International Journal of Mathematics and Statistics Invention (IJMSI)
ISSN (Online): 2321 – 4767, ISSN (Print): 2321 – 4759
www.ijmsi.org ||Volume 6 Issue 4 ||April. 2017 || PP.23-25

On Some Notable Properties of Zero Divisors in the Ring of Integers Modulo m (□$_m$, +, ×)

Amina Muhammad Lawan (Ph. D)
(*Department of Mathematical Sciences, Bayero University, Kano, Nigeria*)

Abstract: *The algebraic structure (□$_m$, +, ×) is a commutative ring with unity. When we examine the multiplicative structure (□$_m$, ×) we noticed that the product of some two non-zero elements is zero, thus the ring*
(□$_m$, +, ×) has zero divisors. In this study, we made some observations on some of the theorems regarding the zero divisors of the ring (□$_m$, +, ×).We established some of the properties of the zero divisors of (□$_m$, +, ×) . Our results showed that, For an even integer $m \geq 6$ at least one of the quadratic residues modulo m in (□$_m$, +, ×) is a zero divisor also for an odd composite non-perfect square $m \geq 15$ at least three of the quadratic residues are zero divisors. Furthermore, we have found that if m is composite and can be written as a power of prime p, that is $m = p^{\alpha}$ where $\alpha \geq 2$ then:

1. Zero divisors in □$_m$ are multiples of prime p.

2. Let D denote the set of zero divisors in (□$_m$, +, ×) and $\mathrm{D}^{+} = \mathrm{D} \cup \{0\}$, then (a) (D$^+$, +) is a cyclic group generated by p (b) (D$^+$, +, ×) is a cyclic ring (c) (D$^+$, +, ×) is a subring of
(□$_m$, +, ×) (d) (D$^+$, +, ×) is an ideal of (□$_m$, +, ×) (e) (D$^+$, +, ×) is a principal ideal
(f) (D$^+$, +, ×) is a prime ideal (g) (D$^+$, +, ×) is a maximal ideal.(h) (□$_m$, +, ×) is a local ring.

Keywords: *composite integer, quadratic residue modulo m, relatively prime integers, ring of integers modulo m, zero divisor*

I. INTRODUCTION

We have been taught in algebra that, whenever we have $x \times y = 0$ for some real numbers *x, y* then either $x = 0$ or $y = 0$. We cannot make this conclusion in any ring. Some rings may have non-zero elements whose product is zero.

This paper is a study on the zero divisors of the ring of integers modulo m. We were able to establish some number theoretic properties of the set zero divisors of the ring of integers modulo m as well as its structural properties from some existence theorems.

Definitions of some basic terms used were given for easy understanding of the main work. Relevant theorems from which the work is developed were stated. Finally findings/results of the study were presented.

II. PRELIMINARIES

Definition 2.1 (Relatively prime integers): Two positive integers a and b are relatively prime if and only if gcd(a, b)=1

Definition2.2 (Quadratic Residue): An integer q in □$_m$ is called a quadratic residue modulo m if it is congruent to a perfect square modulo m. That is if there exists *x* in □$_m$ such that $x^2 \equiv q \pmod{m}$.

Definition 2.3 (Cyclic group): A group $(\mathrm{G}, *)$ is called cyclic if for some $g \in \mathrm{G}$ every element of G is of the form g^m for *m* in □ then g is called a generator of G and we write $G = \langle g \rangle$ = {g^m : *m* in □ }.□

Definition 2.4 (Ring): Let + and × be binary operations on a non-empty set R. The algebraic structure $(\mathrm{R}, +, \times)$ is called a ring provided the following conditions hold:

R1 : (R , +) is an abelian group.

R2 : (R , ×) is a semigroup.

R3 : The distributive laws hold: $\forall\, a, b, c \in \mathrm{R}$

$(i)\ a \times (b + c) = (a \times b) + (a \times c) \quad (ii)\ (b + c) \times a = (b \times a) + (c \times a)$.

Definition 2.5 (Commutative Ring): A ring (R , +, ×) is said to be commutative if (R, ×) is commutative. That is if $\forall\, a, b \in \mathrm{R}$ we have $a \times b = b \times a$

Definition 2.6 (Zero divisor): Let (R , +, ×) be a be commutative ring with 0 the identity element of the abelian group (R, +). A non-zero element $d \in \mathrm{R}$ is called a zero divisor if there exists non-zero element $q \in \mathrm{R}$ such that $d \times q = 0$.

Definition 2.7 (Subring): Let (R , +, ×) be a ring and S be a non-empty subset of R such that S is a ring with respect to the same binary operations + and × in R. Then (S , +, ×) is a subring of (R , +, ×).

Definition 2.8 (Ideal):An ideal I of a ring (R , +, ×) is a subring such that for all $r \in \mathrm{R}$ and $a \in \mathrm{I}$; we have $a \times r,\ r \times a \in \mathrm{I}$.

Definition 2.9 (Principal Ideal): Let (R , +, ×) be a ring and $a \in \mathrm{R}$, the ideal $\left\langle a \right\rangle = \{ x : x = a \times r = r \times a ,\ r \in \mathrm{R} \}$ is called a principal ideal. That is an ideal generated by one element.

