

involve

a journal of mathematics

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

Maria Isabel Bueno, Kuan-Ying Fang,
Samantha Fuller and Susana Furtado



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

Maria Isabel Bueno, Kuan-Ying Fang,
 Samantha Fuller and Susana Furtado

(Communicated by Joseph Gallian)

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 $[\frac{n}{2} + 1, n - 2]$, $[\frac{n}{3} + 2, \frac{n}{2} - 2]$ and $[\frac{n}{4} + 3, \frac{n}{3} - 2]$ 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 i -th gap depend on the value of $n \bmod i$.

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 $0 \leq i \leq n - 2$, $0 \leq j \leq n - 1$, 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 $|C_n| = 2^n$ [Davis 1979; Lancaster 1969]. This semigroup

MSC2010: 05C25, 05C50, 11P70.

Keywords: exponent, primitive circulant matrix, basis of a cyclic group, order, box.

Bueno was supported by Dirección General de Investigación (Ministerio de Ciencia y Tecnología) of Spain under grant MTM2009-09281 and NSF grant DMS-0852065. Fang and Fuller were supported by NSF Grant DMS-0852065 for the REU program at the University of California, Santa Barbara. Furtado's contribution was done within the activities of Centro de Estruturas Lineares e Combinatórias da Universidade de Lisboa.

was thoroughly investigated by K. K.-H. Butler and J. R. Krabill [1974] and by S. Schwarz [1974].

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 [Bueno et al. 2009] 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 $\text{Cay}(\mathbb{Z}_n, S)$. The vertex set of this graph is \mathbb{Z}_n and there is an arc from u to $u + a \pmod{n}$ 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

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

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 $\text{order}(S)$. It is well known [Butler and Krabill 1974; Schwarz 1974] that the set $S = \{s_0, s_1, \dots, s_r\} \subset \mathbb{Z}_n$ is a basis if and only if $\gcd(s_1 - s_0, \dots, s_r - s_0, n) = 1$. In [Bueno et al. 2009] 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 $\exp(C) = \text{order}(S)$. 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. We note that all the results in this paper will be given in terms of bases for \mathbb{Z}_n , as the techniques we can use following this approach result more convenient.

The problem we study in this paper has applications in different areas. In particular, circulant matrices appear as transition matrices in Markov processes

[Chou et al. 2008]. Also, the problem stated in terms of bases for \mathbb{Z}_n has applications in coding theory and quantum information [Klopsch and Lev 2009].

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 [Huang 1990; Wang and Meng 1997]. *If C is a primitive circulant matrix, then its exponent is either $n - 1$, $\lfloor \frac{n}{2} \rfloor$, $\lfloor \frac{n}{2} \rfloor - 1$ or does not exceed $\lfloor \frac{n}{3} \rfloor + 1$. 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 [Dukes et al. 2010]. *For every $n \geq 3$, the sets $\lfloor \frac{n}{4} \rfloor + 3$, $\lfloor \frac{n}{3} \rfloor - 2$ and E_n are disjoint.*

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 [Bueno et al. 2009] 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. 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 3. *If $C \in C_n$ is primitive, then*

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

In [Dukes et al. 2010], 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 3 produces gaps in the set of exponents which are larger than the ones encountered in [Dukes et al. 2010]. In fact, we have shown that the gaps in our conjecture should be maximal [Bueno and Furtado 2010]. We say that a gap A in E_n is maximal if $A' \cap E_n \neq \emptyset$ for any interval of integers $A' \subset [1, n - 1]$, with A strictly contained in A' . In [Bueno and Furtado 2010], we proved that for each positive integer j , there is an integer n , such that $B_{j,n}$ is a maximal gap in

E_n . However, as stated in [Dukes et al. 2010], we remain far from a complete characterization of the possible exponents of $n \times n$ primitive circulant matrices.

Lemmas 1 and 2 above 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 present the distribution of orders of bases within the first three boxes by showing what orders are attained and which ones are not. The results for the first and second box were already known [Huang 1990; Wang and Meng 1997] and we include them for completeness. 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 [Huang 1990; Wang and Meng 1997] 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 4 [Huang 1990]. *For all n ,*

$$B_1 \subseteq E_n.$$

Concerning the second box, we have the following result obtained in [Huang 1990; Wang and Meng 1997]. In Section 4.1 we include a proof of it using the techniques for bases.

Theorem 5 [Huang 1990; Wang and Meng 1997]. *Let $n \geq 17$ be a positive integer:*

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

The next two theorems are our main results and will be proven in Section 4. In our first result 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 $n \equiv 0 \pmod j$, $j = 3, 4$, B_j is a subset of E_n , for all n .

