Journal of Corrosion and Materials
www.corromat.com

J. Corros. Mater. **48** (2023) 1–18
https://doi.org/10.61336/jcm2023-1

Computing Certain Properties of Additive and Multiplicative Groups of Integers Modulo n Utilizing MATLAB

Waseem Khalid[1,*], Luqman Ali[1]

[1] *School of Engineering and Applied Sciences, Department of Computer Sciences, GIFT University, Gujranwala, Pakistan*

(Received: 20 January 2023. Received in revised form: 23 August 2023. Accepted: 29 August 2023. Published online: 1 September 2023.)

Abstract

This research focuses on two types of finite abelian groups: the group of integers under addition modulo n, and the group of integers under multiplication modulo n, where n is any positive integer up to 300. The computations in this study revolve around various properties of these groups, including the order of the group, the order and inverse of each element, the identification of cyclic subgroups, and the determination of generators within the group. To facilitate these calculations, a specialized program was developed using MATLAB. With this program, users can obtain answers for the aforementioned properties of these groups for any integer ranging from 0 to 300.

Keywords: Generator, Cyclic Subgroup.

1. Introduction

Bjarne Stroustrup pioneered the development of an extension to the C programming language, known as C^{++}, during the early 1980s [1]. In the late 1980s, Microsoft Corp.TM introduced its C^{++} compiler, bundled with a collection of library functions known as the Microsoft Foundation Classes (MFC) [2]. The MFC compiler proved to be a robust tool, empowering programmers to effortlessly design buttons, menus, dialog boxes, as well as incorporate text and graphics to visualize problem-solving. It offered a streamlined approach to making corrections and modifications. This enhanced user-friendliness and visual appeal of the program.

MATLAB was primarily developed by Cleve Moler, a renowned computer scientist and mathematician [3]. Moler's vision for MATLAB was to create a user-friendly environment for matrix computations and numerical analysis. His work on MATLAB has had a profound impact on scientific and engineering fields, as MATLAB has become an indispensable tool for researchers, engineers, and students worldwide, facilitating complex computations and data analysis. Cleve Moler's contribution to computational mathematics and software development is highly regarded in the scientific community.

MATLAB, as highlighted in [7], stands as a high- performance language tailored for technical computing tasks. Its distinguishing feature lies in its seamless integration of computation, visualization, and a comprehensive programming environment. Furthermore, MATLAB presents itself as a contemporary programming language environment, replete with advanced data structures, in-built editing and debugging utilities, and robust support for object- oriented programming. These characteristics collectively position MATLAB as an invaluable resource for both educational and research purposes.

In comparison to traditional programming languages such as C and FORTRAN, MATLAB boasts numerous advantages when it comes to addressing technical challenges. Notably, MATLAB operates as an interactive system where arrays serve as its fundamental data element, eliminating the need for explicit dimensioning. This software package, commercially accessible since 1984, has achieved the status of a standard tool across numerous universities and industries worldwide.

MATLAB impressively incorporates potent built-in routines that facilitate an extensive array of computations. Additionally, it offers user-friendly graphics commands that promptly provide visual representations of results. Specific applications are conveniently bundled in packages known as toolboxes, each tailored to distinct domains like signal processing, symbolic computation, control theory, simulation, optimization, and various other fields within applied science and engineering.

This research centers on the analysis of various properties within Group Theory, encompassing the determination of group order, individual element orders and inverses, identification of cyclic subgroups and compilation of generator lists. In a prior study, Mohd Ali and Sarmin [4] developed a C^{++} program interface to display the properties of two finite abelian groups: the group of integers under addition modulo n, denoted as Z_n , and the group of integers under multiplication modulo n, denoted as $(Z_n)^*$, where n represents a positive integer. However, the previous program had limitations, restricting input values of n to a maximum of 120 and displaying all group properties in a single interface. Later on, Mohd Ali, Noor Azhuan,

*Corresponding author (waseem.khalid@gift.edu.pk)

Sarmin, and Johar [5] endeavored to simulate these group properties for extended integer values, specifically $n \leqq 200$, while allowing users to select their preferred property for display.

Inspired by the work of Mohd Ali, Noor Azhuan, Sarmin, and Johar [5], who explored the computation of properties of additive and multiplicative groups of integers modulo n using C^{++} programming, this research report delves into the same domain but with a novel approach. In this study, we leverage the power of MATLAB as our primary computational tool, offering enhanced capabilities and versatility. Notably, our research extends the boundaries by accommodating values of n up to 300, addressing a limitation present in the previous work. This novel software additionally empowers users to select their preferred property for display, offering a tailored and customizable experience. Through this endeavor, we aim to provide a comprehensive and refined analysis of these groups, shedding new light on their properties and applications.

2. The groups Z_n and $(Z_n)^*$

In this section, we provide relevant definitions and properties of groups. Additionally, we offer an explanation of how to derive certain properties of Z_n and $(Z_n)^*$.

Definition 2.1. *Order of a Group [6]*
The number of elements of a group is called the group's order. The notation $|G|$ is used to denote the order of G.

Definition 2.2. *Order of an Element [6]*
The order of an element g in a group G is the smallest positive integer n such that $g^n = e$ (in additive notation, it would be $ng = 0$). The order of an element g is denoted by $|g|$.

Definition 2.3. *Cyclic Subgroup [6]*
Let G be a group and $a \in G$. Then $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is called a cyclic subgroup of G generated by a.

Definition 2.4. *The Group Z_n [5]*
The set $Z_n = \{0, 1, 2, \ldots, n-1\}$ for $n \leq 1$ is a group under addition modulo n. For any i in Z_n , the inverse of i is $n - i$. This group is commonly known as the group of integers modulo n.

Theorem 2.1. *[6] In a finite group G, the order of each element a in G divides the order of G. In symbols, we write $|a|||G|$, for all $a \in G$.*

Next we give an example of the group Z_{15}, the group of integers under addition modulo 15, with some of its properties.

