Journal of Applied Science and Engineering Methodologies
Volume 3, No.3 (2017): Page.529-534
www.jasem.in

Green's Equivalence Relations on the multiplicative semigroup zn

Rajalekshmi I.S
Research Scholar
Department of Mathematics
University of Kerala, Thiruvananthapuram
lekshmiajith08@gmail.com

Abstract : *The Multiplicative Semigroup Z_n has a vital role in the studies of computer scientists. This paper present the various characteristics of this structure. The rank of Z_n, the characteristics of regular Z_n, the idempotents in Z_n, Green's relations on Z_n and the D-classes of Z_n are the topics under discussion. It is already known that the Multiplicative semigroup Z_n is regular iff n is square free. This paper is expected to be helpful for a comparative study between regular and non-regular Z_n.*

Keywords: *Multiplicative semigroup integers modulo n, rank of a semigroup, regular semigroup, idempotent elements of a semigroup, Euler function, Green's relations, Green's equivalence classes.*

1. Introduction

Z_n is a group under $+_n$ and is a monoid under $\times_n$. If n is a prime, then, Z_n is a group under $\times_n$. For our discussion, Z_n is the semigroup under $\times_n$.[2,3] Already it was observed that Z_n is a regular semigroup iff n is square free.[9] Since Z_n is a commutative semigroup, the Green's equivalence relations on Z_n coincides. Then obviously each D-class of Z_n consists of only one cell in its egg-box diagram. Also regular Z_n is a best known subclass of intersection of locally inverse semigroups and E-solid semigroups. This paper mainly concentrates on the total number of distinct D-classes of Z_n.

2. Preliminaries

Let S be a semigroup. The set of all idempotent elements of S is denoted by E(S). Z_n is an E-semigroup as $E(Z_n)$ forms a subsemigroup of Z_n . An element a of S is called regular if there exists x in S such that $axa = a$.[1,4,5] The set of all regular elements of S is denoted by Reg(S). The semigroup S is called regular if all its elements are regular. S is regular means Reg(S) = S. An element a' is an inverse of a if $aa'a = a$ and $a'aa' = a'$. An element with an inverse is necessarily regular. Also every regular element has an inverse; if there exists x ∈ S such that $axa = a$ then define, $a' = xax$ and then $aa'a = axaxa = axa = a$ and $'aa' = xaxaxax = xaxax = xax = a'$. An element a may have more than one inverse. The set of inverses of an element is denoted by $V(a)$. If every element of a regular semigroup S has a unique inverse, then S is called an inverse semigroup. Obviously, regular Z_n is an orthodox semigroup.

Theorem 2.1 [9] Consider (Z_n, $\times_n$), the multiplicative semigroup of integers modulo 'n, where $Z_n = \{\bar{0}, \bar{1}, \ldots \overline{(n-1)}\}$, then for x ∈ Z_n, $\bar{x}$ is a regular element of Z_n iff x and $\frac{n}{(n,x)}$, where (n, x) is the g.c.d of n and x, are relatively prime.

Corollary 2.1.1. [9] The multiplicative semigroup Z_n is a regular semigroup iff n is square free.

Theorem 2.2 [10,11,12] 1 If (a, b) = 1 and $n = ab$, then any idempotent in Z_n has the form $a^{\varphi(b)}$.

Corollary 2.2.1[10, 11,12] Let the prime factorization of n be $n = p_1^{n_1} p_2^{n_2} p_3^{n_3} \ldots . p_m^{n_m}$, the prime factorization consists of m factors, then the number of idempotents in Z_n is 2^m.

A set K is a generating set of a semigroup S if S contains all possible products of elements of K. Rank of S denote the minimum cardinality of a generating set. Here we introduce a formula for rank of Z_n in the later section.

If a is an element of a semigroup S, the smallest left ideal of S containing a is $Sa \cup \{a\}$, which is denoted by S^1a and is called the principal left ideal generated by a. Similarly, we can define the principal right ideal generated by a as $aS^1 = Sa \cup \{a\}$. Also the principal two-sided ideal of S generated by a is S^1aS^1 . Using the ideals mentioned above J. A. Green(1951), introduced five equivalence relations on a semigroup S which are denoted by L, R, H, D and J. Let $a, b \in S$, then

(i) aLb if and only if $S^1a = S^1 b$
(ii) aRb if and only if $aS^1 = bS^1$
(iii) aJb if and only if $S^1a\, S^1 = S^1bS^1$
(iv) $H = L \cap R$
(v) $D = L \vee R$

The corresponding equivalence classes of an element $a \in S$ are denoted by La, Ra, Ja, Ha and Da respectively.[1] A semigroup S is said to be E-solid if for all $e, f, g \in E(S)$ satisfying $eLfRg$, then there exists an idempotent $h \in S$ such that $eRhLg$. Z_n is an E-solid semigroup. In Z_n, $L = R = H = D = J$, each D-class of Z_n consists of only one cell in its egg-box diagram.