Definition 2.10 (Prime Ideal): Let (R , +, ×) be a commutative ring. An ideal P of (R , +, ×) is called prime provided for every $a \times b \in \mathrm{P}$, either $a \in \mathrm{P}$ or $b \in \mathrm{P}$; for $a, b \in \mathrm{R}$.

Definition 2.11 (Maximal Ideal): A Maximal Ideal of a ring is an ideal that is not contained in any other ideal besides the entire ring.

Definition 2.12 (Local Ring): A local ring is a ring with exactly one maximal ideal.

III. THE RING OF INTEGER MODULO M $(\square_M , +, \times)$

There are two binary operations associated with the set $\square_m$, that of addition and multiplication modulo m. The set of integer modulo m is an additive abelian group. Multiplication is associative, commutative and interacts with addition by means of the distributive property. There is a non-zero element 1 in $\square_m$ such that, for all a in $\square_m$ $1 \times a = a \times 1 = a$ .Thus the structure $(\square_m , +, \times)$ is a commutative ring with unity.

Theorem 3.1: The zero divisors of $(\square_m , +, \times)$ are all non-zero elements that are not relatively Prime to m.

Corollary 3.2: The ring $(\square_p , +, \times)$ with p prime has no zero divisors.

3.1 Some Observations

Based on Theorem 3.1 and Corollary 3.2 we made the following observations:

I. The ring $(\square_m , +, \times)$has zero divisors if m is composite.
II. In the ring $(\square_m , +, \times)$ the elements for which a and m are relatively prime are units.
III. Zero divisors can never be a unit.
IV. In the ring $(\square_m , +, \times)$ every element is either a unit or a zero divisor.
V. The number of zero divisors in $(\square_m , +, \times)$ is $m - (\phi(m) + 1)$.

3.2 Some Notable properties

Q1. What is the inverse of zero divisor in $(\square_m , +, \times)$?

A. Suppose (i) d is a zero divisor in $(\square_m , +, \times)$ such that $d \times d = 0$ then $d + d = 0$.

(ii) d and q are zero divisors in $(\square_m , +, \times)$ such that

$d \times d = 0,\ d \times q = 0$ and $q \times q = 0$ then $d + q = 0$.

(iii) d , q and r are zero divisors in $(\square_m , +, \times)$ such that

$d \times q = 0$ and $q \times r = 0$ then $d + r = 0$ and $q + q = 0$.

Thus the inverse of zero divisor is zero divisor.

Proposition 3.3: An integer a generates $(\square_m , +)$ if and only if gcd(a, m)=1.

Q2. Can zero divisor in $(\square_m , +, \times)$ be a generator of $(\square_m , +)$?

A. Since $(\square_m , +)$ is a cyclic group, it has generators but by proposition 3.3, zero divisor cannot be a generator of $(\square_m , +)$.

Theorem 3.4: At most (m+1)/2 (for m odd) and m/2+1 (for m even) integers in $\square_m$ are quadratic residues modulo m.

Q3. Can zero divisor in $(\square_m , +, \times)$ be a quadratic residue modulo m?

A. Yes, since quadratic residue may be a unit or non-unit element of $\square_m$.

This leads us to come up with the following results:

IV. FINDINGS / RESULTS

Result 4.1: For an even integer $m \geq 6$ at least one of the quadratic residues modulo m is a zero divisor.

Result 4.2: For an odd composite non-perfect square $m \geq 15$ at least three of the quadratic residues are zero divisors.

Result 4.3: If m is composite and can be written as a power of prime p, that is $m = p^{\alpha}$ where $\alpha \geq 2$. Then

1. Zero divisors in $\square_m$ are multiples of prime P.

2. Let D denote the set of zero divisors in $(\square_m , +, \times)$ and $D^{+} = D \cup \{0\}$, then

(a) $(D^{+} , +)$ is a cyclic group generated by p.
(b) $(D^{+} , +, \times)$ is a cyclic ring.
(c) $(D^{+} , +, \times)$ is a subring of $(\square_m , +, \times)$.
(d) $(D^{+} , +, \times)$ is an ideal of $(\square_m , +, \times)$.
(e) $(D^{+} , +, \times)$ is a principal ideal.
(f) $(D^{+} , +, \times)$ is a prime ideal.
(g) $(D^{+} , +, \times)$ is a maximal ideal.
(h) $(\square_m , +, \times)$ is a local ring.

V. CONCLUSION

The paper finds out many important number theoretic properties of the set of zero divisors in the ring of integers modulo m and would be applicable in cryptography and cryptanalysis.

BIBLIOGRAPHY

[1] A. S. Okoro, Foundation of abstract algebra (Sanjo prints, 2005).
[2] C. K. Taylor, An introduction to abstract algebra (e-book, 2013).
[3] D. S. Dummit and R. Foote, Abstract algebra, 3rd edition (John Wiley and Sons, Inc. Hoboken NJ, 2004).
[4] I. Kenneth and R. Michael , A classical introduction to modern number theory, 2nd edition (New York: Springer, 1990)..
[5] J. B. Fraleigh, A first course in abstract algebra, 7th edition (Addison Wesley, New York, 2003).