IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ONE SIMPLE COMPUTING MODEL FOR FINITE FIELDS OF Z_n,

Anand G Puranik*

Abstract: In this paper, I intended to compute subsets of Z_m that form multiplicative groups, (further finite fields) under the operation of multiplication modulo m (along with addition modulo m). These groups from the subsets of Z_m can be evaluated by using programming languages like C, Python and Maxima. Further, those multiplicative groups that form a ring and field over the same set, by the inclusion of additive identity element were also computed. In all the cases identity elements in the multiplicative groups, if exists, will be highlighted (computed with special interest).

Introduction

The present work is not due to intentionally focused work on the target set by the study of group theory, but accidentally took interest in the results of the earlier literature. The results mentioned in this research work, originated from earlier literature mentioned in the references. Hence the results mentioned here, seems to be a slight extension of the earlier results into new larger algebraic structures, to include finite fields. Computing and verification of algebraic structures using programming languages is also an interesting intellectual challenge. In this direction we find very less literatures, but have prime importance in modern world. In the literatures, I read, I find those results that can be seen with a similar view to include finite fields. All the programming concepts were to reduce consumption of high end computer resource and simplify programming concepts. The primary focus of this research work is to provide comparative and alternative programs, those computes finite fields from the subsets of Z_n, where n is not a prime number. At the outset, these ideas were brought from the works of, Nor Muhainiah Mohd Ali, Deborah Lim Shin Fei, Nor Haniza Sarmin, Shaharuddin Salleh, entitled, " A VISUAL MODEL FOR COMPUTING SOME PROPERTIES OF U(n) AND Zn"[]. Later I took interest in finding those subsets of Z_n, (where n is not a prime number), that form multiplicative groups under the binary operation multiplication modulo n (X_n). "ON THE NUMBER OF CYCLIC SUBGROUPS OF A FINITE GROUP", by the authors Mohammad Hossein Jafari and Ali Reza Madadi, provides slight different approach from computer programming concepts. Then the research paper entitled," MULTIPLICATIVE GROUPS IN Z_m", by the aouther, BrianSloan [], gave a fresh impetus over the subject and provided a clue to write C program. Then comparative programs were written extending the idea of the earlier mentioned research work. All the programs were written without using complex source codes or typical built in functions. The programming skills were inspired by the article entitled, " All Cyclic Subgroups In Group (Z_mXZ_n , +) Using Python" , by the authors Bobbi Rahman, Samsul Arifin, Indrabayu Muktyas[]. All the above authors must be thanked, for providing computer programs (with less source codes) connected to groups. In this direction the major challenges seems to be still open (needs more programming ideas) and available even for the graduate students. Below we list initial terms, terminologies and results used (on the same lines of earlier research papers[],[],[]).

Throughout all groups are assumed to be finite. A group is a non-empty set G with a binary operations *, that is closed, associative, includes an identity element and each element in G, has an inverse. **Identity element** refers to an element 'e' (called the identity) in G such that a*e = e*a=a for all a in G. **Inverses**. For each element a in G, there is an element b in G (called an inverse of a) such that a*b=b*a=e. Gallian [ ] has shown that the identity and inverse of any elements on a group are unique, and also cancellation laws holds in the group. If a group G, has another property a*b=b*a, for any a and b in G, then we said that group G is commutative. The basic properties of groups can be studied in [], [] and []. A cyclic group G is a group in which any element g in G can be written as g^n for n = 1, 2,...O(G). Furthermore, the characteristics of cyclic groups were mentioned in resources[ ], [ ] and [ ]. Subgroup is a non-empty subset H, of a group G which is also a group with the same binary operation as in G. For an element 'a' in the group G (i.e, a∈ G), we can form a subset S that contain all those elements of G which are of the forms, a^n for n =1, 2,... . This subset forms a subgroup in G, and called a cyclic subgroup that generate by a. Recall that any cyclic group is commutative and subgroups of a cyclic group are also cyclic. The set of all integers modulo n, denoted by Z_n, is a group of modulo addition operations. The group (Z_n , $+_n$) are constructed using the division algorithm on the set of all integers. This process can be studied in [ ] and [ ]. Furthermore, the formation process of the group (Z_mXZ_n, × +) can be studied in [ ] and [ ]. Python is a multipurpose programming language and easy to study (see [15]). Python can also run on various operating system platforms, such as Windows, Linux, Mac OS, Android (see [8]), and the others. Furthermore, study of the C, Python programs which are the focused results of this paper and its output will be discussed. The group is constructed using the division algorithm on the set of all integers. The binary operations addition modulo n and multiplication modulo n on the set {0, 1, 2, . . . , n-1}, which we denote by Z_n, play an extremely important role in abstract algebra. In certain situations we will want to combine the elements of Z_n by addition modulo n only. The group Z_n under addition modulo n will denote by (Z_n ,$+_n$). Next is a discussion of cyclic subgroups. Following are the definitions of cyclic groups and the generator of a group. Definition 2.2. Gallian [7]. Subgroup A group G is called cyclic if there is an element a in G such that {a^n∈G / n∈Z $+_n$}. Such an element a is called a generator of G. We may indicate that G is a cyclic group generated by 'a' as <a>.

