then,*

$$order(S)\notin \left[\left\lfloor \frac{n}{4} \right\rfloor +3, \left\lfloor \frac{n}{3} \right\rfloor -2\right].$$

Proof. Note that, for $n<45$, the interval in the statement is empty. Assume that $n\geq 45$. Without loss of generality, suppose that $0\in S$. If $S\subset \mathbb{Z}_n$ is a basis such that $\lfloor n/4\rfloor +3\leq order(S)$, by Lemma 10, $|S|\leq 6$. Assume that $n\neq 0 \bmod 3$. If $|S|=5$ or $|S|=6$, by [1, Theorem 3.7], $order(S)\leq \lfloor n/4\rfloor +1$. If $|S|\leq 4$, by Lemma 24, $order(S)\leq \lfloor n/4\rfloor +2$ or $order(S)\geq \lfloor n/3\rfloor$.

Now assume that $n\equiv 0 \bmod 3$. If $|S|=3$, the result follows from Corollary 23. Suppose that $|S|\in\{4,5,6\}$. If $\lfloor n/4\rfloor +3\leq order(S)$, by Corollary 19, the order of the elements in S must be $1,2,3,n/2,n/3$, or n. First note that S contains, or has the same order as a basis which contains, an element of order 2, 3 or n. In fact, if $|S|=4$ and S does not have an element of order 2, 3 or n, then S has an element of order $n/2$ and an element of order $n/3$. Hence, $\{0,2a,3b\}\subseteq S$ for some $a,b\in\mathbb{Z}_n$. Since S is a basis, $3b-2a$ is not an element of order n/2 nor n/3 as, otherwise, 6 would divide $2a$ or $3b$ and all elements of S would be multiples of 2 or multiples of 3. Thus, S has the same order as $S-2a$, which has an element of order 2, 3 or n. A similar argument can be applied if $|S| = 5$ or $|S| = 6$. Thus, assume that S contains an element of order 2, 3 or n. If S contains an element of order 2 or 3, the result follows from Corollaries 20 and 21. Now suppose that S contains an element of order n and no elements of order 2 and 3. If either $n/3+1 \in S$ or n is even and $n/2+1 \in S$, then S can be transformed into a basis with the same order containing zero and an element of order 2 or 3 and we reduce the problem to the previous case. Let $A_1 = \{2, 3, \lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1\}$ and $A_2 = \{2, 3, \lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1, 1 - \lfloor n/2 \rfloor, -2, -1\}$. Assume that $S = \{0, 1, a, b, c, d\}$, with $a \leq \lfloor n/2 \rfloor + 1$ and $b = c = d$ if $|S| = 4$, and $c = d$ if $|S| = 5$. Note that if $S' \subset S$ then $order(S) \leq order(S')$. If $a \notin A_1$ or, b,c, or $d \notin A_2$ the result follows from Corollary 23. Suppose that $a \in A_1$, $b, c, d \in A_2$ and if a, b, c or $d \in \{\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1, 1 - \lfloor n/2 \rfloor\}$ then n is odd. If $|S| = 4$, the result follows from Lemmas 29, 30, 31, 32 and 33. If $|S| = 5$ or $|S| = 6$ the result follows from Remark 34 by noting that S has a subset of cardinality 4 containing 0 and 1 which is not one of the exceptional bases and, therefore, $order(S) \leq \lfloor n/4 \rfloor + 2$.

□

4.3 Proof of Theorem 8

The next table gives examples of bases attaining the orders in the fourth box of $\mathbb{Z}_n$ claimed in Theorem 8. The results follow from Lemmas 14, 15, 16, and 17.