Example 2.1. *The elements of Z_{15} are $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$.*
Hence, its order is 15. The computations of the order of the elements are as follows:
$|0| = 1$ *since the order of the identity element is always 1.*
$|1| = |2| = |4| = |7| = |8| = |11| = |13| = |14| = 15$
since $15 \times 1 \equiv 0$, $15 \times 12 \equiv 0$, $15 \times 4 \equiv 0$
$|10| = |5| = 3$ *and* $|3| = |6| = |9| = |12| = 5$.
Now, to get the inverse of each element, we use the formula $n - i$, where i is the element in $\mathbb{Z}_{15}$. Therefore, $0^{-1} = 0$ (the inverse of the identity element is itself), $1^{-1} = 14$, $2^{-1} = 13$, $3^{-1} = 12$, $4^{-1} = 11$, $5^{-1} = 10$, $6^{-1} = 9$, $7^{-1} = 8$, $8^{-1} = 7$, $9^{-1} = 6$, $10^{-1} = 5$, $11^{-1} = 4$, $12^{-1} = 3$, $13^{-1} = 2$, and $14^{-1} = 1$.
The elements 1, 2, 4, 7, 8, 11, 13, and 14 are generators of this group, since their order is the same as the order of $\mathbb{Z}_{15}$. The cyclic subgroups of $\mathbb{Z}_{15}$ are obtained by generating each element of $\mathbb{Z}_{15}$. The following subgroups are the cyclic subgroups of $\mathbb{Z}_{15}$:
$< 0 >= \{0\}$, $< 5 >=< 10 >= \{0, 5, 10\}$
$< 1 >=< 2 >=< 4 >=< 7 >=< 8 >=< 11 >=< 13 >=< 14 >= \mathbb{Z}_{15}$
$< 3 >=< 6 >=< 9 >=< 12 >= \{0, 3, 6, 9, 12\}$

Definition 2.5. *The Group $(Z_n)^*$. [6]*
(Z_n^* is defined to be the set of all positive integers less than n and relatively prime to n for each $n > 1$. Then $(Z_n)^*$ is a group under multiplication modulo n.

Now we give an example of the group (Z_{15}^*, the group of integers under multiplication modulo 15, with some of its properties.

Example 2.2. *The elements of* $(\mathbb{Z}^*_{15}$ *are* $\{1, 2, 4, 7, 8, 11, 13, 14\}$. *So its order is 8.*

The orders of the elements are as follows:

$|1| = 1$ *since the order of the identity element is always 1.*

$|2| = 4$ *since* $2^4 \equiv 16 \equiv 1 \pmod{15}$,

$|4| = 2$ *since* $4^2 \equiv 16 \equiv 1 \pmod{15}$,

$|7| = 4$ *since* $7^4 \equiv 2401 \equiv 1 \pmod{15}$,

$|8| = 2$ *since* $8^2 \equiv 64 \equiv 1 \pmod{15}$,

$|11| = 4$ *since* $11^4 \equiv 14641 \equiv 1 \pmod{15}$,

$|13| = 4$ *since* $13^4 \equiv 28561 \equiv 1 \pmod{15}$,

$|14| = 2$ *since* $14^2 \equiv 196 \equiv 1 \pmod{15}$.

The inverses of each element are: $1^{-1} = 1$, $2^{-1} = 8$, $4^{-1} = 4$, $7^{-1} = 13$, $8^{-1} = 8$, $11^{-1} = 11$, $13^{-1} = 7$, *and* $14^{-1} = 14$. *The inverse of the identity element is itself.*

Moreover, this group has no generator and the cyclic subgroups of $(\mathbb{Z}^*_{15}$ *are also obtained by generating each element of* $(\mathbb{Z}^*_{15}$. *The following subgroups are the cyclic subgroups of* $(\mathbb{Z}^*_{15}$*:*

$\langle 1\rangle = \{1\}$, $\langle 2\rangle = \langle 8\rangle = \{1, 2, 4, 8\}$, $\langle 4\rangle = \{1, 4\}$, $\langle 7\rangle = \langle 13\rangle = \{1, 7, 4, 13\}$, $\langle 11\rangle = \{1, 11\}$ *and* $\langle 14\rangle = \{1, 14\}$.

3. The program code for the group Z_n

Within this section, we provide programming code snippets along with their corresponding output displays. The purpose of the program is to comprehensively analyze various aspects of the group Z_n. Specifically, it is designed to ascertain the complete set of group elements, the group's order, an element's inverse, an element's order, group generators, and cyclic subgroups.

To utilize the program effectively, one must input the value of interest, prompting the program to present a menu of available properties. Users can then select their desired property, and the program will promptly generate and display the corresponding output.

The following provided code is instrumental in determining each property within the context of the group Z_n. Next, we will explore an example with n ranging from 0 to 300, for the group Z_n.

```
>> n = input('Enter the value of n (1 to 300): ');

if n < 1 || n > 300
    error('Invalid value of n. Please enter a value between 1 and 300.');
end

elements = mod(0:n-1, n); % Elements of the additive group modulo n

disp(['The order of the additive group modulo ', num2str(n), ' is ', num2str(n)]);

generators = [];

for i = 1:n
    element = elements(i);
    subgroup = mod(element * (0:n-1), n);

    if numel(unique(subgroup)) == n % Check if all elements are distinct
        generators = [generators, element];
    end
end

while true
    disp('Choose an option:');
    disp('1. Display elements of the additive group modulo n');
    disp('2. Display orders of the elements');
    disp('3. Display inverses of the elements');
    disp('4. Display generators of the additive group modulo n');
    disp('5. Display cyclic subgroups of the additive group modulo n');
    disp('6. Exit');

    option = input('Enter the option number: ');

    switch option
        case 1
            disp('Elements of the additive group modulo n:');
            disp(elements);

        case 2
            disp('Orders of the elements:');
            for i = 1:n
                element = elements(i);
                element_order = 1;
                power = mod(element, n);

                while power ~= 0
                    power = mod(power + element, n);
                    element_order = element_order + 1;
                end

                disp(['Element ', num2str(element), ': Order ', num2str(element_order)]);
            end
```

```
>> n = input('Enter the value of n (1 to 300): ');

if n < 1 || n > 300
    error('Invalid value of n. Please enter a value between 1 and 300.');
end

elements = mod(0:n-1, n); % Elements of the additive group modulo n

disp(['The order of the additive group modulo ', num2str(n), ' is ', num2str(n)]);

generators = [];

for i = 1:n
    element = elements(i);
    subgroup = mod(element * (0:n-1), n);

    if numel(unique(subgroup)) == n % Check if all elements are distinct
        generators = [generators, element];
    end
end
```

```
while true
    disp('Choose an option:');
    disp('1. Display elements of the additive group modulo n');
    disp('2. Display orders of the elements');
    disp('3. Display inverses of the elements');
    disp('4. Display generators of the additive group modulo n');
    disp('5. Display cyclic subgroups of the additive group modulo n');
    disp('6. Exit');

    option = input('Enter the option number: ');

    switch option
        case 1
            disp('Elements of the additive group modulo n:');
            disp(elements);

        case 2
            disp('Orders of the elements:');
            for i = 1:n
                element = elements(i);
                element_order = 1;
                power = mod(element, n);

                while power ~= 0
                    power = mod(power + element, n);
                    element_order = element_order + 1;
                end

                disp(['Element ', num2str(element), ': Order ', num2str(element_order)]);
            end

        case 3
            disp('Inverses of the elements:');
            for i = 1:n
                element = elements(i);
                inverse = mod(n - element, n); % Compute additive inverse
                disp(['Element ', num2str(element), ': Inverse ', num2str(inverse)]);
            end

        case 4
            disp('Generators of the additive group modulo n:');
            if isempty(generators)
                disp('There are no generators for the given additive group modulo n.');
            else
                disp(generators);
            end

        case 5
            disp('Cyclic subgroups of the additive group modulo n:');
            for i = 1:n
                element = elements(i);
                cyclic_subgroup = mod(element * (0:n-1), n);
                cyclic_subgroup_str = ['Cyclic subgroup generated by element ', num2str↙
(element), ': {', strjoin(string(unique(cyclic_subgroup)), ', '), '}'];
                disp(cyclic_subgroup_str);
            end

        case 6
            disp('Exiting the program...');
            return;

        otherwise
            disp('Invalid option. Please choose a valid option.');
    end
end
```

