Full paper

Sains Humanika

# The Computation of Some Properties of Additive and Multiplicative Groups of Integers Modulo n Using C++ Programming

Nor Muhainiah Mohd Ali*, Nur Azura Noor Azhuan, Nor Haniza Sarmin , Farhana Johar

*Department of Mathematical Sciences, Faculty of Science, 81310 Universiti Teknologi Malaysia, Johor Bahru*

*Corresponding author: normuhainiah@utm.my

**Abstract**

This research is focused on two types of finite abelian groups which are the group of integers under addition modulo $n$, and the group of integers under multiplication modulo $n$, where $n$ is any positive integer at most 200. The computations of some properties of the group including the order of the group, the order and inverse of each element, the cyclic subgroups, the generators of the group, and the lattice diagrams get more complicated and time consuming as n increases. Therefore, a special program is needed in the computation of these properties. Thus in this research, a program has been developed by using Microsoft Visual C++ Programming. This program enables the user to enter any positive integer at most 200 to generate answers for the properties of the groups.

*Keywords*: Microsoft Visual C++; abelian group; lattice diagram; cyclic subgroup



## 1.0 INTRODUCTION

Bjarne Stroustrup was the first person who develops an extension of C programming which is C++ programming, in the early 1980s (Deitel & Deitel, 2013). In the late 1980's, Microsoft Corp.TM released its C++ compiler, bundled with a set of library functions called the Microsoft Foundation Classes (MFC) (Garret, 2008). MFC is a really powerful compiler since it gives opportunity for programmer to create button, menus and dialog boxes, as well as text and graphics to visualize the problem that one is doing. Correction and modification also can be done easily. In addition, the user gets a better visualization and user-friendly program.

The computations of some properties of groups in the Group Theory including the order of the group, order and inverse of each element, the cyclic subgroups, list of all generators of the group and the lattice diagrams is main objective of this research. Previously, Mohd Ali and Sarmin (Mohd Ali & Sarmin, 2010) have developed a C++ program interface to display the properties of two finite abelian groups which are the group of integers under addition modulo $n$, $n$ and the group of integers under multiplication modulo $n$, $U(n)$ where $n$ is any positive integer. However, the input of $n$ for the program is limited to positive values of $n$ up to 120 and all the properties of the groups are shown in one interface. Therefore, in this research, those properties of the groups n and $U(n)$ are simulated and the lattice diagram is visualized for upgraded value of integer $n$ ($n \leq 200$). This new program also let the user to choose specific desired property to be displayed.

## 2.0 THE GROUPS $Z_n$ AND *U(n)*

Some related definitions and properties of groups, as well as explanation on how to obtain some properties of $\mathbb{Z}_n$ and $U(n)$ are included in this section.

### Definition 1 [4] Order of a Group

The number of elements of a group (finite or infinite) is called the groups order. The notation $|G|$ is used to denote the order of $G$.

### Definition 2 [4] Order of an Element

The order of an element g in a group $G$ is the smallest positive integer $n$ such that $g^n = e$ (In additive notation, this would be $ng = 0$). The order of an element g is denoted by $|g|$.

### Definition 3 [4] Cyclic Subgroups

The Let $a \in G$. Then $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}\{e, a, a^2, a^3, \dots\}$ is called a cyclic subgroup $G$ of generated by $a$.

**Definition 4 [4] Lattice Diagram**

This diagram is drawn to show the subgroups of a group. In the diagram, a line running downward from a group $G$ to a group $H$ means that $H$ is a subgroup of $G$. Thus the larger group is placed nearer to the top of the diagram.

**Definition 5 [4] The Group $\mathbb{Z}_n$**

The set $\mathbb{Z}_n = \{0,1,2,\dots,n-1\}$ for $n \geq 1$ is a group under addition modulo $n$. For any $i$ in $\mathbb{Z}_n$, the inverse of $i$ is $n-i$. This group is usually referred to as the group of integers modulo $n$.

**Theorem 1 [5]**

In a finite of group $G$, the order of each element in the group divides the order of the group. In symbols, we write $|a||G|, \forall a \in G$. Example 1 shows an example of a group $\mathbb{Z}_n$ that is $\mathbb{Z}_6$, the group under addition modulo 6 with some of its properties.