Fourth Box for $\mathbb{Z}_n$				
$n \equiv 0 \bmod 4$	$n \equiv 1 \bmod 4$	$n \equiv 2 \bmod 4$	$n \equiv 3 \bmod 4$	$Order(S)$
$\langle n/4 \rangle \cup (1 + \langle n/4 \rangle)$	—	—	—	$\lfloor n/4 \rfloor - 1$
$\{0, 1, 2, 3, 4\}$	$\{0, 1, 2, 3, 4\}$	$\bigcup_{i=0}^{2} (i + \langle n/2 \rangle)$	—	$\lfloor n/4 \rfloor$
$\{0, 1, 2, 4\}$	$\{0, 1, 2, 4\}$	$\{0, 1, 2, 4\}$	$\{0,1,2,4\}$	$\lfloor n/4 \rfloor + 1$
$\{0, 1, (n/4) + 1\}$	$\{0, 1, \lfloor n/4 \rfloor + 1\}$	$\{0, 1, \lfloor n/4 \rfloor + 1\}$	$\{0, 1, \lfloor n/4 \rfloor + 1\}$	$\lfloor n/4 \rfloor + 2$

4.4 Proof of Theorem 9

If $n \leq 4$, the result follows from Table 1. Assume $n \geq 5$. Notice that $\mathbb{Z}_n$ is always a basis for $\mathbb{Z}_n$, which implies that $1 \in E_n$. Consider the set $S = \{0, 1, 2, ..., r-1, r+1\}$ with $2 \leq r \leq n-2$. By Lemma 16, $order(S) = \left\lceil \frac{n+1}{r+1} \right\rceil$. For all $r \geq \sqrt{n} - 1$

$$\frac{n+1}{r+1} - \frac{n+1}{r+2} = \frac{n+1}{(r+1)(r+2)} = \frac{n+1}{r^2+3r+2} \leq \frac{n+1}{n+\sqrt{n}} < 1.$$

It can be easily seen that, for positive real numbers a and b, $\lceil a \rceil - \lceil b \rceil \leq \lceil a - b \rceil$. Thus, $\left\lceil \frac{n+1}{r+1} \right\rceil - \left\lceil \frac{n+1}{r+2} \right\rceil \leq 1$ for all $r \geq \sqrt{n} - 1$, which implies that all integers from 2 to $\left\lceil \frac{n+1}{\lceil \sqrt{n} \rceil - 1 + 1} \right\rceil$ are attained orders. But $\left\lceil \frac{n+1}{\lceil \sqrt{n} \rceil} \right\rceil \geq \left\lceil \frac{n}{\lceil \sqrt{n} \rceil} \right\rceil \geq \lfloor \sqrt{n} \rfloor$ and the result follows.

References

[1] M.I. Bueno, S. Furtado, and N. Sherer, *Maximum exponent of Boolean circulant matrices with constant number of nonzero entries in its generating vector*. Electronic Journal of Combinatorics 16(2009), no. 1, Research Paper 66.

[2] M.I. Bueno and S. Furtado, *On the gaps in the set of exponents of boolean primitive circulant matrices*. Elect. Journal of Linear Algebra, 20 (2010), 640-660.

[3] W-S. Chou, B-S. Du, and P. J.-S. Shiue, *A note of circulant transition matrices in Markov chains*, Linear algebra and its applications, 429 (2008), 1699-1704.

[4] H. Daode, *On Circulant Boolean Matrices*, Linear Algebra and its Applications, 136(1990), 107-117.

[5] P. J. Davis, *Circulant Matrices*, Wiley-Interscience, NY, 1979.

[6] P. Dukes, P. Hegarty, and S. Herke, *On the possible orders of a basis for a finite cyclic group*, Electron. Journal of Combinatorics, 17(2010), no. 1, Paper R79.

[7] K. H. Kim-Buttler and J. R. Krabill, *Circulant Boolean relation matrices*, Czechoslovak Math. J. 24(1974), 247-251.

[8] B. Klopsch and V. F. Lev, *Generating Abelian Groups by Addition Only*, Forum Math. 21 (2009), 23-41.

[9] P. Lancaster, *Theory of Matrices*, Academic press, NY, 1969.

[10] S. Schwarz, *Circulant Boolean relation matrices*, Czechoslovak Math. J. 24(1974), 252-253.