3.1 The computations in the group $(Z_{209}$

```
Enter the value of n (1 to 300): 209
The order of the additive group modulo 209 is 209
Choose an option:
1. Display elements of the additive group modulo n
2. Display orders of the elements
3. Display inverses of the elements
4. Display generators of the additive group modulo n
5. Display cyclic subgroups of the additive group modulo n
6. Exit
Enter the option number: 1
Elements of the additive group modulo n:
  Columns 1 through 18
    0     1     2     3     4     5     6     7     8     9    10    11    12    13
14    15    16    17
  Columns 19 through 36
   18    19    20    21    22    23    24    25    26    27    28    29    30    31

32    33    34    35
  Columns 37 through 54
   36    37    38    39    40    41    42    43    44    45    46    47    48    49
50    51    52    53
  Columns 55 through 72
   54    55    56    57    58    59    60    61    62    63    64    65    66    67
68    69    70    71
  Columns 73 through 90
   72    73    74    75    76    77    78    79    80    81    82    83    84    85
86    87    88    89
  Columns 91 through 108
   90    91    92    93    94    95    96    97    98    99   100   101   102   103
104   105   106   107
  Columns 109 through 126
  108   109   110   111   112   113   114   115   116   117   118   119   120   121
122   123   124   125
  Columns 127 through 144
  126   127   128   129   130   131   132   133   134   135   136   137   138   139
140   141   142   143
  Columns 145 through 162
  144   145   146   147   148   149   150   151   152   153   154   155   156   157
158   159   160   161
  Columns 163 through 180
  162   163   164   165   166   167   168   169   170   171   172   173   174   175
176   177   178   179
  Columns 181 through 198
  180   181   182   183   184   185   186   187   188   189   190   191   192   193
194   195   196   197
  Columns 199 through 209
  198   199   200   201   202   203   204   205   206   207   208
Choose an option:
1. Display elements of the additive group modulo n
2. Display orders of the elements
3. Display inverses of the elements
4. Display generators of the additive group modulo n
5. Display cyclic subgroups of the additive group modulo n
6. Exit
Enter the option number: 2
Orders of the elements:
Element 0: Order 1
Element 1: Order 209
Element 2: Order 209
Element 3: Order 209


Element 4: Order 209
Element 5: Order 209
Element 6: Order 209
Element 7: Order 209
Element 8: Order 209
Element 9: Order 209
Element 10: Order 209
Element 11: Order 19
```

```
Element 12: Order 209
Element 13: Order 209
Element 14: Order 209
Element 15: Order 209
Element 16: Order 209
Element 17: Order 209
Element 18: Order 209
Element 19: Order 11
Element 20: Order 209
Element 21: Order 209
Element 22: Order 19
Element 23: Order 209
Element 24: Order 209
Element 25: Order 209
Element 26: Order 209
Element 27: Order 209
Element 28: Order 209
Element 29: Order 209
Element 30: Order 209
Element 31: Order 209
Element 32: Order 209
Element 33: Order 19
Element 34: Order 209
Element 35: Order 209
Element 36: Order 209
Element 37: Order 209
Element 38: Order 11
Element 39: Order 209
Element 40: Order 209
Element 41: Order 209
Element 42: Order 209
Element 43: Order 209
Element 44: Order 19
Element 45: Order 209
Element 46: Order 209
Element 47: Order 209
Element 48: Order 209
Element 49: Order 209
Element 50: Order 209
Element 51: Order 209
Element 52: Order 209
Element 53: Order 209
Element 54: Order 209
Element 55: Order 19
Element 56: Order 209
Element 57: Order 11
Element 58: Order 209
Element 59: Order 209
Element 60: Order 209
Element 61: Order 209
Element 62: Order 209
```

```
Element 63: Order 209
Element 64: Order 209
Element 65: Order 209
Element 66: Order 19
Element 67: Order 209
Element 68: Order 209
Element 69: Order 209
Element 70: Order 209
Element 71: Order 209
Element 72: Order 209
Element 73: Order 209
Element 74: Order 209
Element 75: Order 209
Element 76: Order 11
Element 77: Order 19
```

```
Element 78: Order 209
Element 79: Order 209
Element 80: Order 209
Element 81: Order 209
Element 82: Order 209
Element 83: Order 209
Element 84: Order 209
Element 85: Order 209
Element 86: Order 209
Element 87: Order 209
Element 88: Order 19
Element 89: Order 209
Element 90: Order 209
Element 91: Order 209
Element 92: Order 209
Element 93: Order 209
Element 94: Order 209
Element 95: Order 11
Element 96: Order 209
Element 97: Order 209
Element 98: Order 209
Element 99: Order 19
Element 100: Order 209
Element 101: Order 209
Element 102: Order 209
Element 103: Order 209
Element 104: Order 209
Element 105: Order 209
Element 106: Order 209
Element 107: Order 209
Element 108: Order 209
Element 109: Order 209
Element 110: Order 19
Element 111: Order 209
Element 112: Order 209
Element 113: Order 209
```

```
Element 114: Order 11
Element 115: Order 209
Element 116: Order 209
Element 117: Order 209
Element 118: Order 209
Element 119: Order 209
Element 120: Order 209
Element 121: Order 19
Element 122: Order 209
Element 123: Order 209
Element 124: Order 209
Element 125: Order 209
Element 126: Order 209
Element 127: Order 209
Element 128: Order 209
Element 129: Order 209
Element 130: Order 209
Element 131: Order 209
Element 132: Order 19
Element 133: Order 11
Element 134: Order 209
Element 135: Order 209
Element 136: Order 209
Element 137: Order 209
Element 138: Order 209
Element 139: Order 209
Element 140: Order 209
Element 141: Order 209
Element 142: Order 209
Element 143: Order 19
Element 144: Order 209
Element 145: Order 209
Element 146: Order 209
Element 147: Order 209
Element 148: Order 209
Element 149: Order 209
Element 150: Order 209
Element 151: Order 209
Element 152: Order 11
```

```
Element 153: Order 209
Element 154: Order 19
Element 155: Order 209
Element 156: Order 209
Element 157: Order 209
Element 158: Order 209
Element 159: Order 209
Element 160: Order 209
Element 161: Order 209
Element 162: Order 209
Element 163: Order 209
Element 164: Order 209
Element 165: Order 19
Element 166: Order 209
Element 167: Order 209
Element 168: Order 209
Element 169: Order 209
Element 170: Order 209
Element 171: Order 11
Element 172: Order 209
Element 173: Order 209
Element 174: Order 209
Element 175: Order 209
Element 176: Order 19
Element 177: Order 209
Element 178: Order 209
Element 179: Order 209
Element 180: Order 209
Element 181: Order 209
Element 182: Order 209
Element 183: Order 209
Element 184: Order 209
Element 185: Order 209
Element 186: Order 209
Element 187: Order 19
Element 188: Order 209
Element 189: Order 209
Element 190: Order 11
Element 191: Order 209
Element 192: Order 209
Element 193: Order 209
Element 194: Order 209
Element 195: Order 209
Element 196: Order 209
Element 197: Order 209
Element 198: Order 19
Element 199: Order 209
Element 200: Order 209
Element 201: Order 209
Element 202: Order 209
Element 203: Order 209
Element 204: Order 209
Element 205: Order 209
Element 206: Order 209
Element 207: Order 209
Element 208: Order 209
Choose an option:
1. Display elements of the additive group modulo n
2. Display orders of the elements
3. Display inverses of the elements
4. Display generators of the additive group modulo n
5. Display cyclic subgroups of the additive group modulo n
6. Exit
Enter the option number: 3
Inverses of the elements:
Element 0: Inverse 0
Element 1: Inverse 208
Element 2: Inverse 207
Element 3: Inverse 206
```

```
Element 4: Inverse 205
Element 5: Inverse 204
Element 6: Inverse 203
Element 7: Inverse 202
Element 8: Inverse 201
Element 9: Inverse 200
Element 10: Inverse 199
Element 11: Inverse 198
Element 12: Inverse 197
Element 13: Inverse 196
Element 14: Inverse 195
Element 15: Inverse 194
Element 16: Inverse 193
Element 17: Inverse 192
Element 18: Inverse 191
Element 19: Inverse 190
Element 20: Inverse 189
Element 21: Inverse 188
Element 22: Inverse 187
Element 23: Inverse 186
Element 24: Inverse 185
Element 25: Inverse 184
Element 26: Inverse 183
Element 27: Inverse 182
Element 28: Inverse 181
Element 29: Inverse 180
Element 30: Inverse 179
Element 31: Inverse 178
Element 32: Inverse 177
Element 33: Inverse 176
Element 34: Inverse 175
Element 35: Inverse 174
Element 36: Inverse 173
Element 37: Inverse 172
Element 38: Inverse 171
Element 39: Inverse 170
Element 40: Inverse 169
Element 41: Inverse 168
Element 42: Inverse 167
Element 43: Inverse 166
Element 44: Inverse 165
Element 45: Inverse 164
Element 46: Inverse 163
Element 47: Inverse 162
Element 48: Inverse 161
Element 49: Inverse 160
Element 50: Inverse 159
Element 51: Inverse 158
Element 52: Inverse 157
Element 53: Inverse 156