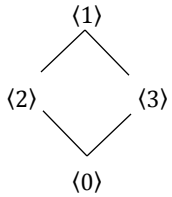
***Example 1***

The elements of $\mathbb{Z}_6$ are 0,1,2,3,4 and 5. Hence the order of the group is 6. The computations of the order of the elements are as follows:
$|0| = 1$ since the order of the identity element is always 1.
$|1| = |5| = 6$ since $6 \times 1 = 6 \equiv 0$ and $6 \times 5 = 30 \equiv 0$.
$|2| = |4| = 4$ and $|3| = 2$.

One way of getting the inverse of each element is to use the formula n –i, where i is the element of 6. Therefore, $0^{-1} = 0$ (the inverse of identity element is identity), $1^{-1} = 5$, $2^{-1} = 4$ and $3^{-1} = 3$. The elements 1 and 5 are the generators of this group since the order of those elements is same as the order of $\mathbb{Z}_6$. The cyclic subgroups of $\mathbb{Z}_6$ are obtained by generating each element of the group. The following shows the cyclic subgroups of $\mathbb{Z}_6$:

$$\langle 0\rangle = \{0\}, \langle 1\rangle = \langle 5\rangle = \mathbb{Z}_6, \langle 2\rangle = \langle 4\rangle = \{0,2,4\} \text{ and } \langle 3\rangle = \{0,3\}$$

Hence the lattice diagram of $\mathbb{Z}_6$ is:




**Definition 6 [4] The Group $U(n)$**

For each $n > 1, U(n)$ is defined to be the set of all positive integer less than $n$ and relatively prime to $n$. Then $U(n)$ is a group under multiplication modulo $n$.

Example 2 presents an example of a group $U(n)$, that is $U(6)$ under multiplication modulo 6 and some of its properties:

***Example 2:***

The elements of $U(6)$ consists of 1 and 5 only. Hence the order of the group is 2. The computations of the order of the elements are as follows:
$|1| = 1$ since the order of the identity element is always 1.
$|5| = 2$ since $5 \times 5 = 1$
The inverse of each element are: $1^{-1} = 1$ (the inverse of identity element is identity, $5^{-1} = 5$. Generator of this group is 5. The cyclic subgroup of $U(6)$ are also obtained by generating each element of the group. The following shows the cyclic subgroups:

$$\langle 1\rangle = \{1\}, \langle 5\rangle = U(6)$$

Hence the lattice diagram of $U(6)$ is as follows of $U(6)$.

## ■3.0 THE PROGRAM

In this section, some programming codes involved in the program together the output displays are given.

### Some Programming Codes

The following codes are written to create a small box (called edit box) for the users to enter the value of *n* and to create three buttons for the properties of $Z_n$ and $U(n)$ and a button to clear the interface. The buttons are the element of the group, order of the group and the lattice diagram.

```
enterN.Create(WS_CHILD | WS_VISIBLE | WS_BORDER | SS_CENTER, CRect(CPoint(55,70),CSize(50,25)), this,
IDC_ENTER_VALUE);
DrawRegion=CRect(CPoint(xMIN,yMIN),CPoint(xMAX,yMAX));
btnElmtZ.Create(L"Element ", WS_CHILD | WS_VISIBLE | BS_DEFPUSHBUTTON, CRect(CPoint(30,125),
CSize(100,30)), this, IDC_BTNOPT_ElmtZ);
btnOrdZ.Create(L"Order ", WS_CHILD | WS_VISIBLE | BS_DEFPUSHBUTTON, CRect(CPoint(30,160), CSize(100,30)),
this, IDC_BTNOPT_OrdZ);
btnLatZ.Create(L"Lattice", WS_CHILD | WS_VISIBLE | BS_DEFPUSHBUTTON, CRect(CPoint(30,195), CSize(100,30)),
this, IDC_BTNOPT_LatZ);
clear.Create(L"Clear", WS_CHILD | WS_VISIBLE | BS_DEFPUSHBUTTON, CRect(CPoint(30,230), CSize(100,30)),
this, IDC_CLEAR);
```

### The Output

This section shows the interface of the program and some output displays starting with Figure 1 which illustrates the interface for the written program.