Theorem 6. *Let $n \geq 45$ be a positive integer.*

- *If $n \equiv 0 \pmod 3$, then $B_3 \subseteq E_n$.*
- *If $n \equiv 1 \pmod 3$, then $B_3 \cap E_n = \{\lfloor \frac{n}{3} \rfloor + 1, \lfloor \frac{n}{3} \rfloor\}$.*
- *If $n \equiv 2 \pmod 3$, then $B_3 \cap E_n = \{\lfloor \frac{n}{3} \rfloor + 1\}$.*

Theorem 7. *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 $\{\lfloor \frac{n}{4} \rfloor + 2, \lfloor \frac{n}{4} \rfloor + 1, \lfloor \frac{n}{4} \rfloor\} \subseteq E_n$.*
- *If $n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$, then $\{\lfloor \frac{n}{4} \rfloor + 2, \lfloor \frac{n}{4} \rfloor + 1\} \subseteq E_n$.*

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

In Tables 1 and 2 we give the exact orders attained by bases for \mathbb{Z}_n with $n = 2, 3, 4, \dots, 104$. As the numerical experiments show, for each n there is a number of

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, 17, 18, 19, 26, 27, 53
13	1...6, 12	34	1...12, 16, 17, 33	55	1...15, 18, 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, 18, 19, 20, 28, 56
16	1...8, 15	37	1...13, 18, 36	58	1...16, 19, 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 .

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, 96
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 .

consecutive orders that can be attained by bases of \mathbb{Z}_n . Though we prove Theorem 8, according to our numerical experiments, we conjecture that at least all consecutive integers up to $2\sqrt{n} - 2$ are attainable orders.

Theorem 8. *Let n be a positive integer. Then $[1, \lfloor \sqrt{n} \rfloor] \subseteq E_n$.*

Though this result is cited in [Dukes et al. 2010], it seems that the paper where its proof is said to be is not available.

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

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

where $b*S = \{bs \bmod n : s \in S\}$. 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 9 [Klopsch and Lev 2009]. *Let $n \in \mathbb{N}$ and $\rho \in [2, n - 1]$. Let S be a basis for \mathbb{Z}_n such that $\text{order}(S) \geq \rho$. 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 $\text{order}(S) \geq \frac{n}{k}$ and $n \gg 0$, 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 10 [Bueno and Furtado 2010]. *Let $2 \leq b \leq n - 1$. Then*

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

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 j -th box, $j \leq \sqrt{n}$, belongs to E_n for all n .

Lemma 11 [Bueno et al. 2009]. *For $j \in \{1, 2, \dots, \lfloor \sqrt{n} \rfloor\}$,*

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

Lemma 12 [Bueno and Furtado 2010]. *Let $2 \leq j \leq \sqrt{n}$ be a positive integer. Then*

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

Lemma 13 [Bueno et al. 2009]. *Let $2 \leq r \leq n - 1$ and $t = n - r \lfloor \frac{n}{r} \rfloor$. Then*

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

Lemma 14. *Let $2 \leq r \leq n - 2$. Then*

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

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

Lemma 15. *Suppose that m is a divisor of n and let $1 \leq q < m \leq n$. Then*

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

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

As a consequence of the previous result, we obtain that, if j is a divisor of n , the smallest element of the j -th box is an element of E_n , since

$$\text{order} (\langle n/j \rangle \cup (1 + \langle n/j \rangle)) = n/j - 1.$$

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 $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_{n/m}$. We denote by $\text{order}_n(S)$ the order of the basis S as a subset of \mathbb{Z}_n . The next result is well known. For that reason, we include it without proof.

Lemma 16. *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*

$$\text{order}_{n/m}(\phi(S)) \leq \text{order}_n(S) \leq \text{order}_{n/m}(\phi(S)) + m - 1.$$

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

Corollary 1 [Huang 1990]. *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 $\text{order}(S) \leq (n/m) + m - 2$.*

Corollary 2. *Let S be a basis for \mathbb{Z}_n and assume that S contains zero and an element of order 2. Then $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 1$ or $\text{order}(S) \geq \lfloor \frac{n}{2} \rfloor - 1$.*

Corollary 3. *Let S be a basis for \mathbb{Z}_n and assume that S contains zero and an element of order 3. Then $\text{order}(S) \leq \lfloor \frac{n}{6} \rfloor + 2$ or $\text{order}(S) \geq \lfloor \frac{n}{3} \rfloor - 1$.*

The next technical lemma allows us to prove Corollary 4, which is a key result in the proof of our main theorems.

Lemma 17. *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

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

Proof. Let $S = \{0, 1, b\}$. First we observe that $j+1 < (j+1)b - n < b$. We 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

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

The inequality on the left follows from Corollary 1 while the right inequality follows after a few computations. Thus,

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

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

$$\bigcup_{i=0}^q [ip, ip+(q-i)k] \cup [b, b+qk-1] \subset qkS \tag{2}$$

and

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

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 $q \geq 2$. Also, the gaps between consecutive intervals in the unions in (2) and (3) have at most $l-1$ elements. Thus, we have

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

Moreover, $[0, jb+(q-1)p+l+j-1] \subseteq (qk+l-1+(j-1))S$. Since $n-jb = b-p$, we get that $(q-1)p+l+j \geq n-jb$ is equivalent to $l+j \geq b-qp$, which is true because of the definition of l . This implies

$$\text{order}(S) \leq qk + \max\{b-pq, p-k\} + j - 2. \tag{4}$$

Let $b = pq+r$, $0 \leq r < p$ and $q_1 = \lfloor rk/p \rfloor$. It is easy to show that

$$\max\{b-pq, p-k\} \leq q_1 + p - k \tag{5}$$

which implies

$$\text{order}(S) \leq \left\lfloor \frac{bk}{p} \right\rfloor + p - k + j - 2. \tag{6}$$