3. Greens Equivalence relations on Z_n

In this paper, the set of all numbers less than n and relatively prime to n is denoted by $R[n]$. Corresponding to each factor $x \neq 1$ of n, a set is constructed which is denoted by M_x to contain all multiples of x less than n, which are not divisible by a larger factor of n. Obviously, the sets M_x are disjoint. Example: For n = 30, the set M_2 = {2, 4, 8, 14, 16, 22, 26, 28}

Lemma 3.1.1 $Z_n = R[n] \cup (\bigcup_x M_x)$.

Proof: For each factor x of n there is an M_x and all the sets M_x are disjoint by their construction. If there is an integer u which is less than n and which does not belongs to

$(\bigcup_x M_x)$, then it will be relatively prime to n and hence belongs to R[n]. Thus the lemma.

Lemma 3.1.2 Rank(Z_n) is the number of factors of n .

Proof: By lemma 3.1.1. Z_n is the disjoint union $R[n] \cup (\bigcup_x M_x)$. Then a generating set K for Z_n consists of each facor of n. Thus the result.

Theorem 3.1 The number of distinct D-classes in Z_n is the number of factors of n.

OR

If $n = p_1^{m_1} p_2^{m_2} p_3^{m_3} .... p_k^{m_k}$, then the number of distinct D-classes in Z_n is $(m_1 + 1)(m_2 + 1)(m_3 + 1)....(m_k + 1)$.

Proof: By lemma 3.1.1, $Z_n = R[n] \cup(\bigcup_x M_x)$.

Claim01: The D-class of any element in R[n] is the same as D_1. Let $t \in R[n]$ be arbitrary. $\Longrightarrow$ $(n, t) = 1 \Longrightarrow \exists\ t' \in Z_n$ such that $tt' = t'\,t = 1$ It is needed to prove $D_t = D_1$. It is obvious that

$tZ_n \subseteq Z_n$. Let $y \in Z_n$ be arbitrary Then $y = y1 = ytt' = tyt' \Longrightarrow y \in t\,Z_n \Longrightarrow Z_n \subseteq t\,Z_n$. Thus $Z_n = t\,Z_n \Longrightarrow tD1 \Longrightarrow D_1 = D_t$.

Claim02: For each factor $x \neq 1$ of n, the D-class of any element in M_x is the same as D_x. Let $mx \in M_x$ where $m \neq 1$ be arbitrary. Obviously $mx\,Z_n \subseteq x\,Z_n$. To prove the converse a function f from $x\,Z_n$ to $mx\,Z_n$ is defined as, $f(xt) = mxt$, for each $t \in Zn$. Now $f(xt_1) = f(xt_2) \Longrightarrow mxt_1 = mxt_2 \Longrightarrow mx(t_1 - t_2) \equiv 0(modn)$. But M_x is constructed so that mx is not a factor of n. $\Longrightarrow (t_1 - t_2) \equiv 0(modn) \Longrightarrow t_1 \equiv t_2(modn) \Longrightarrow xt_1 \equiv xt_2(modn)$. Thus f is an injective function. Shows that $x\,Z_n \subseteq mx\,Z_n$. Thus $x\,Z_n = mx\,Z_n \Longrightarrow xDmx \Longrightarrow D_x = D_{mx}$.

From lemma 3.1.1, claim01 and claim02 it is obvious that R[n] contributes the D-class D_1 and each M_x contributes the D-class D_x, where $x \neq 1$ is a factor of n. Thus it is concluded that the number of distinct D-classes in Z_n is the number of factors of n, provided the D-class D_0 corresponds to the factor n itself.

Corollary: 3.1.1 The number of distinct D-classes in regular Z_n is 2^m .

Proof: By Corollary 2.1.1. we have Z_n as regular iff $n = p_1p_2p_3...p_m$, a product of distinct primes. Then by theorem 3. 1. there will be 2^m distinct D-classes.

Example 3.1.1. Consider Z_{30}, an example for a regular Z_n.

We have R[30] = {1, 7, 11, 13, 17, 19, 23, 29} and the Euler Phi function $\varphi(30) = 8$.