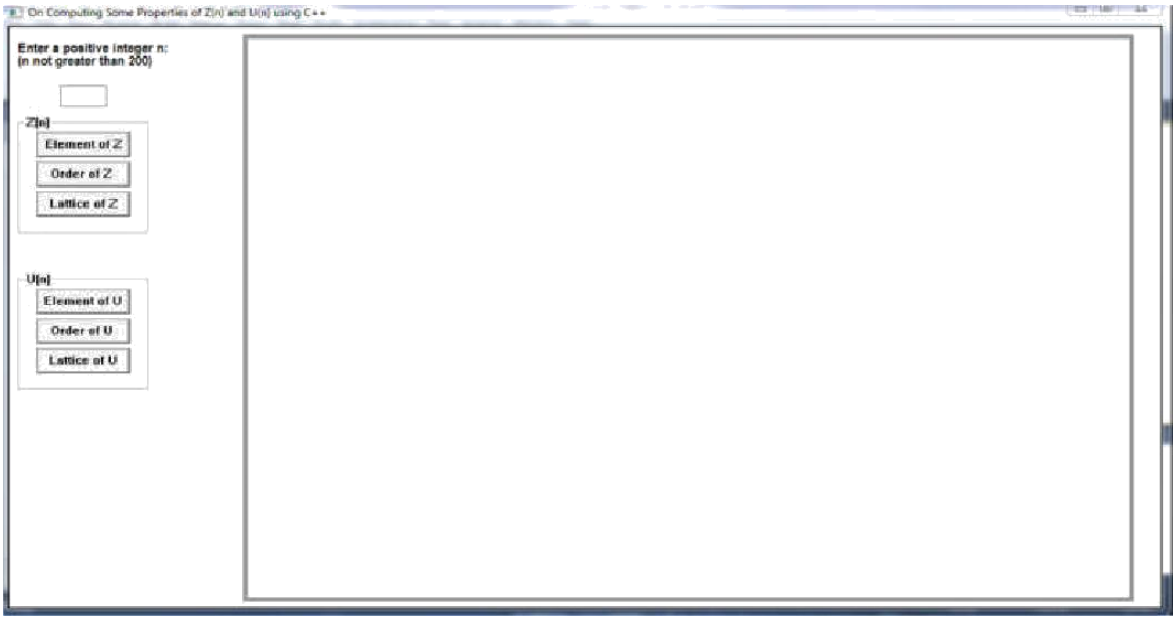



**Figure 1** Program Interface

Figure 2 shows the list of elements of $Z_{168}$ displayed in the interface when the user clicks at the "Element of Z" button.