Taking into account (6), to complete the proof it is sufficient to show that

$$\left\lfloor \frac{bk}{p} \right\rfloor + p - k + j - 2 \leq \left\lfloor \frac{n}{j+2} \right\rfloor + j. \tag{7}$$

Let g be the function given by

$$g(b) = \frac{bk}{p} + p - 3 = \frac{n}{p} + p - 2.$$

To see that (7) holds it is enough to note that $g(b) \leq \frac{n}{j+2} + j$, or, equivalently,

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

Case 3: Assume $(j+1)b - n > b/2$. Note that $j = \lfloor \frac{n}{b} \rfloor$. 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

$$[0, qj+1] \cup \bigcup_{i=0}^{q-1} [b - (q-i)r_3, b - (q-i)r_3 + ij] \cup [b, b+qj] \subset (qj+1)S \quad (8)$$

Denote by q the largest integer such that $qj+2 \leq b - qr_3$, that is, $q = \left\lfloor \frac{b-2}{j+r_3} \right\rfloor$. An argument similar to Case 2 implies that

$$\text{order}(S) \leq qj + \max\{r_3, b - q(j+r_3) - 1\} + j - 1. \quad (9)$$

Let $l = \max\{r_3, b - q(j+r_3) - 1\}$. Now we show that

$$qj + l + j - 1 \leq \left\lfloor \frac{j(b-1)}{j+r_3} \right\rfloor + j + r_3 - 1 \leq \left\lfloor \frac{n}{j+2} \right\rfloor + j. \quad (10)$$

To see the first inequality in (10), 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 (10), 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 $j+n-jb = \lfloor \frac{n}{j+2} \rfloor + 1$, we get $\lfloor h(b) \rfloor = \lfloor \frac{n}{j+2} \rfloor + j$, since by [Bueno and Furtado 2010, Theorem 5.7], and taking into account that $j < \sqrt{n}$,

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

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

$$b \in \left[\frac{n + j - 1 - \frac{n}{j+2}}{j}, \frac{n - 2}{j} \right], \tag{11}$$

then the second inequality in (10) holds. We finish the proof by showing that any b satisfying our assumptions is such that (11) holds. Note that, as $(j + 1)b - n > \frac{b}{2}$, we have $2n / (2j + 1) < b \leq \lfloor \frac{n}{j} \rfloor - 1$. Thus, because $j \geq 2$, it follows that $b \leq \frac{n}{j} - 1 \leq \frac{n-2}{j}$. First we note that if $|I_j| \geq 2$, then

$$\frac{n + j - 1 - \frac{n}{j+2}}{j} \leq \frac{2n}{2j + 1} < b. \tag{12}$$

If $|I_j| = 1$, then $b = \lfloor n/j \rfloor - 1$. If (12) holds, we are done. Otherwise, it can be proven that

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

From the previous lemma we obtain the next corollary, which includes some results presented in [Dukes et al. 2010] without proof.

Corollary 4. *Let $n \geq 16$. Suppose that $2 \leq b \leq \lfloor \frac{n}{2} \rfloor + 1$.*

- (i) *If either $b \notin \{2, 3, \lfloor \frac{n}{3} \rfloor, \lfloor \frac{n}{3} \rfloor + 1, \lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor + 1\}$, or $b = \lfloor \frac{n}{3} \rfloor$ and $n \not\equiv 0 \pmod 3$, then $\text{order}(\{0, 1, b\}) \leq \lfloor \frac{n}{4} \rfloor + 2$.*
- (ii) *If either $b \in \{3, \lfloor \frac{n}{3} \rfloor + 1\}$, or $b = \lfloor \frac{n}{3} \rfloor$ and $n \equiv 0 \pmod 3$, or $b = \lfloor \frac{n}{2} \rfloor$ with n odd, then $\text{order}(\{0, 1, b\}) = \lfloor \frac{n}{3} \rfloor + 1$.*
- (iii) *If either $b \in \{2, \lfloor \frac{n}{2} \rfloor + 1\}$, or $b = \lfloor \frac{n}{2} \rfloor$ and n is even, then $\text{order}(\{0, 1, b\}) = \lfloor \frac{n}{2} \rfloor$.*

Proof. By Lemma 17, if $b \in [\lfloor \frac{n}{4} \rfloor + 2, \lfloor \frac{n}{3} \rfloor - 1] \cup [\lfloor \frac{n}{3} \rfloor + 2, \lfloor \frac{n}{2} \rfloor - 1]$, the order of $\{0, 1, b\}$ is at most $\lfloor \frac{n}{4} \rfloor + 2$. By Lemma 10, if $4 \leq b \leq n/4$, then $\text{order}(\{0, 1, b\}) \leq \lfloor \frac{n}{4} \rfloor + 2$. By Lemma 12, $\text{order}(\{0, 1, \lfloor \frac{n}{4} \rfloor + 1\}) = \lfloor \frac{n}{4} \rfloor + 2$. If $b = \lfloor \frac{n}{3} \rfloor$ and $n \not\equiv 0 \pmod 3$ then

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

and the result follows from Lemmas 19 and 20. Thus, (i) follows. If $b \in \{3, \lfloor \frac{n}{3} \rfloor + 1\}$ the result follows from Lemmas 12 and 14. If n is odd, then

$$\text{order}(\{0, 1, \lfloor \frac{n}{2} \rfloor\}) = \text{order}(1 + 2 * \{0, 1, b\}) = \{0, 1, 3\}$$

and the result follows from Lemma 14. If $n \equiv 0 \pmod 3$ 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, $k = 1 + n/3$, which completes 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, $\text{order}(S) = n/2$. If $b \in \{2, \lfloor \frac{n}{2} \rfloor + 1\}$, the result follows from Lemmas 12 and 13. \square

4. Proofs of the main results

In this section we prove Theorems 5, 6, 7, and 8. 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 5. In the next table, we give examples of bases attaining the orders in the second box according to Theorem 5. The results follow from Lemmas 13 and 15.