[11] J.Z. Wang and J. X. Meng, *The exponent of the primitive Cayley digraphs on finite Abelian groups*, Discrete Appl. Math., 80(1997), 177-191.

A Gallery of bases and their orders.

Lemma 26. *For $n \geq 6$, order$(\{0,1,4\}) = \lfloor n/4 \rfloor + 2$.*

Proof. Let $S = \{0,1,4\}$. It can be shown by induction on k that in $\mathbb{Z}$, for all $k \geq 2$,

$$kS = [0, 4k-6] \cup [4k-4, 4k-3] \cup \{4k\}.$$

Let $q = \lfloor n/4 \rfloor$. Then,

$$(q+1)S = [0, 4q-2] \cup [4q, 4q+1] \cup \{4q+4\} \quad \text{and} \quad [0, 4q+2] \subseteq (q+2)S.$$

Note that, as $n \geq 6$, $4q+4 \neq 4q-1 \pmod{n}$. Thus, $(q+1)S \neq \mathbb{Z}_n \pmod{n}$. On the other hand, $4q+2 \geq n-1$. Thus, the result follows.

□

Lemma 27. *For $n \geq 6$, order$(\{0,2,5\}) \leq \lfloor n/5 \rfloor + 3$.*

Proof. Let $S = \{0, 2, 5\}$. It can be shown by induction on k that in $\mathbb{Z}$, for all $k \geq 2$,

$$kS = \{0, 2\} \cup [4, 5k - 8] \cup [5k - 6, 5k - 5] \cup \{5k - 3, 5k\}.$$

Let $q = \lfloor n/5 \rfloor$. Then,

$$\{0, 2\} \cup [4, 5q + 7] \subseteq (q + 3)S.$$

Since $5q + 7 \geq n + 3$, the result follows. □

Lemma 28. *For $n \geq 4$, order$(\{0, 2, 3, 4\}) = \lfloor n/4 \rfloor + 1$.*

Proof. Let $S = \{0, 2, 3, 4\}$. By induction on k, it can be shown that $kS = \{0\} \cup [2, 4k]$, $k \geq 1$. Let $q = \lfloor n/4 \rfloor$. Since $4q \leq n$, then $1 \notin qS \pmod n$. On the other hand, $4(q+1) \geq n + 1$. Thus, the result follows. □

Bases of the form $\{0, 1, 2, a\}$

Lemma 29. *Let $n \geq 21$. Let $a \in \{3, \lfloor n/3 \rfloor + 1, \lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1, 1 - \lfloor n/2 \rfloor, -\lfloor n/3 \rfloor, -2, -1\}$ and $S = \{0, 1, 2, a\}$. Then,*

$$\mathit{order}(S) \leq \lfloor n/4 \rfloor + 2 \quad \mathit{or} \quad \mathit{order}(S) \geq \lfloor n/3 \rfloor - 1.$$

Moreover, if $n \equiv 1$ mod 3, then order$(S) \neq \lfloor n/3 \rfloor - 1$ and if $n \equiv 2$ mod 3, then order$(S) \notin \{\lfloor n/3 \rfloor - 1, \lfloor n/3 \rfloor\}$.

Proof. Case 1: If $a \in \{3, -1\}$, then the basis S has the same order as $\{0, 1, 2, 3\}$ and the result follows by Lemma 15.

Case 2: If $a = -2$, then S has the same order as $2 + S = \{0, 2, 3, 4\}$ and the result follows from Lemma 28.

