زانكۆى صلاح الدين- هەولێر

Salahaddin University-Erbil

On Strongly Unit Elements in The Ring Z_n

Research Project

Submitted to the department of Mathematic in partial fulfilment of the requirements for the degree of BSc. in Mathematic

By

Hozan Shakr Tahr

Supervised by

MS. Suham H. Awla

2022-2023

Certification of the Supervisors

I certify that this work was prepared under my supervision at the Department of Mathematics/ College of Education /Salahaddin University-Erbil in partial fulfillment of the requirements for the degree of Bachelor of philosophy of Science in Mathematics

Signature:
Supervisor : **MS. Suham H. Awla**
Scientific grade: Assist. Professor
Date: 5 /4 /2023

In view of the available recommendations, I forward this work for debate by the examining committee.

Signature :
Name: **Dr. Rashad Rasheed Haje**
Scientific grade: Assist. Professor
Chairman of mathematics Department
Date: 5 /4 /2023

Acknowledgment

I express my deep sense of gratitude and thanks to the Almighty **ALLAH** for

providing me with strength, health, faith, patience, willing and self- confidence to accomplish this study.

My sincere thanks and appreciation are extended to the presidency of Salahaddin University, especially the deanery of the College of Education for their facilities to carry out my research work.

I would like to give special thanks to my supervisor **“Suham H. Awla”** for her constant and valuable guidance and encouragement during my research work. Her attention, support and timely suggestions were useful and the most needed in the preparation of my bachelor thesis.

My deepest thanks go to professor **“Rashad Rasheed Haji”** the head of Mathematics Department of the College of Education, further more I wish to thank the

staff members of the College of Education, especially the library staff of the College of Education.

Hozan Shakr Tahr
2023

Content

Abstract

In this work we study and discuss the concept of strongly unit elements in rings. It is shown that In ring Z_{p^2}, p is prime, unit x is a strongly unit if it is of the from $lp - 1 or\ l\,p + 1$ for $1 \leq l \leq p - 1$.

List of symbols

Symbols	Descriptions
$gcd(a,b)$	Greatest Common Divisors Between a and b
$\forall$	For all
$\in$	Belong to
Ø	Euler’s Phi-Function
Z_n	The Ring of Integers modulo n
$a \equiv b (mod n)$	a is Congruent to b modulo n

Introduction

The study of numbers has always occupied a unique position in the world of mathematics. It may very well be the best subject for a student trying to learn what constitutes a mathematical proof, and to construct the proofs, such as the theories of congruences and prime numbers. Most of the results of this work can be considered as an application of the number theory.

The present work consists of two chapters along with a list of references at the end. The first chapter deals with some definitions and theorems about ring theory and number theory, which are needed in our work.

In chapter two we study the concept of strongly unit elements in the ring Z_n. We prove that Let Z_p be a ring, p is an odd prime. Then a unit x is a strongly unit if and only if $= p - 1$. Also In the ring $Z_{p^2},$, p is prime, a unit x is a strongly unit if it is of the from $lp - 1 or\ lp + 1$ for $1 \leq l \leq p - 1$. Moreover we prove that In the ring Z_{p^3}, p is prime, has at least five strongly units which are $p + 1$, p^2+1 , $p^2+p + 1$, p^2-1 , p^3-p^2-1.

Chapter one

Background

In this chapter we take some known definitions and results that we are needed in our work.

Definition1.1: (John 1982) A binary operation $*$ on a set S is a function mapping $S \times S$ into S. For each $(a, b) \in S \times S$, we will denote the element $*\ ((a, b))$ of S by $a * b$.

Example1.2: Our usual addition + is a binary operation on the set R. Our usual multiplication $\cdot$ is a different binary operation on R.

Definition1.3: (David 1980) Let a and b be given integers, with at least one of them different from zero. the greatest common divisor of a and b, denoted by $gcd(a,b)$, is the positive integer d satisfying the following.

(a) $d|a$ and $d|b$

(b) If $c|a$ and $c|b$ then $c \geq d$

Example1.4: Let $a = 12$, and $b = 3$.then $gcd(12,3) = 12$.

Definition1.5: (John 1982)A ring $(R, +,\cdot)$ is a set R together with two binary operations $+$ and $\cdot$, which we call addition and multiplication, defined on R such that the following axioms are satisfied:

1. $(R, +)$ is an abelian group.

2. Multiplication is associative.

3. For all $a, b, c \in R$, the left distributive law, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the right distributive law $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.

Example1.6: $(\mathbb{Z}, +,\cdot)$ and $(\mathbb{R}, +,\cdot)$ are rings.

Definition 1.7: (David 1980) Let R be a ring with a unity. an element a in R is unit of R if it has a multiplicative invers in R.

Example1.8: Let $\mathbb{R}$ be a ring of real numbers then $2 \in \mathbb{R}$ is unit, since for $\frac{1}{2}$ we have $\frac{1}{2}$. 2=1.

Definition1.9: (Joshi 1989) An element x in a ring R is called a zero - divisor if there exists $y \in R$ such that y 0 and either $xy = 0$ or $yx = 0$.