Element 54: Inverse 155
Element 55: Inverse 154
Element 56: Inverse 153
Element 57: Inverse 152
Element 58: Inverse 151
Element 59: Inverse 150
Element 60: Inverse 149
Element 61: Inverse 148
Element 62: Inverse 147
Element 63: Inverse 146
Element 64: Inverse 145
Element 65: Inverse 144
Element 66: Inverse 143
Element 67: Inverse 142
Element 68: Inverse 141
Element 69: Inverse 140
Element 70: Inverse 139
Element 71: Inverse 138
Element 72: Inverse 137
Element 73: Inverse 136
Element 74: Inverse 135
Element 75: Inverse 134
Element 76: Inverse 133
Element 77: Inverse 132
Element 78: Inverse 131
Element 79: Inverse 130
Element 80: Inverse 129

Element 81: Inverse 128
Element 82: Inverse 127
Element 83: Inverse 126
Element 84: Inverse 125
Element 85: Inverse 124
Element 86: Inverse 123
Element 87: Inverse 122
Element 88: Inverse 121
Element 89: Inverse 120
Element 90: Inverse 119
Element 91: Inverse 118
Element 92: Inverse 117
Element 93: Inverse 116
Element 94: Inverse 115
Element 95: Inverse 114
Element 96: Inverse 113
Element 97: Inverse 112
Element 98: Inverse 111
Element 99: Inverse 110
```

```
Element 100: Inverse 109
Element 101: Inverse 108
Element 102: Inverse 107
Element 103: Inverse 106
Element 104: Inverse 105
Element 105: Inverse 104
Element 106: Inverse 103
Element 107: Inverse 102
Element 108: Inverse 101
Element 109: Inverse 100
Element 110: Inverse 99
Element 111: Inverse 98
Element 112: Inverse 97
Element 113: Inverse 96
Element 114: Inverse 95
Element 115: Inverse 94
Element 116: Inverse 93
Element 117: Inverse 92
Element 118: Inverse 91
Element 119: Inverse 90
Element 120: Inverse 89
Element 121: Inverse 88
Element 122: Inverse 87
Element 123: Inverse 86
Element 124: Inverse 85
Element 125: Inverse 84
Element 126: Inverse 83
Element 127: Inverse 82
Element 128: Inverse 81
Element 129: Inverse 80
Element 130: Inverse 79
Element 131: Inverse 78
Element 132: Inverse 77
Element 133: Inverse 76
Element 134: Inverse 75
Element 135: Inverse 74
Element 136: Inverse 73
Element 137: Inverse 72
Element 138: Inverse 71
Element 139: Inverse 70
Element 140: Inverse 69
Element 141: Inverse 68
Element 142: Inverse 67
Element 143: Inverse 66
Element 144: Inverse 65
Element 145: Inverse 64
Element 146: Inverse 63
Element 147: Inverse 62
Element 148: Inverse 61
Element 149: Inverse 60
Element 150: Inverse 59

Element 151: Inverse 58
Element 152: Inverse 57
Element 153: Inverse 56
Element 154: Inverse 55
Element 155: Inverse 54
Element 156: Inverse 53
Element 157: Inverse 52
Element 158: Inverse 51
Element 159: Inverse 50
Element 160: Inverse 49
Element 161: Inverse 48
Element 162: Inverse 47
Element 163: Inverse 46
Element 164: Inverse 45
Element 165: Inverse 44
Element 166: Inverse 43
Element 167: Inverse 42
Element 168: Inverse 41
Element 169: Inverse 40
Element 170: Inverse 39
Element 171: Inverse 38
Element 172: Inverse 37
Element 173: Inverse 36
Element 174: Inverse 35
Element 175: Inverse 34
Element 176: Inverse 33
Element 177: Inverse 32
Element 178: Inverse 31
Element 179: Inverse 30
Element 180: Inverse 29
Element 181: Inverse 28
Element 182: Inverse 27
Element 183: Inverse 26
Element 184: Inverse 25
Element 185: Inverse 24
Element 186: Inverse 23
Element 187: Inverse 22
Element 188: Inverse 21
Element 189: Inverse 20
Element 190: Inverse 19
Element 191: Inverse 18
Element 192: Inverse 17
Element 193: Inverse 16
Element 194: Inverse 15
Element 195: Inverse 14
Element 196: Inverse 13
Element 197: Inverse 12
Element 198: Inverse 11
Element 199: Inverse 10
Element 200: Inverse 9
Element 201: Inverse 8
Element 202: Inverse 7
Element 203: Inverse 6
Element 204: Inverse 5
Element 205: Inverse 4
Element 206: Inverse 3
Element 207: Inverse 2
Element 208: Inverse 1
Choose an option:
1. Display elements of the additive group modulo n
2. Display orders of the elements
3. Display inverses of the elements
4. Display generators of the additive group modulo n
5. Display cyclic subgroups of the additive group modulo n
6. Exit
Enter the option number: 4
Generators of the additive group modulo n:
  Columns 1 through 18
     1     2     3     4     5     6     7     8     9    10    12    13    14    15↙
16    17    18    20
  Columns 19 through 36
    21    23    24    25    26    27    28    29    30    31    32    34    35    36↙
37    39    40    41
  Columns 37 through 54
    42    43    45    46    47    48    49    50    51    52    53    54    56    58↙
```

```
59    60    61    62
  Columns 55 through 72
    63    64    65    67    68    69    70    71    72    73    74    75    78    79↙
80    81    82    83
  Columns 73 through 90
    84    85    86    87    89    90    91    92    93    94    96    97    98   100↙
101   102   103   104
  Columns 91 through 108
   105   106   107   108   109   111   112   113   115   116   117   118   119   120↙
122   123   124   125
  Columns 109 through 126
   126   127   128   129   130   131   134   135   136   137   138   139   140   141↙
142   144   145   146
  Columns 127 through 144
   147   148   149   150   151   153   155   156   157   158   159   160   161   162↙
163   164   166   167
  Columns 145 through 162
   168   169   170   172   173   174   175   177   178   179   180   181   182   183↙
184   185   186   188
  Columns 163 through 180
   189   191   192   193   194   195   196   197   199   200   201   202   203   204↙
205   206   207   208
Choose an option:
1. Display elements of the additive group modulo n
2. Display orders of the elements
3. Display inverses of the elements
4. Display generators of the additive group modulo n
5. Display cyclic subgroups of the additive group modulo n
6. Exit
Enter the option number: 5
Cyclic subgroups of the additive group modulo n:
    "Cyclic subgroup g…"    "0"    ": {"    "0"    "}"
    "Cyclic subgroup g…"    "1"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "2"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "3"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "4"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "5"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "6"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "7"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "8"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "9"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "10"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "11"    ": {"    "0, 11, 22, 33, 44…"    "}"
    "Cyclic subgroup g…"    "12"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "13"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "14"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "15"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "16"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "17"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "18"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "19"    ": {"    "0, 19, 38, 57, 76…"    "}"
    "Cyclic subgroup g…"    "20"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "21"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "22"    ": {"    "0, 11, 22, 33, 44…"    "}"
    "Cyclic subgroup g…"    "23"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "24"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "25"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "26"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "27"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "28"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "29"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "30"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "31"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "32"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "33"    ": {"    "0, 11, 22, 33, 44…"    "}"
    "Cyclic subgroup g…"    "34"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "35"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "36"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "37"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "38"    ": {"    "0, 19, 38, 57, 76…"    "}"
    "Cyclic subgroup g…"    "39"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "40"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
    "Cyclic subgroup g…"    "41"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"

"Cyclic subgroup g…"    "42"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
"Cyclic subgroup g…"    "43"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
"Cyclic subgroup g…"    "44"    ": {"    "0, 11, 22, 33, 44…"    "}"
"Cyclic subgroup g…"    "45"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
"Cyclic subgroup g…"    "46"    ": {"    "0, 1, 2, 3, 4, 5,…"    "}"
```