Case 3: Suppose that $a \in \{\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1, 1 - \lfloor n/2 \rfloor\}$. Assume n is even. Note that $1 - \lfloor n/2 \rfloor = \lfloor n/2 \rfloor + 1$. In this case, S contains an element of order 2 or it has the same order as a basis containing 0 and an element of order 2. Thus, the result follows from Corollary 20. Assume n is odd. Then,

$$\mathit{order}(\{0, 1, 2, \lfloor n/2 \rfloor\}) = \mathit{order}(\{0, 1, 3, 5\}) \leq \mathit{order}(\{0, 1, 5\}),$$

and

$$\mathit{order}(\{0, 1, 2, \lfloor n/2 \rfloor + 1\}) = \mathit{order}(\{0, 1, 2, 4\}) \leq \mathit{order}(\{0, 1, 4\}).$$

In both cases, $\mathit{order}(S) \leq \lfloor n/4 \rfloor + 2$ by Corollary 23. Also,

$$\mathit{order}(\{0, 1, 2, \lfloor n/2 \rfloor + 2\}) = \mathit{order}(\{0, 2, 3, 4\}) \leq \lfloor n/4 \rfloor + 2$$

by Lemma 28. Note that $1 - \lfloor n/2 \rfloor = \lfloor n/2 \rfloor + 2$.

Case 4: Suppose that $a \in \{-\lfloor n/3 \rfloor, \lfloor n/3 \rfloor + 1\}$. If $n \equiv 0$ mod 3, then S contains an element of order 3 or it has the same order as a basis containing 0 and an element of order

3. Thus, the result follows from Corollary 21. Let $n \equiv 1 \bmod 3$. If $a = -\lfloor n/3 \rfloor$, then $3 * S = \{0, 1, 3, 6\}$ and

$$order(S) = order(3 * S) \leq order(\{0, 1, 6\});$$

if $a = \lfloor n/3 \rfloor + 1$, then $3 * S - 2 = \{0, 1, 4, -2\}$ and

$$order(S) = order(3 * S - 2) \leq order(\{0, 1, 4\}).$$

In both cases, $order(S) \leq \lfloor n/4 \rfloor + 2$ by Corollary 23. If $n \equiv 2 \bmod 3$, then

$$order(\{0, 1, 2, -\lfloor n/3 \rfloor\}) = order(\{0, 1, 4, -2\})$$

and

$$order(\{0, 1, 2, \lfloor n/3 \rfloor + 1\}) = order(\{0, 1, 3, 6\}),$$

and the result follows as before. □

Bases of the form $\{0, 1, 3, a\}$

Lemma 30. *Let* $n \geq 30$. *Let* $a \in \{\lfloor n/3 \rfloor + 1, \lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1, 1 - \lfloor n/2 \rfloor, -\lfloor n/3 \rfloor, -2, -1\}$ *and* $S = \{0, 1, 3, a\}$. *Then,*

$$order(S) \leq \left\lfloor \frac{n}{4} \right\rfloor + 2 \quad or \quad order(S) \geq \left\lfloor \frac{n}{3} \right\rfloor - 1.$$

Moreover, if $n \equiv 1$ *mod 3, then* $order(S) \neq \lfloor n/3 \rfloor - 1$ *and if* $n \equiv 2$ *mod* 3, *then* $order(S) \notin \{\lfloor n/3 \rfloor - 1, \lfloor n/3 \rfloor\}$.

Proof. Case 1: If $a = -1$, then $order(S) = order\{0, 1, 2, 4\} \leq \lfloor n/4 \rfloor + 2$ by Corollary 23.

Case 2: If $a = -2$, then $order(S) = order(\{0, 2, 3, 5\}) \leq \lfloor n/4 \rfloor + 2$ by Lemma 27.

Case 3: Suppose that $a \in \{\lfloor n/3 \rfloor + 1, -\lfloor n/3 \rfloor\}$. If $n \equiv 0 \bmod 3$, then S contains an element of order 3 or it has the same order as a basis containing 0 and an element of order 3. Thus, the result follows from Corollary 21. If either $a = \lfloor n/3 \rfloor + 1$ and $n \equiv 1 \bmod 3$ or $a = -\lfloor n/3 \rfloor$ and $n \equiv 2 \bmod 3$, we have

$$order(S) = order(\{0, 2, 3, 9\}) = order(\{-2, 0, 1, 7\}) \leq order(\{0, 1, 7\});$$

if either $a = \lfloor n/3 \rfloor + 1$ and $n \equiv 2 \bmod 3$ or $a = -\lfloor n/3 \rfloor$ and $n \equiv 1 \bmod 3$, we have

$$order(S) = order(\{0, 1, 3, 9\}) \leq order(\{0, 1, 9\}).$$

In both cases, by Corollary 23, $order(S) \leq \lfloor n/4 \rfloor + 2$.