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

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 $\text{order}(S) = \lfloor \frac{n}{2} \rfloor - 1$.

Assume that $S \subset \mathbb{Z}_n$ is a basis such that $\text{order}(S) = \lfloor \frac{n}{2} \rfloor - 1$. By Lemma 9, $|S| \leq 3$. Note that, by definition of basis, $|S| \geq 2$ and, by Lemma 1, $|S| \neq 2$ if $\text{order}(S) \neq n - 1$. Thus $|S| = 3$. Suppose $S = \{0, a, b\}$ where $a, b \in \mathbb{Z}_n$. If a had order $m \neq n$, then $3 \leq m < \lfloor \frac{n}{2} \rfloor$, since n is odd. By Corollary 1, this would imply that $\text{order}(S) \leq m + n/m - 2 < \lfloor \frac{n}{2} \rfloor - 1$, 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 $c > \lfloor \frac{n}{2} \rfloor + 1$, then S has the same order as $1 - a^{-1}S = \{0, 1, d\}$ with $d \leq \lfloor \frac{n}{2} \rfloor + 1$. Thus, we can assume that $c \leq \lfloor \frac{n}{2} \rfloor + 1$. Now using Corollary 4, we get $\text{order}(S) \neq \lfloor \frac{n}{2} \rfloor - 1$, a contradiction.

4.2. Proof of Theorem 6. The next table gives examples of bases attaining the conjectured orders in the third box according to Theorem 6. The results follow from Lemmas 13–15.

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

The fact that, for $n \geq 45$, $\text{order}(S) \neq \lfloor \frac{n}{3} \rfloor - 1$, if $n \equiv 1 \pmod 3$, and $\text{order}(S) \notin \{ \lfloor \frac{n}{3} \rfloor - 1, \lfloor \frac{n}{3} \rfloor \}$, if $n \equiv 2 \pmod 3$, follows from Lemma 18. Just note that, if $\text{order}(S) \in \{ \lfloor \frac{n}{3} \rfloor - 1, \lfloor \frac{n}{3} \rfloor \}$, then, by Lemma 9, $|S| \leq 4$.

The statement of the next lemma is stronger than what is needed to prove Theorem 6. However, the techniques we developed before allowed us to get this result, which in turn is useful in the proof of Corollary 5.

Lemma 18. *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 $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 2$ or $\text{order}(S) \geq \lfloor \frac{n}{3} \rfloor$. Moreover, if $\text{order}(S) = \lfloor \frac{n}{3} \rfloor$, then $n \equiv 1 \pmod 3$.*

Proof. Without loss of generality, assume $0 \in S$. Suppose that $n \not\equiv 0 \pmod 3$. Since S is a basis, $|S| > 1$. If $|S| = 2$, then $\text{order}(S) = n - 1 > \lfloor \frac{n}{3} \rfloor$. 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 1, the result follows since there can't be an element of order 3 or $n/3$. Thus, this element has order ≥ 4 or $\leq n/4$. 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 2. 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 $S = \{0, 1, a\}$, with $1 < a \leq \lfloor \frac{n}{2} \rfloor + 1$. In this case, the result follows from Corollary 4. If $|S| = 4$, assume that $S = \{0, 1, a, b\}$ with $a \leq \lfloor \frac{n}{2} \rfloor + 1$. Since for $S' \subset S$, $\text{order}(S) \leq \text{order}(S')$, we have

$$\text{order}(\{0, 1, a, b\}) \leq \min\{\text{order}(\{0, 1, a\}), \text{order}(\{0, 1, b\})\}. \tag{13}$$

Let

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

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

Note that $-\lfloor \frac{n}{2} \rfloor \in A_2$. Also, $1 - \lfloor \frac{n}{2} \rfloor \equiv \lfloor \frac{n}{2} \rfloor + 1 \pmod n$, for n even. If $a \notin A_1$ or $b \notin A_2$ then, by Corollary 4 and taking into account (13),

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

Recall that $\text{order}(\{0, 1, 1-b\}) = \text{order}(\{0, 1, b\})$. If $a \in A_1$ and $b \in A_2$, the 25 and 26 \rightarrow result follows from Lemmas 22–26. \square

The following result was presented in [Dukes et al. 2010]. 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 5. *Let S be a basis for \mathbb{Z}_n . Then*

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

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 $\lfloor \frac{n}{4} \rfloor + 3 \leq \text{order}(S)$, by Lemma 9, $|S| \leq 6$. Assume that $n \not\equiv 0 \pmod{3}$. If $|S| = 5$ or $|S| = 6$, by [Bueno et al. 2009, Theorem 3.7], $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 1$. If $|S| \leq 4$, by Lemma 18, $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 2$ or $\text{order}(S) \geq \lfloor \frac{n}{3} \rfloor$.