$Z_{30} = 7Z_{30} = 11Z_{30} = 13Z_{30} = 17Z_{30} = 19Z_{30} = 23Z_{30} = 29Z_{30}$. The D-classes of all elements of R[30] are the same as D-class of 1 denoted by D_1.

Now $2Z_{30} = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28\} = 4Z_{30} = 8Z_{30} = 14Z_{30} = 16Z_{30} = 22Z_{30} = 26Z_{30} = 28Z_{30}$. Shows that the D-class of 2 consists of $D_2 = \{2, 4, 8, 14, 16, 22, 26, 28\}$.

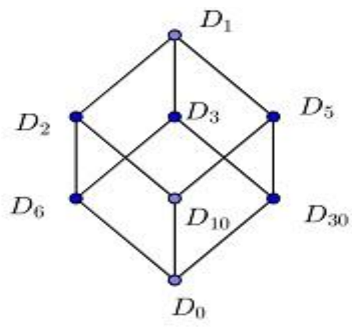
$3Z_{30} = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27\} = 9Z_{30} = 21Z_{30} = 27Z_{30}$. Shows that the D-class of 3 consists of $D_3 = \{3, 9, 21, 27\}$.

$5Z_{30} = \{0, 5, 10, 15, 20, 25\} = 25Z_{30}$ Shows that the D-class of 5 consists of $D_5 = \{5, 25\}$. $6Z_{30} = \{0, 6, 12, 18, 24\} = 12Z_{30} = 18Z_{30} = 24Z_{30}$ Shows that the D-class of 6 consists of $D_6 = \{6, 12, 18, 24\}$.

$10Z_{30} = \{0, 10, 20\} = 20Z_{30}$ Shows that the D-class of 10 consists of $D_{10} = \{10, 20\}$.

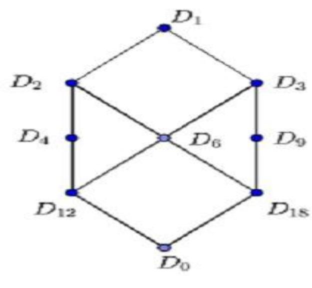
$15Z_{30} = \{0, 15\}$ Shows that the D-class of 15 consists of $D_{15} = \{15\}$. Now $0Z_{30} = \{0\}$ Shows that the D-class of 0 consists of $D_0 = \{0\}$.

Thus the distinct D-classes of Z_{30} are D_1, D_2, D_3, D_5, D_6, D_{10}, D_{15}, D_0. Corresponding to each factor of 30 there is a D-class. Totally there are 8 distinct classes. The natural partial ordering on the set of D-classes is given by the Hasse diagram,



Example 3.1.2. Consider Z_{36}, an example for a non-regular Z_n.

The distinct D-classes of Z_{36} are D_1, D_2, D_3, D_4, D_6, D_9, D_{12}, D_{18} and D_0, the Hasse Diagram of the lattice of D-classes of Z_{36} is given below:



Corollary 3.1.2 In Z_n, the number of idempotents is less than or equal to the number of distinct D-classes.

Proof: By theorem 3.1, the number of distinct D-classes in Z_n is $(m_1+1)(m_2+1)(m_3+1)....(m_k+1)$ whenever $n = p_1^{m_1} p_2^{m_2} p_3^{m_3} .... p_k^{m_k}$. But by corollary 2.2.1 the number of idempotents in Z_n is 2^k . Since each $m_i \geq 1$, each $m_i + 1 \geq 2$, which yields the result.

Theorem 3.2 If D represents a D-class of Z_n, then D contains at most one idempotent.

Proof: In a D-class, either every element of D is regular or no element of D is regular.[1] Also no H-class contains more than one idempotent.[1] Since idempotents are regular, every D-class containing an idempotent is regular. Since in a regular D-class, each L-class and each R-class contains an idempotent and in Z_n, L = R = H = D = J., each H-class contains exactly one idempotent. If D is not regular, it doesn't contain an idempotent. Thus the result is obvious.

Theorem 3.3 $Z_{p_1^{m_1} p_2^{m_2} p_3^{m_3} .... p_k^{m_k}}$ is not regular if at least one $m_i > 1$.

Proof: If at least one $m_i > 1$, the number of idempotents 2^k (by corollary 2.2.1), will be strictly less than the number of distinct D-classes $\prod_i (m_i + 1)$(by theorem 3.1). But by theorem 3.2 there will be at least one D-class which does not contain any idempotent. As the D-class which does not contain an idempotent is irregular, the semigroup $Z_{p_1^{m_1} p_2^{m_2} p_3^{m_3} .... p_k^{m_k}}$ is irregular.