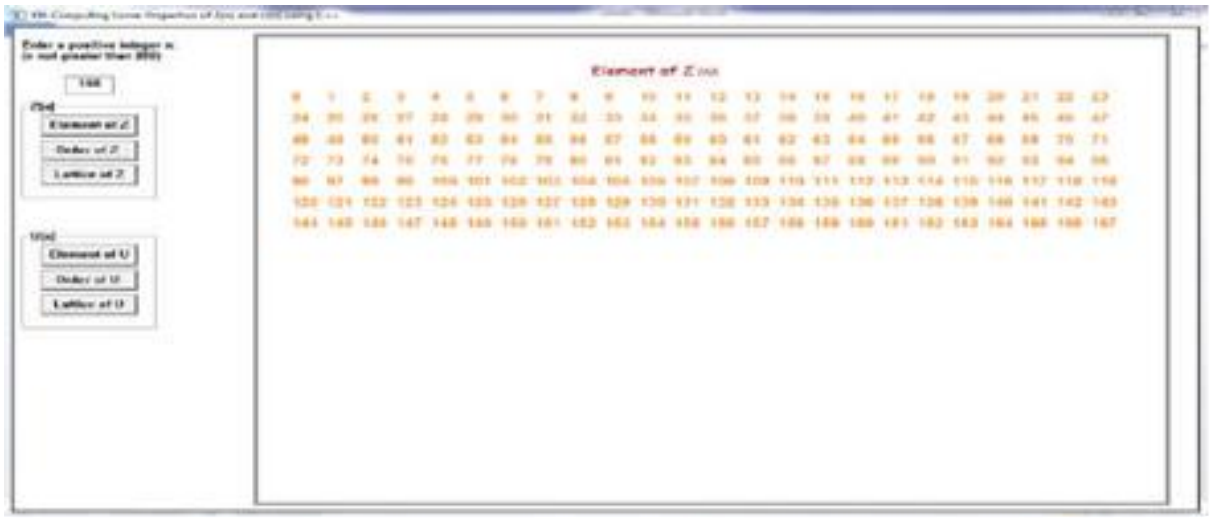


**Figure 2** Output Display – "Element of Z"

The order and inverse of each element, the cyclic subgroups, and the list of all generators of $Z_{168}$ are shown in Figure 3 when the user input the number 168 in the box and check at the "Order of Z" button.

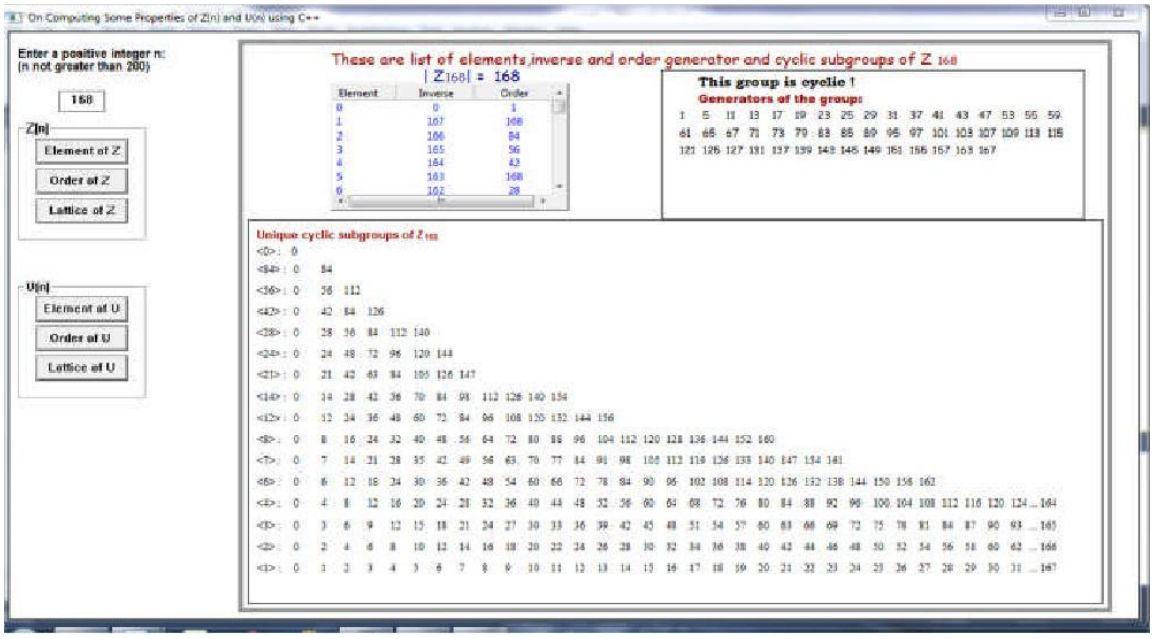


**Figure 3** Output Display – "Order of Z"

Next, the lattice diagram of $\mathbb{Z}_{168}$ is shown as in Figure 4 when the user checks at the "Lattice of Z" button,