Now assume that $n \equiv 0 \pmod{3}$. If $|S| = 3$, the result follows from Corollary 4. Suppose that $|S| \in \{4, 5, 6\}$. If $\lfloor \frac{n}{4} \rfloor + 3 \leq \text{order}(S)$, by Corollary 1, 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 2 and 3. 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

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

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

Assume that $S = \{0, 1, a, b, c, d\}$, with $a \leq \lfloor \frac{n}{2} \rfloor + 1$ and $b = c = d$ if $|S| = 4$, and $c = d$ if $|S| = 5$. Note that if $S' \subset S$ then $\text{order}(S) \leq \text{order}(S')$. If $a \notin A_1$ or $b, c, d \notin A_2$ the result follows from Corollary 4. Suppose that $a \in A_1$, $b, c, d \in A_2$ and if a, b, c or $d \in \left\{ \lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor + 1, 1 - \lfloor \frac{n}{2} \rfloor \right\}$ then n is odd. If $|S| = 4$, the result follows from Lemmas 22–26. If $|S| = 5$ or $|S| = 6$ the result follows from the Remark on page 204 by noting that S has a subset of cardinality 4 containing 0 and 1 which is not one of the exceptional bases and, therefore, $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 2$. \square

4.3. Proof of Theorem 7. The next table gives examples of bases attaining the orders in the fourth box of \mathbb{Z}_n claimed in Theorem 7. The results follow from Lemmas 12–15.

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

4.4. Proof of Theorem 8. 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 $S = \{0, 1, 2, \dots, r - 1, r + 1\}$ with $2 \leq r \leq n - 2$. By Lemma 14, $\text{order}(S) = \lceil \frac{n+1}{r+1} \rceil$. 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, $\lceil \frac{n+1}{r+1} \rceil - \lceil \frac{n+1}{r+2} \rceil \leq 1$ 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.

Appendix: Gallery of bases and their orders

Here we provide the order of some particular bases that are necessary to prove the main results in this paper. We do not include all the proofs since many of them are similar.

Lemma 19. For $n \geq 6$, $\text{order}(\{0, 1, 4\}) = \lfloor \frac{n}{4} \rfloor + 2$.

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 $q = \lfloor \frac{n}{4} \rfloor$. Then

$$(q + 1)S = [0, 4q - 2] \cup [4q, 4q + 1] \cup \{4q + 4\}$$

and $[0, 4q + 2] \subseteq (q + 2)S$. Note that $4q + 4 \not\equiv 4q - 1 \pmod n$, since $n \geq 6$. Thus, $(q + 1)S \not\equiv \mathbb{Z}_n \pmod n$. On the other hand, $4q + 2 \geq n - 1$. The result follows. \square

Lemma 20. For $n \geq 6$, $\text{order}(\{0, 2, 5\}) \leq \lfloor \frac{n}{5} \rfloor + 3$.

Lemma 21. For $n \geq 4$, $\text{order}(\{0, 2, 3, 4\}) = \lfloor \frac{n}{4} \rfloor + 1$.

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

Lemma 22. Let $n \geq 21$. Let $a \in \{3, \lfloor \frac{n}{3} \rfloor + 1, \lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor + 1, 1 - \lfloor \frac{n}{2} \rfloor, -\lfloor \frac{n}{3} \rfloor, -2, -1\}$ and $S = \{0, 1, 2, a\}$. Then $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 2$ or $\text{order}(S) \geq \lfloor \frac{n}{3} \rfloor - 1$. Moreover, if $n \equiv 1 \pmod{3}$, then $\text{order}(S) \neq \lfloor \frac{n}{3} \rfloor - 1$ and if $n \equiv 2 \pmod{3}$, then $\text{order}(S) \notin \{\lfloor \frac{n}{3} \rfloor - 1, \lfloor \frac{n}{3} \rfloor\}$.

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 13.

Case 2: If $a = -2$, then S has the same order as $2 + S = \{0, 2, 3, 4\}$ and the result follows from Lemma 21.

Case 3: Suppose that $a \in \{\lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor + 1, 1 - \lfloor \frac{n}{2} \rfloor\}$. Assume n is even. Note that $1 - \lfloor \frac{n}{2} \rfloor = \lfloor \frac{n}{2} \rfloor + 1$. 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 2. Assume n is odd. Then

$$\begin{aligned} \text{order}(\{0, 1, 2, \lfloor \frac{n}{2} \rfloor\}) &= \text{order}(\{0, 1, 3, 5\}) \leq \text{order}(\{0, 1, 5\}), \\ \text{order}(\{0, 1, 2, \lfloor \frac{n}{2} \rfloor + 1\}) &= \text{order}(\{0, 1, 2, 4\}) \leq \text{order}(\{0, 1, 4\}). \end{aligned}$$

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

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

by Lemma 21. Note that $1 - \lfloor \frac{n}{2} \rfloor = \lfloor \frac{n}{2} \rfloor + 2$.