Case 4: Suppose that $a \in \{\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1, 1 - \lfloor n/2 \rfloor\}$. Assume n is even. In this case, S contains an element of order 2 or it has the same order as a basis containing 0 and an element of order 2. Thus, the result follows from Corollary 20. Assume n is odd. Then,

$$order(\{0, 1, 3, \lfloor n/2 \rfloor\}) = order(\{0, 1, 3, 7\}) \leq order(\{0, 1, 7\}),$$

$$order(\{0,1,3,\lfloor n/2\rfloor+1\}) = order(\{0,1,2,6\}) \leq \ order(\{0,1,6\}),$$

and

$$\begin{aligned} order(\{0,1,3,1-\lfloor n/2\rfloor\}) = order(0,2,3,6\}) = order(\{-2,0,1,4\}) \leq \\ \leq order(\{0,1,4\}). \end{aligned}$$

In any case, by Corollary 23, $order(S) \leq \lfloor n/4\rfloor + 2$.

□

Bases of the form $\{0, 1, \left\lfloor \frac{n}{3} \right\rfloor + 1, a\}$

Lemma 31. *Let $n \geq 30$. Let $a \in \left\{\left\lfloor \frac{n}{2}\right\rfloor, \left\lfloor \frac{n}{2}\right\rfloor + 1, 1 - \left\lfloor \frac{n}{2}\right\rfloor, -\left\lfloor \frac{n}{3}\right\rfloor, -2, -1\right\}$ and $S = \{0, 1, \left\lfloor \frac{n}{3}\right\rfloor + 1, a\}$. Then,*

$$order(S) \leq \left\lfloor \frac{n}{4}\right\rfloor + 2 \quad or \quad order(S) \geq \left\lfloor \frac{n}{3}\right\rfloor - 1.$$

Moreover, if $n \equiv 1$ mod 3, then $order(S) \neq \lfloor n/3\rfloor - 1$ and if $n \equiv 2$ mod 3, then $order(S) \notin \{\lfloor n/3\rfloor - 1, \lfloor n/3\rfloor\}$.

Proof. If $n \equiv 0$ mod 3, then S contains an element of order 3 or it has the same order as a basis containing 0 and an element of order 3. Thus, the result follows from Corollary 21. Now assume $n \not\equiv 0$ mod 3.

Case 1: Suppose that n is even and $a \in \{n/2, n/2+1, 1-n/2\}$. Then S contains (or can be transformed into a basis of the same order with) 0 and an element of order 2, which, by Corollary 20, implies the result.

Case 2: Suppose that either $a \in \{-2, -1, -\lfloor n/3\rfloor\}$ or n is odd and $a \in \{\lfloor n/2\rfloor, \lfloor n/2\rfloor + 1, 1 - \lfloor n/2\rfloor\}$.

Subcase 2.1. Suppose that $n \equiv 1$ mod 3. Then, $3 * S = \{0, 2, 3, 3a\}$. If $a = -\lfloor n/3\rfloor$, then $3a = 1$ and, by Lemma 15, $order(S) = \lfloor n/3\rfloor$. If $a \in \{-2, -1\}$, then

$$\begin{aligned} order(S) &= order(3 * S - 2) = order(\{0,1,3a-2,-2\}) \leq order(\{0,1,3a-2\}) \\ &= order(\{0,1,3-3a\}); \end{aligned}$$

if n is odd and $a \in \{\lfloor n/2\rfloor, \lfloor n/2\rfloor + 2\}$, then $3a \in \{\lfloor n/2\rfloor - 1, \lfloor n/2\rfloor + 5\}$ and

$$\begin{aligned} order(S) &= order(3 * S - 2) = order(\{0,1,3a-2,-2\}) \\ &\leq order(\{0,1,3a-2\}). \end{aligned}$$