Example1.10: Let $n = 12$. Then in the ring Z_{12} we have 3 and 4 are different from zero and $3.4 \equiv 0(mod12)$ hence 3 and 4 are divisors of zero.

Definition 1.11: (David 1980) For $n \geq 1$, let $\varphi(n)$ denoted the number of positive integers not exceeding n that are relatively prime to n **.**

Example1.12: $\varphi(30) = 8$ for among the positive integers that do not exceed 30 there are eight that are relatively prime to30 specifically,

1,7,11,13,17,19,23 and 29

Note that if n is a prime number, then every integer less than n is relatively prime to it, whence, $\varphi(n) = n - 1$. For example $\varphi(7) = 6$.

Theorem 1.13: (David 1980) For $n > 2$, $\varphi(n)$ is an even integer.

Theorem 1.14: (David 1980) The linear congruence $ax \equiv b(modn)$ has a solution if and only if $d|b$ where $d = gcd(a, n)$ If $d|b$, then it has d mutually incongruent solutions modulo n **.**

Theorem 1.15: (David 1980) (Euler) If $n \geq 1$,and $gcd(a, n)$=1 ,then $a^{\emptyset(n)} \equiv 1(modp)$

Example 1.16: Let $n = 7$and, Let$a = 5$

Then $gcd(7,5) = 1$ and $\emptyset(7) = 6$ Hence by theorem 1.15,

then $5^6 \equiv 1(mod7)$

Definition 1.17: (A.K.S .Chandra Sekhar Rou n.d.) Let R be a ring, an element x in R is said to be a strongly

unit if there exists an element $y \in R$ such that $xy = 1$ and there are $a, b \in R\backslash\{0, x, y\}$ such that

1. $\boldsymbol{ax = b \ or \ xa = b}$
2. $\boldsymbol{ay = b \ or \ ya = b}$.

Example1.16: Let Z_{42}be a ring. Then 5,11,13,17,19,23,25,29,31,37 and 41 are strongly units.

Solution: In the following we show select the elements $a, b \in Z_{42} \backslash \{0, x, y\}$ such that where $xy \equiv 1(mod\ Z_{42})$, $xa \equiv b(mod\ Z_{42})$ and $ya \equiv b(mod\ Z_{42})$,

$$\mathbf{5.17 \equiv 1(\boldsymbol{mod}42)}$$

$$5.7 \equiv 35(mod42)$$

$$17.7 \equiv 35(mod42)$$

$$\mathbf{11.23 \equiv 1(\boldsymbol{mod}42)}$$

$$11.7 \equiv 35(mod42)$$

$$23.7 \equiv 35(mod42)$$

$$\mathbf{13^2 \equiv 1(\boldsymbol{mod}42)}$$

$$13.7 \equiv 7(mod42)$$

$$\mathbf{19.31 \equiv 1(\boldsymbol{mod}42)}$$

$$19.7 \equiv 7(mod42)$$

$$31.7 \equiv 7(mod42)$$

$$\mathbf{25.37 \equiv 1(\boldsymbol{mod}42)}$$

$$25.7 \equiv 7(mod42)$$

$$37.7 \equiv 7(mod42)$$

$$\mathbf{29^2 \equiv 1(\boldsymbol{mod}42)}$$

$$29.7 \equiv 35(mod42)$$

$$\mathbf{41^2 \equiv 1(\boldsymbol{mod}42)}$$

$$41.7 \equiv 35(mod42).$$

Chapter Two

On Strongly Unit Elements

In this chapter we study and discuss the concept of strongly unit elements in rings.

Proposition 2.1: Let R be a ring. A unit element $x \in R$ such that $x^2 = 1$. Then x is strongly unit.

Proof: Suppose that x is a unit such that $y = x$, then $xy = x^2 = 1$, consider the linear congruence $xa \equiv b(modn)$ ... (1) .

Since x is a unit, then $gcd(x, n) = 1$, then by Theorem 1.14, the linear congruence (1) has a unique solution let be s. hence x is strongly unit of a ring R.

Proposition 2.2: If x is a unit of a ring R, then x^k is strongly unit.

Proof: Let $x \in Z_n$be a unit. Then by Theorem 1.15,

we have

$$x^{\varphi(n)} \equiv 1(mod\ n)$$

and by Theorem 1.13 we have $\varphi(n)$ is an even integer, suppose that $\varphi(n) = 2k, k \in \mathbb{Z}^+$

$$x^{\varphi(n)} = x^{2k} = (x^k)^2 = 1(mod\ n)$$

and by Proposition 2.1, we get x^k is strongly unit of Z_n.

Proposition 2.3: Let Z_p be a ring, p is an odd prime. Then a unit x is a strongly unit if and only if $x = p - 1$.

Proof: Suppose that x is strongly unit .Then $\exists$ y in Z_p such that $xy \equiv 1(mod\ p)$ and $\exists$ $a, b \in \backslash R\{0, x, y\}$ such that

$$xa \equiv b(mod\ p)$$

$$ya \equiv b(mod\ p)$$

since $a \in Z_p$, then a is a unit. we get $x \equiv y(modp)$.