Case 4: Suppose that $a \in \{-\lfloor \frac{n}{3} \rfloor, \lfloor \frac{n}{3} \rfloor + 1\}$. If $n \equiv 0 \pmod{3}$, 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 3. Let $n \equiv 1 \pmod{3}$. If $a = -\lfloor \frac{n}{3} \rfloor$, then $3 * S = \{0, 1, 3, 6\}$ and

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

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

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

In both cases, $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 2$ by Corollary 4. If $n \equiv 2 \pmod{3}$, then

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

and the result follows as before. \square

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

Lemma 23. *Let $n \geq 30$. Let $a \in \{\lfloor \frac{n}{3} \rfloor + 1, \lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor + 1, 1 - \lfloor \frac{n}{2} \rfloor, -\lfloor \frac{n}{3} \rfloor, -2, -1\}$ and $S = \{0, 1, 3, a\}$. Then $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 2$ or $\text{order}(S) \geq \lfloor \frac{n}{3} \rfloor - 1$. Moreover, if $n \equiv 1 \pmod 3$, then $\text{order}(S) \neq \lfloor \frac{n}{3} \rfloor - 1$ and if $n \equiv 2 \pmod 3$, then $\text{order}(S) \notin \{\lfloor \frac{n}{3} \rfloor - 1, \lfloor \frac{n}{3} \rfloor\}$.*

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

Lemma 24. *Let $n \geq 30$. Let $a \in \{\lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor + 1, 1 - \lfloor \frac{n}{2} \rfloor, -\lfloor \frac{n}{3} \rfloor, -2, -1\}$ and $S = \{0, 1, \lfloor \frac{n}{3} \rfloor + 1, a\}$. Then $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 2$ or $\text{order}(S) \geq \lfloor \frac{n}{3} \rfloor - 1$. Moreover, if $n \equiv 1 \pmod 3$, then $\text{order}(S) \neq \lfloor \frac{n}{3} \rfloor - 1$ and if $n \equiv 2 \pmod 3$, then $\text{order}(S) \notin \{\lfloor \frac{n}{3} \rfloor - 1, \lfloor \frac{n}{3} \rfloor\}$.*

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

Lemma 25. *Let $n \geq 22$. Let $a \in \{\lfloor \frac{n}{2} \rfloor + 1, 1 - \lfloor \frac{n}{2} \rfloor, -\lfloor \frac{n}{3} \rfloor, -2, -1\}$ and $S = \{0, 1, \lfloor \frac{n}{2} \rfloor, a\}$. Then $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 2$ or $\text{order}(S) \geq \lfloor \frac{n}{3} \rfloor - 1$. Moreover, if $n \equiv 1 \pmod 3$, then $\text{order}(S) \neq \lfloor \frac{n}{3} \rfloor - 1$ and if $n \equiv 2 \pmod 3$, then $\text{order}(S) \notin \{\lfloor \frac{n}{3} \rfloor - 1, \lfloor \frac{n}{3} \rfloor\}$.*

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

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

For $a = -\lfloor \frac{n}{3} \rfloor$ and $n \equiv 0 \pmod 3$, S contains an element of order 3 and the result follows from Corollary 4.

For $a = \lfloor \frac{n}{2} \rfloor + 1$, $\text{order}(S) = \text{order}(2 * S + 1) = \{0, 1, 2, 3\}$ and the result follows from Lemma 13.

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

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

Lemma 26. *Let $n \geq 21$, $a \in \{1 - \lfloor \frac{n}{2} \rfloor, -\lfloor \frac{n}{3} \rfloor, -2, -1\}$ and $S = \{0, 1, \lfloor \frac{n}{2} \rfloor + 1, a\}$. Then $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 2$ or $\text{order}(S) \geq \lfloor \frac{n}{3} \rfloor - 1$. Moreover, if $n \equiv 1 \pmod 3$, then $\text{order}(S) \neq \lfloor \frac{n}{3} \rfloor - 1$ and if $n \equiv 2 \pmod 3$, then $\text{order}(S) \notin \{\lfloor \frac{n}{3} \rfloor - 1, \lfloor \frac{n}{3} \rfloor\}$.*

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 2. Now suppose that n is odd. Then $\text{order}(S) = \text{order}(\{0, 1, 2, 2a\})$.

If $a = 1 - \lfloor \frac{n}{2} \rfloor = \lfloor \frac{n}{2} \rfloor + 2$, then $2a = 3$ and the result follows from Lemma 13.

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

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

If $a = -1$, then $2a = -2$ and, by Lemma 21, $\text{order}(S) = \text{order}(\{0, 2, 3, 4\}) \leq \lfloor \frac{n}{4} \rfloor + 2$.

Suppose that $a = -\lfloor \frac{n}{3} \rfloor$. If $n \equiv 0 \pmod{3}$, then S contains 0 and an element of order 3 and the result follows from Corollary 3. If $n \equiv 1 \pmod{3}$, then $S = \{0, 1, 2, \lfloor \frac{n}{3} \rfloor + 1\}$ and the result follows from Lemma 22. If $n \equiv 2 \pmod{3}$, then, by Corollary 4,

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

Remark. Suppose that $S = \{0, 1, a, b\}$, with $a \in \{2, 3, \lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor + 1\}$ and $b \in \{2, 3, \lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor + 1, 1 - \lfloor \frac{n}{2} \rfloor, -2, -1\}$, where n is odd if a or b belong to the set $\{\lfloor \frac{n}{2} \rfloor, \lfloor \frac{n}{2} \rfloor + 1, -\lfloor \frac{n}{2} \rfloor\}$. From the proofs of Lemmas 22–26, we get that $\text{order}(S) \leq \lfloor \frac{n}{4} \rfloor + 2$ if S is not one of the next exceptional bases:

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

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

Acknowledgements

We would like to thank the anonymous referee whose comments and suggestions helped us improve the presentation of our paper.