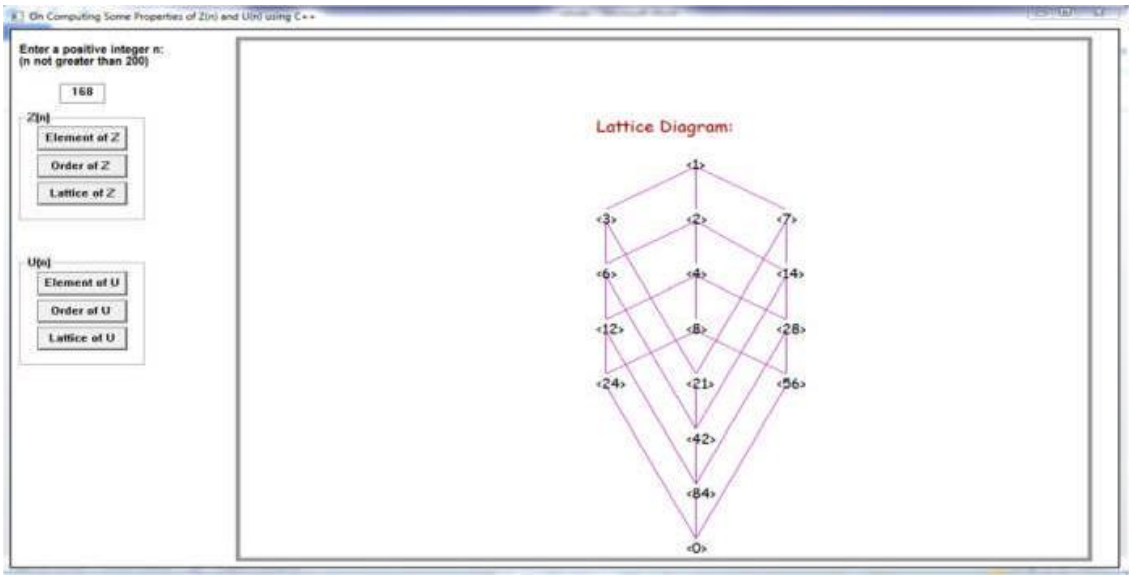



**Figure 4** Output Display – "Lattice of $Z$"

Figure 5 shows the list of elements of $U(151)$ displayed in the interface when the user input the number 151 in the box and check the "Element of U" button.

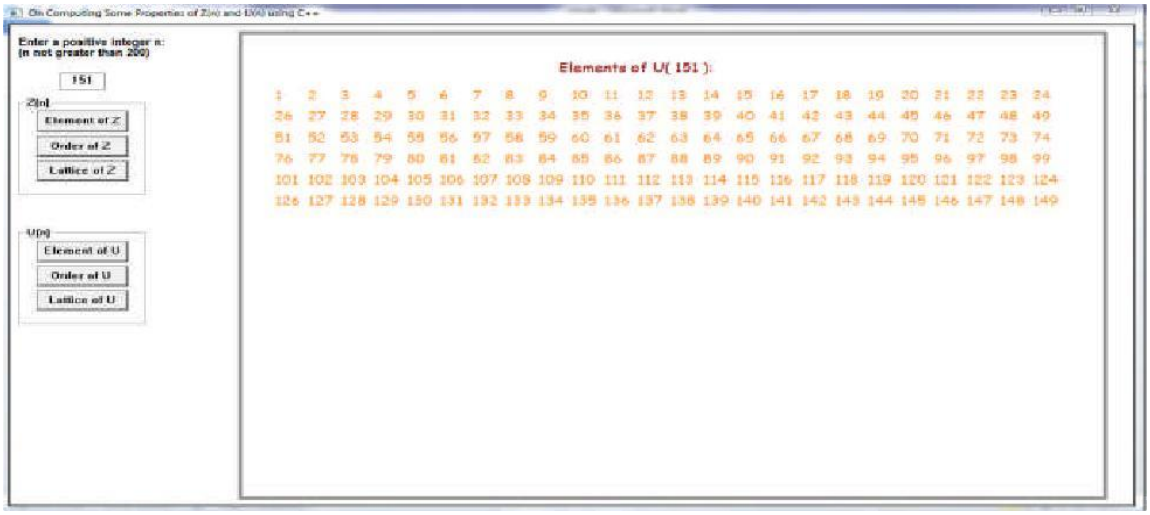



**Figure 5** Output Display – "Element of U"

The order and inverse of each element, the cyclic subgroups, and the list of all generators of $U(151)$ are shown in Figure 6 when the user click at the "Order of U" button.