"Cyclic subgroup g…"	"47"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"48"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"49"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"50"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"51"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"52"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"53"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"54"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"55"	": {"	"0, 11, 22, 33, 44…"	"}"
"Cyclic subgroup g…"	"56"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"57"	": {"	"0, 19, 38, 57, 76…"	"}"
"Cyclic subgroup g…"	"58"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"59"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"60"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"61"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"62"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"63"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"64"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"65"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"66"	": {"	"0, 11, 22, 33, 44…"	"}"
"Cyclic subgroup g…"	"67"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"68"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"69"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"70"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"71"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"72"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"73"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"74"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"75"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"76"	": {"	"0, 19, 38, 57, 76…"	"}"
"Cyclic subgroup g…"	"77"	": {"	"0, 11, 22, 33, 44…"	"}"
"Cyclic subgroup g…"	"78"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"79"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"80"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"81"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"82"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"83"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"84"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"85"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"86"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"87"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"88"	": {"	"0, 11, 22, 33, 44…"	"}"
"Cyclic subgroup g…"	"89"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"90"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"91"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"92"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"93"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"94"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"95"	": {"	"0, 19, 38, 57, 76…"	"}"
"Cyclic subgroup g…"	"96"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"97"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"98"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"99"	": {"	"0, 11, 22, 33, 44…"	"}"
"Cyclic subgroup g…"	"100"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"101"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"102"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"103"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"104"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"105"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"106"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"107"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"108"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"109"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"110"	": {"	"0, 11, 22, 33, 44…"	"}"
"Cyclic subgroup g…"	"111"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"112"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"113"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"114"	": {"	"0, 19, 38, 57, 76…"	"}"
"Cyclic subgroup g…"	"115"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"116"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"117"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"118"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"119"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"120"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"121"	": {"	"0, 11, 22, 33, 44…"	"}"
"Cyclic subgroup g…"	"122"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"123"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"124"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"125"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"126"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"127"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"128"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"129"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"130"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"131"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"132"	": {"	"0, 11, 22, 33, 44…"	"}"
"Cyclic subgroup g…"	"133"	": {"	"0, 19, 38, 57, 76…"	"}"
"Cyclic subgroup g…"	"134"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"135"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"136"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"137"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"138"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"139"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"140"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"141"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"142"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"143"	": {"	"0, 11, 22, 33, 44…"	"}"
"Cyclic subgroup g…"	"144"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"145"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"146"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"147"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"
"Cyclic subgroup g…"	"148"	": {"	"0, 1, 2, 3, 4, 5,…"	"}"

```
"Cyclic subgroup g..."    "149"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "150"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "151"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "152"    ": {"    "0, 19, 38, 57, 76..."    "}"
"Cyclic subgroup g..."    "153"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "154"    ": {"    "0, 11, 22, 33, 44..."    "}"
"Cyclic subgroup g..."    "155"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "156"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "157"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "158"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "159"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "160"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "161"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "162"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "163"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "164"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "165"    ": {"    "0, 11, 22, 33, 44..."    "}"
"Cyclic subgroup g..."    "166"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "167"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "168"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "169"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "170"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "171"    ": {"    "0, 19, 38, 57, 76..."    "}"
"Cyclic subgroup g..."    "172"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "173"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "174"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "175"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "176"    ": {"    "0, 11, 22, 33, 44..."    "}"
"Cyclic subgroup g..."    "177"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "178"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "179"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "180"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "181"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "182"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "183"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "184"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"

"Cyclic subgroup g..."    "185"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "186"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "187"    ": {"    "0, 11, 22, 33, 44..."    "}"
"Cyclic subgroup g..."    "188"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "189"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "190"    ": {"    "0, 19, 38, 57, 76..."    "}"
"Cyclic subgroup g..."    "191"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "192"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "193"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "194"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "195"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "196"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "197"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "198"    ": {"    "0, 11, 22, 33, 44..."    "}"
"Cyclic subgroup g..."    "199"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "200"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "201"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "202"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "203"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "204"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "205"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "206"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "207"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
"Cyclic subgroup g..."    "208"    ": {"    "0, 1, 2, 3, 4, 5,..."    "}"
Choose an option:
1. Display elements of the additive group modulo n
2. Display orders of the elements
3. Display inverses of the elements
4. Display generators of the additive group modulo n
5. Display cyclic subgroups of the additive group modulo n
6. Exit
Enter the option number: 6
Exiting the program...
>>
```