References

- [Bueno and Furtado 2010] M. I. Bueno and S. Furtado, “On the gaps in the set of exponents of Boolean primitive circulant matrices”, *Electron. J. Linear Algebra* **20** (2010), 640–660. MR 2011g:15054 Zbl 05850040
- [Bueno et al. 2009] M. I. Bueno, S. Furtado, and N. Sherer, “Maximum exponent of Boolean circulant matrices with constant number of nonzero entries in their generating vector”, *Electron. J. Combin.* **16**:1 (2009), Research Paper 66. MR 2010m:11121 Zbl 1165.05329
- [Butler and Krabill 1974] K. K.-H. Butler and J. R. Krabill, “Circulant Boolean relation matrices”, *Czechoslovak Math. J.* **24**:2 (1974), 247–251. MR 50 #515 Zbl 0329.20049
- [Chou et al. 2008] W.-S. Chou, B.-S. Du, and P. J.-S. Shiue, “A note on circulant transition matrices in Markov chains”, *Linear Algebra Appl.* **429**:7 (2008), 1699–1704. MR 2010a:15077 Zbl 1148.60045
- [Davis 1979] P. J. Davis, *Circulant matrices*, Wiley, New York, 1979. MR 81a:15003 Zbl 0418.15017
- [Dukes et al. 2010] P. Dukes, P. Hegarty, and S. Herke, “On the possible orders of a basis for a finite cyclic group”, *Electron. J. Combin.* **17**:1 (2010), Research Paper 79. MR 2011e:11014 Zbl 1201.11017

- [Huang 1990] D. D. Huang, “On circulant Boolean matrices”, *Linear Algebra Appl.* **136** (1990), 107–117. MR 91m:15024 Zbl 0701.15010
- [Klopsch and Lev 2009] B. Klopsch and V. F. Lev, “Generating abelian groups by addition only”, *Forum Math.* **21**:1 (2009), 23–41. MR 2010c:20068 Zbl 1172.20038
- [Lancaster 1969] P. Lancaster, *Theory of matrices*, Academic Press, New York, 1969. MR 39 #6885 Zbl 0186.05301
- [Schwarz 1974] Š. Schwarz, “Circulant Boolean relation matrices”, *Czechoslovak Math. J.* **24**:2 (1974), 252–253. MR 50 #516 Zbl 0315.15011
- [Wang and Meng 1997] J.-Z. Wang and J.-X. Meng, “The exponent of the primitive Cayley digraphs on finite abelian groups”, *Discrete Appl. Math.* **80**:2-3 (1997), 177–191. MR 99h:05058 Zbl 0897.05045

Received: 2011-06-10 Revised: 2011-09-21 Accepted: 2011-09-22

mbueno@math.ucsb.edu *Mathematics Department and College of Creative Studies,
University of California, Santa Barbara,
Santa Barbara, CA 93106, United States*

kuanyingfang2011@u.northwestern.edu *Department of Mathematics, Northwestern University,
Evanston, IL 60208, United States*

saf5132@psu.edu *Department of Mathematics, Pennsylvania State University,
University Park, PA 16802, United States*

sbf@fep.up.pt *Faculdade de Economia do Porto, Universidade do Porto,
Rua Doutor Roberto Frias, 4200-464 Porto, Portugal*