In both cases, $order(S) \leq \lfloor n/4\rfloor + 2$ by Corollary 23. Note that for $3a = \lfloor n/2\rfloor + 5$, $order(\{0,1,3a-2\}) = order(\{0,1,\lfloor n/2\rfloor - 1\})$. If $a = \lfloor n/2\rfloor + 1$, then

$$\begin{aligned} order(S) &= order(6 * S - 3) = order(\{0,1,3,-3\}) \leq order(\{0,1,-3\}) \\ &= order(\{0,1,4\}) \leq \lfloor n/4\rfloor + 2, \end{aligned}$$

by Corollary 23.

Subcase 2.2. Suppose that $n \equiv 2 \bmod 3$. Then, $3 * S = \{0, 1, 3, 3a\}$. If $a = -\lfloor n/3 \rfloor$, then $3a = 2$ and, by Lemma 15, $order(S) = \lfloor n/3 \rfloor + 1$. If $a \in \{-2, -1\}$, then

$$\begin{aligned} order(S) &= order(3 * S) = order(\{0, 1, 3, 3a\}) \leq order(\{0, 1, 3a\})\} \\ &= order(\{0, 1, 1 - 3a\}); \end{aligned}$$

if n is odd and $a \in \{\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 2\}$, then $3a \in \{\lfloor n/2 \rfloor - 1, \lfloor n/2 \rfloor + 5\}$ and

$$order(S) = order(\{0, 1, 3, 3a\}) \leq order(\{0, 1, 3a\}).$$

In both cases, $order(S) \leq \lfloor n/4 \rfloor + 2$ by Corollary 23. Note that, for $3a = \lfloor n/2 \rfloor + 5$, $order(\{0, 1, 3a\}) = order(\{0, 1, \lfloor n/2 \rfloor - 3\})$. If $a = \lfloor n/2 \rfloor + 1$, then $3a = \lfloor n/2 \rfloor + 2$ and

$$\begin{aligned} order(S) &= order(\{0, 1, 3, \lfloor n/2 \rfloor + 2\}) = order(\{0, 2, 3, 6\}) \\ &= order(\{-2, 0, 1, 4\}) \leq order(\{0, 1, 4\}) \leq \lfloor n/4 \rfloor + 2, \end{aligned}$$

by Corollary 23. □

Bases of the form $\{0, 1, \left\lfloor \frac{n}{2} \right\rfloor, a\}$

Lemma 32. *Let* $n \geq 22$. *Let* $a \in \{\lfloor n/2 \rfloor + 1, 1 - \lfloor n/2 \rfloor, -\lfloor n/3 \rfloor, -2, -1\}$ *and* $S = \{0, 1, \lfloor n/2 \rfloor, a\}$. *Then,*

$$order(S) \leq \left\lfloor \frac{n}{4} \right\rfloor + 2 \quad or \quad order(S) \geq \lfloor n/3 \rfloor - 1.$$

Moreover, if $n \equiv 1$ *mod 3, then* $order(S) \neq \lfloor n/3 \rfloor - 1$ *and if* $n \equiv 2$ *mod* 3, *then* $order(S) \notin \{\lfloor n/3 \rfloor - 1, \lfloor n/3 \rfloor\}$.

Proof. If n is even, then S contains an element of order 2 and the result follows from Corollary 20. Now suppose that n is odd. Note that $2 * S + 1 = \{0, 1, 3, 2a + 1\}$.

For $a = -1$, $order(S) = order(\{0, 1, 3, -1\}) = order(\{0, 1, 2, 4\}) \leq \lfloor n/4 \rfloor + 2$, by Corollary 23.