4. The program code for the group $(Z_n)^*$

Within this section, we provide programming code snippets along with their corresponding output displays. The purpose of the program is to comprehensively analyze various aspects of the group $(Z_n)^*$. Specifically, it is designed to ascertain the complete set of group elements, the group's order, an element's inverse, an element's order, group generators, and cyclic subgroups.

To utilize the program effectively, one must input the value of interest, prompting the program to present a menu of available properties. Users can then select their desired property, and the program will promptly generate and display the corresponding output.

The following provided code is instrumental in determining each property within the context of the group $(Z_n)^*$. Next, we will explore an example with n ranging from 0 to 300, for the group $(Z_n)^*$.

```
>> n = input('Enter the value of n (1 to 300): ');

if n < 1 || n > 300
    error('Invalid value of n. Please enter a value between 1 and 300.');
end

order = 0;
elements = [];

for k = 1:n-1
    if gcd(k, n) == 1
        order = order + 1;
        elements = [elements, k];
    end
end

disp(['The order of the multiplicative group modulo ', num2str(n), ' is ', num2str
(order)]);

all_cyclic_subgroups = cell(1, order);
all_cyclic_subgroups{1} = [1]; % Identity subgroup

for i = 2:order
    element = elements(i);
    cyclic_subgroup = [1]; % Initialize with the identity element

    power = mod(element, n);
    while power ~= 1
        cyclic_subgroup = [cyclic_subgroup, power];
        power = mod(power * element, n);
    end

    all_cyclic_subgroups{i} = cyclic_subgroup;
end


generators = [];

for i = 2:order
    subgroup = all_cyclic_subgroups{i};
    if numel(subgroup) == order
        generators = [generators, elements(i)];
    end
end

while true
    disp('Choose an option:');
    disp('1. Display elements of the multiplicative group modulo n');
    disp('2. Display orders of the elements');
    disp('3. Display inverses of the elements');
    disp('4. Display generators of the multiplicative group modulo n');
    disp('5. Display cyclic subgroups of the multiplicative group modulo n');
```

```
    disp('6. Exit');

    option = input('Enter the option number: ');

    switch option
        case 1
            disp('Elements of the multiplicative group modulo n:');
            disp(elements);

        case 2
            disp('Orders of the elements:');
            for i = 1:length(elements)
                element = elements(i);
                element_order = 1;
                power = mod(element, n);

                while power ~= 1
                    power = mod(power * element, n);
                    element_order = element_order + 1;
                end

                disp(['Element ', num2str(element), ': Order ', num2str(element_order)]);
            end

        case 3
            disp('Inverses of the elements:');
            for i = 1:length(elements)
                element = elements(i);
                [~, inverse, ~] = gcd(element, n);
                inverse = mod(inverse, n); % Ensure positive inverse
                disp(['Element ', num2str(element), ': Inverse ', num2str(inverse)]);
            end

        case 4
            disp('Generators of the multiplicative group modulo n:');
            if isempty(generators)
                disp('There are no generators for the given multiplicative group modulo
n.');
            else
                disp(generators);
            end

        case 5
            disp('Cyclic subgroups of the multiplicative group modulo n:');
            disp('Identity Subgroup: {1}');
            for i = 2:order
                subgroup = all_cyclic_subgroups{i};
                subgroup_str = ['Element ', num2str(elements(i)), ': {', strjoin(string
(subgroup), ', '), '}'];
                disp(subgroup_str);
            end


         case 6
             disp('Exiting the program...');
             return;

         otherwise
             disp('Invalid option. Please choose a valid option.');
     end
 end
```

4.1 The computations in the group $(Z_{210}^*$

```
Enter the value of n (1 to 300): 210
The order of the multiplicative group modulo 210 is 48
Choose an option:
1. Display elements of the multiplicative group modulo n
2. Display orders of the elements
3. Display inverses of the elements
4. Display generators of the multiplicative group modulo n
5. Display cyclic subgroups of the multiplicative group modulo n
6. Exit
Enter the option number: 1
Elements of the multiplicative group modulo n:
  Columns 1 through 17

     1    11    13    17    19    23    29    31    37    41    43    47    53    59
61    67    71

  Columns 18 through 34

    73    79    83    89    97   101   103   107   109   113   121   127   131   137
139   143   149

  Columns 35 through 48

   151   157   163   167   169   173   179   181   187   191   193   197   199   209

Choose an option:
1. Display elements of the multiplicative group modulo n
2. Display orders of the elements
3. Display inverses of the elements
4. Display generators of the multiplicative group modulo n
5. Display cyclic subgroups of the multiplicative group modulo n
6. Exit
Enter the option number: 2
Orders of the elements:
Element 1: Order 1
Element 11: Order 6
Element 13: Order 4
Element 17: Order 12

Element 19: Order 6
Element 23: Order 12
Element 29: Order 2
Element 31: Order 6
```

```
Element 37: Order 12
Element 41: Order 2
Element 43: Order 4
Element 47: Order 12
Element 53: Order 12
Element 59: Order 6
Element 61: Order 6
Element 67: Order 12
Element 71: Order 2
Element 73: Order 12
Element 79: Order 6
Element 83: Order 4
Element 89: Order 6
Element 97: Order 4
Element 101: Order 6
Element 103: Order 12
Element 107: Order 12
Element 109: Order 6
Element 113: Order 4
Element 121: Order 3
Element 127: Order 4
Element 131: Order 6
Element 137: Order 12
Element 139: Order 2
Element 143: Order 12