involve

msp.berkeley.edu/involve

EDITORS

MANAGING EDITOR

Kenneth S. Berenhaut, Wake Forest University, USA, berenhks@wfu.edu

BOARD OF EDITORS

Colin Adams	Williams College, USA colin.c.adams@williams.edu	David Larson	Texas A&M University, USA larson@math.tamu.edu
John V. Baxley	Wake Forest University, NC, USA baxley@wfu.edu	Suzanne Lenhart	University of Tennessee, USA lenhart@math.utk.edu
Arthur T. Benjamin	Harvey Mudd College, USA benjamin@hmc.edu	Chi-Kwong Li	College of William and Mary, USA ckli@math.wm.edu
Martin Bohner	Missouri U of Science and Technology, USA bohner@mst.edu	Robert B. Lund	Clemson University, USA lund@clemson.edu
Nigel Boston	University of Wisconsin, USA boston@math.wisc.edu	Gaven J. Martin	Massey University, New Zealand g.j.martin@massey.ac.nz
Amarjit S. Budhiraja	U of North Carolina, Chapel Hill, USA budhiraj@email.unc.edu	Mary Meyer	Colorado State University, USA meyer@stat.colostate.edu
Pietro Cerone	Victoria University, Australia pietro.cerone@vu.edu.au	Emil Minchev	Ruse, Bulgaria eminchev@hotmail.com
Scott Chapman	Sam Houston State University, USA scott.chapman@shsu.edu	Frank Morgan	Williams College, USA frank.morgan@williams.edu
Jem N. Corcoran	University of Colorado, USA corcoran@colorado.edu	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran moslehian@ferdowsi.um.ac.ir
Toka Diagana	Howard University, USA tdiagana@howard.edu	Zuhair Nashed	University of Central Florida, USA znashed@mail.ucf.edu
Michael Dorff	Brigham Young University, USA mdorff@math.byu.edu	Ken Ono	Emory University, USA ono@mathcs.emory.edu
Sever S. Dragomir	Victoria University, Australia sever@matilda.vu.edu.au	Timothy E. O'Brien	Loyola University Chicago, USA tobrie1@luc.edu
Behrouz Emamizadeh	The Petroleum Institute, UAE bemamizadeh@pi.ac.ae	Joseph O'Rourke	Smith College, USA orourke@cs.smith.edu
Joel Foisy	SUNY Potsdam foisyjs@potsdam.edu	Yuval Peres	Microsoft Research, USA peres@microsoft.com
Errin W. Fulp	Wake Forest University, USA fulp@wfu.edu	Y.-F. S. Pétermann	Université de Genève, Switzerland petermann@math.unige.ch
Joseph Gallian	University of Minnesota Duluth, USA jgallian@d.umn.edu	Robert J. Plemmons	Wake Forest University, USA rplemmons@wfu.edu
Stephan R. Garcia	Pomona College, USA stephan.garcia@pomona.edu	Carl B. Pomerance	Dartmouth College, USA carl.pomerance@dartmouth.edu
Anant Godbole	East Tennessee State University, USA godbole@etsu.edu	Vadim Ponomarenko	San Diego State University, USA vadim@sciences.sdsu.edu
Ron Gould	Emory University, USA rg@mathcs.emory.edu	Bjorn Poonen	UC Berkeley, USA poonen@math.berkeley.edu
Andrew Granville	Université Montréal, Canada andrew@dms.umontreal.ca	James Propp	U Mass Lowell, USA jpropp@cs.uml.edu
Jerrold Griggs	University of South Carolina, USA griggs@math.sc.edu	József H. Przytycki	George Washington University, USA przytyck@gwu.edu
Ron Gould	Emory University, USA rg@mathcs.emory.edu	Richard Rebarber	University of Nebraska, USA rrebarbe@math.unl.edu
Sat Gupta	U of North Carolina, Greensboro, USA sngupta@uncg.edu	Robert W. Robinson	University of Georgia, USA rwr@cs.uga.edu
Jim Haglund	University of Pennsylvania, USA jhaglund@math.upenn.edu	Filip Saidak	U of North Carolina, Greensboro, USA f_saidak@uncg.edu
Johnny Henderson	Baylor University, USA johnny_henderson@baylor.edu	James A. Sellers	Penn State University, USA sellersj@math.psu.edu
Jim Hoste	Pitzer College jhoste@pitzer.edu	Andrew J. Sterge	Honorary Editor andy@ajsterge.com
Natalia Hritonenko	Prairie View A&M University, USA nahritonenko@pvamu.edu	Ann Trenk	Wellesley College, USA atrenk@wellesley.edu
Glenn H. Hurlbert	Arizona State University, USA hurlbert@asu.edu	Ravi Vakil	Stanford University, USA vakil@math.stanford.edu
Charles R. Johnson	College of William and Mary, USA crjohnso@math.wm.edu	Ram U. Verma	University of Toledo, USA verma99@msn.com
K. B. Kulasekera	Clemson University, USA kk@ces.clemson.edu	John C. Wierman	Johns Hopkins University, USA wierman@jhu.edu
Gerry Ladas	University of Rhode Island, USA gladas@math.uri.edu	Michael E. Zieve	University of Michigan, USA zieve@umich.edu

PRODUCTION

Silvio Levy, Scientific Editor

Sheila Newbery, Senior Production Editor

Cover design: © 2008 Alex Scorpan


See inside back cover or <http://msp.berkeley.edu/involve> for submission instructions.

The subscription price for 2012 is US \$105/year for the electronic version, and \$145/year (+\$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
<http://msp.org/>

A NON-PROFIT CORPORATION

Typeset in L^AT_EX

Copyright ©2012 by Mathematical Sciences Publishers

involve

2012

vol. 5

no. 2

A Giambelli formula for the S^1 -equivariant cohomology of type A Peterson varieties DARIUS BAYEGAN AND MEGUMI HARADA	115
Weak Allee effect, grazing, and S-shaped bifurcation curves EMILY POOLE, BONNIE ROBERSON AND BRITTANY STEPHENSON	133
A BMO theorem for ϵ -distorted diffeomorphisms on \mathbb{R}^D and an application to comparing manifolds of speech and sound CHARLES FEFFERMAN, STEVEN B. DAMELIN AND WILLIAM GLOVER	159
Modular magic sudoku JOHN LORCH AND ELLEN WELD	173
Distribution of the exponents of primitive circulant matrices in the first four boxes of \mathbb{Z}_n . MARIA ISABEL BUENO, KUAN-YING FANG, SAMANTHA FULLER AND SUSANA FURTADO	187
Commutation classes of double wiring diagrams PATRICK DUKES AND JOE RUSINKO	207
A two-step conditionally bounded numerical integrator to approximate some traveling-wave solutions of a diffusion-reaction equation SIEGFRIED MACÍAS AND JORGE E. MACÍAS-DÍAZ	219
The average order of elements in the multiplicative group of a finite field YILAN HU AND CARL POMERANCE	229



1944-4176(2012)5:2;1-B