Let (G , ∗) be a group and H⊆ G is a non-empty subset. Recall that the set H is called a subgroup of G if H is also a group of G, with same "binary operations" as in group G, denoted by H⊆G (see [9]). Rotman [16] explained about subgroup test that a subset of a group can be tested whether a subgroup or not, ie, if H is a subset of group G, then H is a subgroup of G if and only if ∀ a, b∈H, implies a∗b^{-1}∈H. Furthermore, Dummit [5] show us that for an element g∈G, we can form a subgroup in G generated by g. Theorem 2.3. Dummit [5]. Cyclic Subgroup Let G is a group and g G ∈ , then { } n g g n + = ∈ Z is a subgroup of G. Furthermore, g is called the cyclic subgroup of G which is generated by g. Recall that the order of a subgroup is the number of elements of the subgroup. The notion of order of a group element is as follows. Definition 2.4. Gallian [7]. Order of an Element The order of an element g in a group G is the smallest positive integer n such that n g e = . (In additive notation, this would be ng = 0 .) If no such integer exists, we say that g has infinite order. The order of an element g is denoted by |g|. The following is example of a group which will closed this session.

A well-known result in group theory says that a cyclic group of order n has a unique subgroup of order d, for any divisor d of n, so a cyclic group of order n has exactly τ (n) (necessarily cyclic) subgroups. A generalization of this result was obtained by Richards in [3]. He proved that a group of order n has at least τ (n) cyclic subgroups, and the group is cyclic if and only if it has exactly τ (n) cyclic subgroups. In this paper we generalize Richards' result and then classify groups of order n with τ (n) + 2 subgroups. Also we obtain a generalization of the Kesava Menon identity [2].

In this paper, initially given n is tested as a prime or composite number, if n is prime, then Z_n itself is a finite Field, so when n is not prime, without going deep in the theory of groups, both the additive subgroups in Z_n and multiplicative subgroups in $Z_n - \{0\}$ are generated by each element of the bigger set Z_n. Later, only distinct additive groups and multiplicative groups were considered, to test the field property or rings. Hence the finite Fields of the Z_n are computed. Computer programs to compute both the number of Fields and Fields in the set Z_n written in C, Phython and Maxima were given. A flow chart of the computer program, is given before converting the same into high language program.

5 CONCLUSION The conclusions that can be obtained from this study are as follows: a)Finite fields from the set of integers modulo n (Z_n) were computed. b) Using the Python program, we can determine all cyclic subgroups and Finite fields of the group or set ($Z_n \times_n +_n$) easily. c) From the program that has been created, the maximum number of Finite fields may be verified. This value corresponds to the upper limit of integers in Python that can be checked by writing the following command. import sys int(sys.float_info.max)

References:

(1) Gallian, Joseph A. Contemporary Abstract Algebra: Fourth Edition. Boston, MA: Houghton Mifflin Co., 1998.

[1] Adkins, W.A. and Weintraub, S.H., 2012. Algebra: an approach via module theory (Vol. 136). Springer Science & Business Media.

[2] Arifin, S., 2018. Grup Faktor dari Sebarang Subgrup Siklik dari Grup (Zn,+). SCIENCE TECH: Jurnal Ilmiah Ilmu Pengetahuan dan Teknologi, 4 (2), 53-58.

[3] Arifin, S. and Garminia, H. 2018. Valuation Dimension of Ring n Using Python. International Journal of Engineering & Technology, 7 (4), 6351-6356

[4] Arifin, S. and Garminia, H. 2019. Uniserial Dimension Of Module m n × Over Using Python. International Journal of Scientific & Technology Research, 8(7), 194-199

[5] Dummit, D.S. and Foote, R.M., 2004. Abstract algebra (Vol. 3). Hoboken: Wiley.

[6] Fraleigh, J.B. 2000. A First Course in Abstract Algebra, Sixth Edition, Addison-Wesley, New York.

[7] Gallian, J.A. 2017. Contemporary Abstract Algebra, 9th Edition, USA.

[8] Google. (2018, 30 April): available at https://play.google.com/store/apps/details?id=org.qpython.qpy&hl=e n

[9] Herstein I. 1996. Abstract Algebra, 3rd Edition, Prentice Hall, New York.

[10] Huang, H. 2018, 28th July. Algebra Lecture Notes, Auburn University Press, available at http://www.auburn.edu/ huanghu/math5310/

[11] Isaacs, I.M., 1994. Algebra, a graduate course, Brooks. Cole Publishing Company, Pacific Grove, California.

[12] Malik, D.S., Moderson, J.N., and Sen, M.K. 1997. Fundamentals of Abstract Algebra, USA. [13] Muktyas, I.B., and Arifin, S. 2018. Sebarang Pembangun Subgrup Siklik Dari Suatu Grup (Zn,+). Jurnal Matematika" MANTIK", 4 (2), 116-121. [14] Muktyas, I.B., and Arifin, S. 2018. Semua Subgrup Siklik dari Grup (Zn,+). Jurnal Teorema: Teori dan Riset Matematika. Vol 3 No 2, 177-186, September 2018.

[15] Python. 2018, 30 April. available at https://www.python.org/.

[16] Rotman, J. J. 2003. Advanced Modern Algebra, Prentice Hall, New York