Element 149: Order 6
Element 151: Order 3
Element 157: Order 12
Element 163: Order 12
Element 167: Order 4
Element 169: Order 2
Element 173: Order 12
Element 179: Order 6
Element 181: Order 2
Element 187: Order 12
Element 191: Order 6
Element 193: Order 12
Element 197: Order 4
Element 199: Order 6
Element 209: Order 2
Choose an option:
1. Display elements of the multiplicative group modulo n
2. Display orders of the elements
3. Display inverses of the elements
4. Display generators of the multiplicative group modulo n
5. Display cyclic subgroups of the multiplicative group modulo n
6. Exit
Enter the option number: 3
Inverses of the elements:
Element 1: Inverse 1
Element 11: Inverse 191
Element 13: Inverse 97
Element 17: Inverse 173
Element 19: Inverse 199
Element 23: Inverse 137
Element 29: Inverse 29
Element 31: Inverse 61
Element 37: Inverse 193
Element 41: Inverse 41
Element 43: Inverse 127
Element 47: Inverse 143
Element 53: Inverse 107
Element 59: Inverse 89
Element 61: Inverse 31
```

```
Element 61: Inverse 31
Element 67: Inverse 163
Element 71: Inverse 71
Element 73: Inverse 187
Element 79: Inverse 109
Element 83: Inverse 167
Element 89: Inverse 59
Element 97: Inverse 13
Element 101: Inverse 131
Element 103: Inverse 157
Element 107: Inverse 53
Element 109: Inverse 79
Element 113: Inverse 197
Element 121: Inverse 151
Element 127: Inverse 43
Element 131: Inverse 101
Element 137: Inverse 23
Element 139: Inverse 139
Element 143: Inverse 47
Element 149: Inverse 179
Element 151: Inverse 121
Element 157: Inverse 103
Element 163: Inverse 67
Element 167: Inverse 83
Element 169: Inverse 169
Element 173: Inverse 17
Element 179: Inverse 149
Element 181: Inverse 181
Element 187: Inverse 73
Element 191: Inverse 11
Element 193: Inverse 37
Element 197: Inverse 113
Element 199: Inverse 19
Element 209: Inverse 209
Choose an option:
1. Display elements of the multiplicative group modulo n
2. Display orders of the elements
3. Display inverses of the elements
4. Display generators of the multiplicative group modulo n
```

```
5. Display cyclic subgroups of the multiplicative group modulo n
6. Exit
Enter the option number: 4
Generators of the multiplicative group modulo n:
There are no generators for the given multiplicative group modulo n.
Choose an option:
1. Display elements of the multiplicative group modulo n
2. Display orders of the elements
3. Display inverses of the elements
4. Display generators of the multiplicative group modulo n
5. Display cyclic subgroups of the multiplicative group modulo n
6. Exit
Enter the option number: 5
Cyclic subgroups of the multiplicative group modulo n:
Identity Subgroup: {1}
    "Element "    "11"    ": {"    "1, 11, 121, 71, 1..."    "}"

    "Element "    "13"    ": {"    "1, 13, 169, 97"    "}"

    "Element "    "17"    ": {"    "1, 17, 79, 83, 15..."    "}"

    "Element "    "19"    ": {"    "1, 19, 151, 139, ..."    "}"

    "Element "    "23"    ": {"    "1, 23, 109, 197, ..."    "}"

    "Element "    "29"    ": {"    "1, 29"    "}"
     "Element "    "31"    ": {"    "1, 31, 121, 181, ..."    "}"

     "Element "    "37"    ": {"    "1, 37, 109, 43, 1..."    "}"


     "Element "    "41"    ": {"    "1, 41"    "}"

     "Element "    "43"    ": {"    "1, 43, 169, 127"    "}"

     "Element "    "47"    ": {"    "1, 47, 109, 83, 1..."    "}"

     "Element "    "53"    ": {"    "1, 53, 79, 197, 1..."    "}"

     "Element "    "59"    ": {"    "1, 59, 121, 209, ..."    "}"

     "Element "    "61"    ": {"    "1, 61, 151, 181, ..."    "}"

     "Element "    "67"    ": {"    "1, 67, 79, 43, 15..."    "}"

     "Element "    "71"    ": {"    "1, 71"    "}"

     "Element "    "73"    ": {"    "1, 73, 79, 97, 15..."    "}"

     "Element "    "79"    ": {"    "1, 79, 151, 169, ..."    "}"
    "Element "    "83"    ": {"    "1, 83, 169, 167"    "}"

    "Element "    "89"    ": {"    "1, 89, 151, 209, ..."    "}"

    "Element "    "97"    ": {"    "1, 97, 169, 13"    "}"

    "Element "    "101"    ": {"    "1, 101, 121, 41, ..."    "}"

    "Element "    "103"    ": {"    "1, 103, 109, 97, ..."    "}"

    "Element "    "107"    ": {"    "1, 107, 109, 113,..."    "}"

    "Element "    "109"    ": {"    "1, 109, 121, 169,..."    "}"

    "Element "    "113"    ": {"    "1, 113, 169, 197"    "}"

    "Element "    "121"    ": {"    "1, 121, 151"    "}"

    "Element "    "127"    ": {"    "1, 127, 169, 43"    "}"

    "Element "    "131"    ": {"    "1, 131, 151, 41, ..."    "}"

    "Element "    "137"    ": {"    "1, 137, 79, 113, ..."    "}"

    "Element "    "139"    ": {"    "1, 139"    "}"

    "Element "    "143"    ": {"    "1, 143, 79, 167, ..."    "}"

    "Element "    "149"    ": {"    "1, 149, 151, 29, ..."    "}"

    "Element "    "151"    ": {"    "1, 151, 121"    "}"

    "Element "    "157"    ": {"    "1, 157, 79, 13, 1..."    "}"

    "Element "    "163"    ": {"    "1, 163, 109, 127,..."    "}"

    "Element "    "167"    ": {"    "1, 167, 169, 83"    "}"

    "Element "    "169"    ": {"    "1, 169"    "}"

    "Element "    "173"    ": {"    "1, 173, 109, 167,..."    "}"

    "Element "    "179"    ": {"    "1, 179, 121, 29, ..."    "}"

    "Element "    "181"    ": {"    "1, 181"    "}"

    "Element "    "187"    ": {"    "1, 187, 109, 13, ..."    "}"

    "Element "    "191"    ": {"    "1, 191, 151, 71, ..."    "}"

    "Element "    "193"    ": {"    "1, 193, 79, 127, ..."    "}"



       "Element "    "197"    ": {"    "1, 197, 169, 113"    "}"

       "Element "    "199"    ": {"    "1, 199, 121, 139,..."    "}"

       "Element "    "209"    ": {"    "1, 209"    "}"

  Choose an option:
  1. Display elements of the multiplicative group modulo n
  2. Display orders of the elements
  3. Display inverses of the elements
  4. Display generators of the multiplicative group modulo n
  5. Display cyclic subgroups of the multiplicative group modulo n
  6. Exit
  Enter the option number: 6
  Exiting the program...
  >>
```