For $a = -\lfloor n/3 \rfloor$ and $n \equiv 0 \bmod 3$, S contains an element of order 3 and the result follows from Corollary 23.

For $a = \lfloor n/2 \rfloor + 1$, $order(S) = order(2 * S + 1) = \{0, 1, 2, 3\}$ and the result follows from Lemma 15.

Now suppose that a does not satisfy the previous cases. We have $order(S) = order(\{0, 1, 3, b\})$, with $b \in \{4, \lfloor n/3 \rfloor + t + 1, -3\}$, where $0 < t = n - 3\lfloor n/3 \rfloor \leq 2$. Thus,

$$order(S) \leq order(\{0, 1, b\}) \leq \lfloor n/4 \rfloor + 2$$

by Corollary 23. □

Bases of the form $\{0, 1, \left\lfloor \frac{n}{2} \right\rfloor + 1, a\}$

Lemma 33. *Let $n \geq 21$. Let $a \in \{1 - \lfloor n/2 \rfloor, -\lfloor n/3 \rfloor, -2, -1\}$ and $S = \{0, 1, \lfloor n/2 \rfloor + 1, a\}$. Then,*

$$order(S) \leq \left\lfloor \frac{n}{4} \right\rfloor + 2 \quad or \quad order(S) \geq \lfloor n/3 \rfloor - 1.$$

Moreover, if $n \equiv 1$ mod 3, then $order(S) \neq \lfloor n/3 \rfloor - 1$ and if $n \equiv 2 \bmod 3$, then $order(S) \notin \{\lfloor n/3 \rfloor - 1, \lfloor n/3 \rfloor\}$.

Proof. If n is even, then S has the same order as $S - 1$, which contains 0 and an element of order 2. Thus, the result follows from Corollary 20. Now suppose that n is odd. Then, $order(S) = order(\{0, 1, 2, 2a\})$.

If $a = 1 - \lfloor n/2 \rfloor = \lfloor n/2 \rfloor + 2$, then $2a = 3$ and the result follows from Lemma 15.

If $a = -2$, then $2a = -4$ and, by Corollary 23,

$$order(S) \leq order(\{0, 1, -4\}) = order(\{0, 1, 5\}) \leq \lfloor n/4 \rfloor + 2.$$

If $a = -1$, then $2a = -2$ and, by Lemma 28, $order(S) = order(\{0, 2, 3, 4\}) \leq \lfloor n/4 \rfloor + 2$.

Suppose that $a = -\lfloor n/3 \rfloor$. If $n \equiv 0$ mod 3, then S contains 0 and an element of order 3 and the result follows from Corollary 21. If $n \equiv 1$ mod 3, then $S = \{0, 1, 2, \lfloor n/3 \rfloor + 1\}$ and the result follows from Lemma 29. If $n \equiv 2$ mod 3, then, by Corollary 23,

$$order(S) = order(\{0, 1, 2, \lfloor n/3 \rfloor + 2\}) \leq order(\{0, 1, \lfloor n/3 \rfloor + 2\}) \leq \lfloor n/4 \rfloor + 2.$$

□

Remark 34. *Suppose that $S = \{0, 1, a, b\}$, with $a \in \{2, 3, \lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1\}$ and $b \in \{2, 3, \lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1, 1 - \lfloor n/2 \rfloor, -2, -1\}$, where n is odd if a or $b \in \{\lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1, -\lfloor n/2 \rfloor\}$. From the proofs of Lemmas 29, 30, 31, 32 and 33, we get that $order(S) \leq \lfloor n/4 \rfloor + 2$ if S is not one of the next exceptional bases:*

$$\{0, 1, 2, 3\}, \quad \{0, 1, 2, -1\}, \quad \{0, 1, \lfloor n/2 \rfloor, \lfloor n/2 \rfloor + 1\}, \quad \{0, 1, \lfloor n/2 \rfloor + 1, 1 - \lfloor n/2 \rfloor\}.$$

Note that all of them have the same order as $\{0, 1, 2, 3\}$.