Theorem 3.4: A regular Z_n is isomorphic to some $Zp_1p_2p_3...p_k$.

Proof: By fundamental theorem of Arithmetic(Unique Prime Factorization Theorem), every integer $n \geq 1$, can be expressed as $n = p_1^{m_1} p_2^{m_2} p_3^{m_3} .... p_k^{m_k}$, where $p_1, p_2, p_3, ..., p_k$ are distinct primes. If Z_n is regular, each D-class of Z_n contains exactly one idempotent. By theorem 3.1 there will be $\prod_i (m_i + 1)$ distinct D-classes for Z_n. Since each D-class of regular Z_n has exactly one idempotent there will be $\prod_i (m_i + 1)$ idempotents in Z_n . Then $2^k = \prod_i (m_i + 1)$, where i = 1, 2, 3, ...k. Here the L. H. S. and R. H. S. Consists of k-factors, therefore by comparing them, each $(m_i + 1) = 2$. $\Rightarrow (m_i + 1) = 2 \Rightarrow m_i = 1$, for each i. Then $n = p_1 p_2 p_3 ... p_k$. Shows that there exists some $k \in Z$ such that $| Z_n | = | Zp_1p_2p_3...p_k |$. Hence they are isomorphic.

Theorem 3.5 If $n = p_1 p_2 p_3 ... p_k$, a product of distinct primes then Z_n, is an inverse semigroup.

Proof: Since Z_n, is a commutative semigroup, its idempotents commute. $Z_{p_1 p_2 p_3 \cdots p_k}$ is regular by corollary 2.1.1. Let e and f be two idempotents in a single L-class then e and f are two right identities in the same L-class.Thus $ef = e$ and $= f$. But in Z_n , we have

$ef = fe$. Thus it means $e = f$, every L-class in regular Z_n contains exactly one idempotent. Also for Z_n, L = R = H = D = J. Thus in a D-class of regular Z_n , there will be exactly one idempotent . Let x ∈ Z_n where $n = p_1 p_2 p_3 ... p_k$. Suppose there exists two inverses say x' and x'' for x. Then the idempotents, $xx'$and xx'' belongs to D_x and so by the above argument $' = xx''$. Similarly, the idempotents $x'x$ and $x''x$ are equal. Then $x' = x'xx' = x'(xx') = x'(xx'') = (x'x)x'' = (x''x)x'' = x''xx'' = x''$. Therefore, each x ∈ Z_n possesses a unique inverse in Z_n. Thus regular Z_n is an inverse semigroup.

4. Conclusion

For every positive integer n we can easily identify all possible distinct D-classes of Z_n using the sets R[n] and M_x of each factor $x \neq 1$ of n. Also the Hasse Diagram of the Lattice of the partially ordered set of D-classes of Z_n can be constructed, using which we can compare the lattices of D-classes of a regular Z_n and a non-regular Z_n.

REFERENCES

1. Howie, J.M. An Introduction to Semigroup Theory. London: Academic Press, 1976.
2. Clifford, A.H. and Preston, G.B. The Algebraic Theory of Semigroups, vol. I. Math. Surveys of the American Math. Soc. 7, Providence, R.I., 1961.
3. Edwards, P.M. Fundamental semigroups. Proc. R. Soc. Edinb. Sec. A. 99(1985), 313-317.
4. Grillet, P.A. The structure of regular semigroups. I. A representation. Semigroup Forum.8 (1974), 177183.
5. Hall, T.E. On regular semigroups. J. Algebra. 24 (1973), 124.
6. Higgins, P.M. Techniques of Semigroup Theory. Oxford University Press, 1992.
7. Nambooripad, K.S.S. Structure of regular semigroups. I. Fundamental regular semigroups. Semigroup Forum. 9 (1975), 354363.
8. Nambooripad, K.S.S. Structure of regular semigroups. I.Mem. Amer. Math. Soc.22 (1979).
9. Ng. Danpattanamongkon and Y. Kemprasit, Regular Elements and BQ-elements of the semigroup , International Mathematical Forum, 5, 2010 no. 51- 2533-2539.
10. SEMIGROUP PRESENTATIONS Nikola Ruskuc A Thesis Submitted for the Degree of PhD at the University of St. Andrews.
11. American Mathematical Society Translations Series2, Volume 15. 1960
12. Applied Discrete Structures By K. D. Joshi .
13. Subgroups of Free Idempotent Generated Semigroups need not be Free, Mark Brittenham, Stuart W. Margolis, & John Meakin.
14. Multiplicative Subgroups of Z_n by Stanley E. Payne(10th October, 1995)