5. Summary

This software has been developed with the explicit purpose of calculating various properties of a group. These properties encompass the identification of all elements within the group, determination of the group's order, computation of the inverses and orders of individual elements, identification of group generators, and the exploration of cyclic subgroups within the groups Z_n and $(Z_n)^*$.

To utilize the program, you simply input your desired value for 'n' and then select one of the available options. Subsequently, the program will generate and display the relevant properties based on your selection. It is our aspiration that this program will serve as an initial step towards the creation of more advanced and sophisticated software tools for similar purposes.

Acknowledgements

The authors would like to express their sincere gratitude to GIFT University, Gujranwala, Pakistan, for their support and resources that facilitated this research. This work was made possible through the academic and research environment provided by the School of Engineering and Applied Sciences, Department of Computer Sciences at GIFT University.

References

[1] Deitel, H. M., & Deitel, P. J. (2013). *C^{++} How to Program* (9th ed.). Prentice Hall.
[2] Garret, P. B. (2008). *Abstract Algebra* (6th ed.). Chapman and Hall/CRC.
[3] Attaway, S. (2013). *MATLAB: A Practical Introduction to Programming and Problem Solving.* Elsevier Inc.
[4] Mohd Ali, N. M., & Sarmin, N. H. (2010). On some problems in group theory of probabilistic nature. *Menemui Matematik (Discovering Mathematics)*, *32*(2), 35-41.
[5] Mohd Ali, N. M., Noor Azhuan, N. A., Sarmin, N. H. & Johar, F. (2017). The Computation of Some Properties of Additive and Multiplicative Groups of Integers Modulo n Using C^{++} Programming. *Sains Humanika*, *9*(1-2), 57-63.
[6] Fraleigh, J. B. (2003). *A First Course in Abstract Algebra* (7th ed.). Reading, Massachusetts.
[7] The Mathworks Inc. (2005). *MATLAB 7.0 (R14SP2).* The MathWorks Inc.