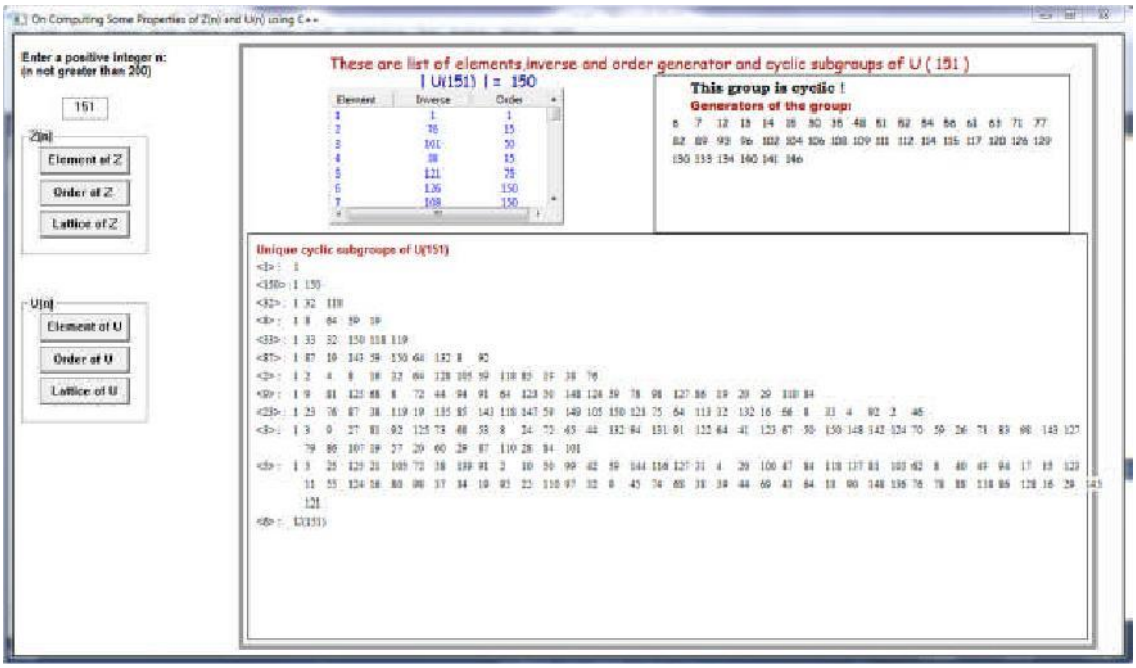



**Figure 6** Output Display –"Order of U"

Next, the lattice diagram of $U(151)$ is shown as in Figure 7 when the user check at the "Lattice of Z" button,

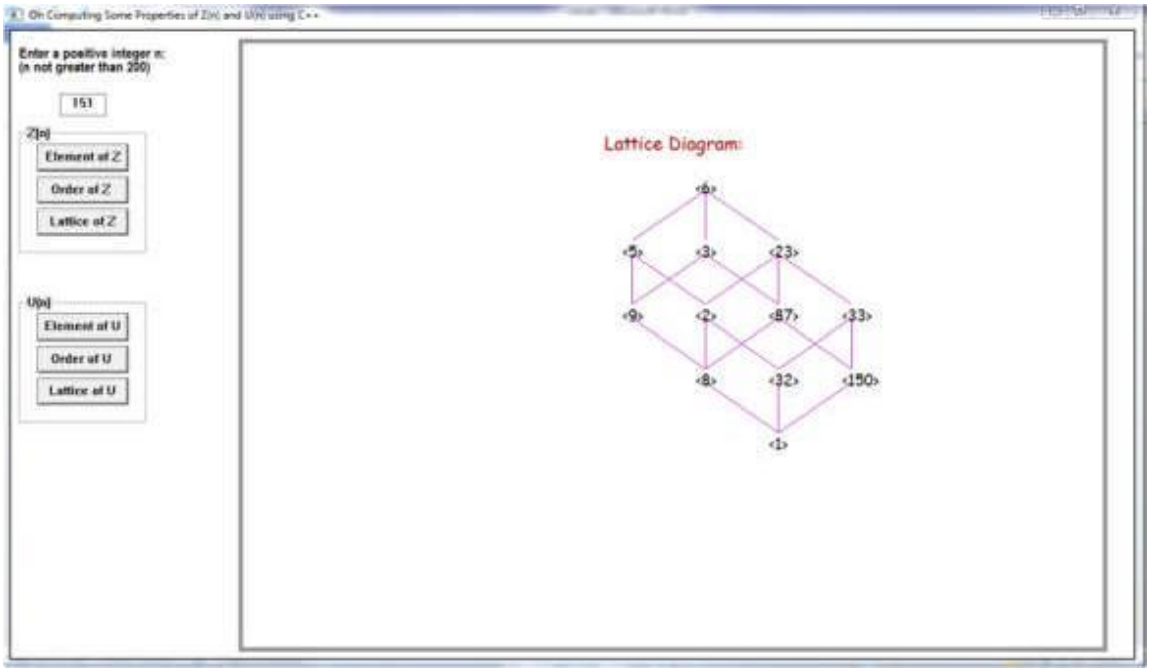



**Figure 7** Output Display –"Lattice of U"

This program is written with a message box as in Figure 8 that will appear when the user enters the invalid value of $n$.

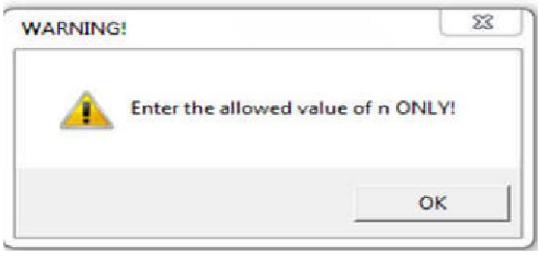



**Figure 8** Message Box

Another message box that is shown in Figure 9 informs the user about the display, that is, cyclic subgroups and lattice diagram will only be displayed if the chosen group is cyclic.

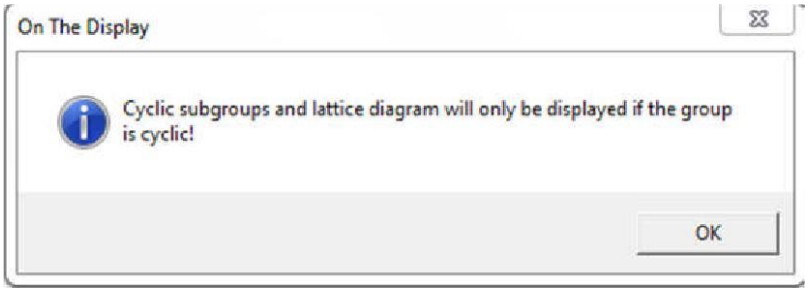



**Figure 9** Message box for "On The Display"

## ■4.0 CONCLUSION

This program has been constructed to determine all elements of a group, order of a group, inverse and order of each element, generators of a group, cyclic subgroups as well as the lattice diagram of group and $U(n)$. By $n$ entering the desired value of $n$ and checking at one of the buttons, the properties will appear. This program is hoped to be able to serve as a starting point for developing better and sophisticated programs.

## Acknowledgments

The authors would like to acknowledge Ministry of Education (MOE) Malaysia and Research Management Centre, Universiti Teknologi Malaysia (RMC, UTM) for the financial funding through the Research University Grant (RUG) Vote No 10J68.

## References

Deitel, H. M and Deitel, P. J. C++ (2013). How to Program, 9th ed. United States of America: Prentice Hall.
Gallian, J. A. (2012). Contemporary Abstract Algebra, 8th ed. Canada: Nelson Education, Ltd.
Garret, P. B. (2008). Abstract Algebra, 6th ed. United States of America: Chapman & Hall/CRC.
Fraleigh, J.B. (2003). A First Course in Abstract Algebra, 7th ed. Reading, Massachusetts: Addision-Wesley Publishing Company, Inc.
Matematik (Discovering Mathematics) (2010). 32(2), 35-4.
Mohd Ali, N.M and Sarmin (2010), N.H. On Some Problems in Group Theory of Probabilistic Nature, Menemui Matematik (Discovering Mathematics) 32(2), 35-41.