Clearly the only unit x in Z_p such that $x^2 = 1$ is $p - 1$. Hence $x = y = p - 1$. We know that $(p-1)^2 \equiv 1(mod\ p)$. Hence by proposition 2.1, x is strongly unit.

Remark 2.4: For every $x \in Z_p$,p is odd prime, x^k is a strongly unit because every element of Z_p is a unit, then by Proposition 2.1, x is a strongly unit.

Proposition 2.5: In the ring Z_{p^2},, p is prime, a unit x is a strongly unit if it is of the from $lp - 1 or\ lp + 1$ for $1 \leq l \leq p - 1$.

Proof: Let $x \in Z_{p^2}$, such that $x = lp - 1$. Then for $y = (\ p - l)\ \ p - 1$ for $1 \leq l \leq p - 1$.

We have

$$xy = (lp - 1)\big((p - l)p - 1\big)$$

$$= (lp - 1)(\ p^2 - \ lp - 1)$$

$$= l\,p^3 - l^2p^2 - \ lp - p^2 + \ lp + 1$$

$$\equiv 1(mod\ p^2)$$

We take $a = p\ and\ b = p^2 - p$ then $a, b \in Z_{p^2}\backslash\{0, x, y\}$

$$xa \equiv (\ lp - 1)p$$

$$= \ lp^2 - p$$

$$\equiv -p(modp^2)$$

$$\equiv p^2 - p(mod\ p^2)$$

$$ya = \big((p - l)p - 1\big)p$$

$$= \ (p^2 - lp - 1)p$$

$$\equiv -p(mod\ p^2)$$

$$\equiv p^2 - p(mod\ p^2)\ )$$

For $x\ = lp + 1$ then and we take $y = (p - l)p + 1$, for $1 \leq l \leq p - 1$.

$$xy = (lp + 1)\big((p - l)p + 1\big)$$

$$= lp^3 - l^2p^2 + lp + p^2 - lp + 1$$

$$\equiv 1(mod\ p^2)$$

We take $a = p\ and\ b = p$, then $a, b \in Z_{p^2} \backslash \{0, x, y\}$

Now $\quad xa \equiv (\ lp + 1)$

$$= \ lp^2 + p$$

$$\equiv p(mod\ p^2)$$

$$ya = \big((p - l)p + 1\big)p$$

$$= \ (p^2 - \ lp + 1)p$$

$$\equiv p(mod\ p^2)$$

Therefore by Definition 1.16, $l\,p - 1$ and and $lp + 1$ are strongly units of Z_{p^2}

Example 2.6: Let Z_{25} be a ring, then the elements 4,19,6,21,9,14,11,16 and 24 are strongly units.

Solution: In the following we show select the elements $a, b \in Z_{25} \backslash \{0, x, y\}$ such that where $xy \equiv 1(mod\ Z_{25})$, $xa \equiv b(mod\ Z_{25})$ and $ya \equiv b(mod\ Z_{25})$,

$$\mathbf{4.19 \equiv 1(\boldsymbol{mod}\ 25)}$$

$$4.10 \equiv 15(mod\ 25)$$

$$19.10 \equiv 15(mod\ 25)$$

$$\mathbf{6.21 \equiv 1(\boldsymbol{mod}\ 25)}$$

$$6.5 \equiv 5\ (mod\ 25)$$

$$21.5 \equiv 5(mod\ 25)$$

$$\mathbf{9.14 \equiv 1(mod\ 25)}$$

$$9.5 \equiv 20(mod\ 25)$$

$$14.5 \equiv 20(mod\ 25)$$

$$\mathbf{11.16 \equiv 1(mod\ 25)}$$

$$11.5 \equiv 5(mod\ 25)$$

$16.5 \equiv 5(mod\ 25)$ and

$$\mathbf{24^2 \equiv 1(mod\ 25)}$$

$$24.5 \equiv 20(mod\ 25)$$

Proposition 2.7: In the ring Z_{p^3}, p is prime, has at least five strongly units which are $p+1$, p^2+1 , p^2+p+1 , p^2-1 , p^3-p^2-1.

Proof: Let we first proof for $x_1 = p + 1$. Then for $y_1 = p^2 - p + 1$,

We have

$$x_1 y_1 \equiv 1(mod\ p^3)$$

Now we take $a = b = p^2$, then

$$\begin{aligned} xa &= (p^2+1)p^2 \\ &\equiv p^4 + p^2 (mod\ p^3) \\ &\equiv p^2 (mod\ p^3) \end{aligned}$$

For $x_2 = p^2 + 1$, we take $y_2 = p^3 + p^2 + 1$.

We have

$$\begin{aligned} x_2 y_2 &= (p^2+1)(p^3+p^2+1) \\ &\equiv p^5 - p^4 + p^2 + p^3 - p^2 + 1 \\ &\equiv 1(mod\ p^3) \end{aligned}$$

For $a = b = p^2$, we have

$$x_2a = (p^2 + 1\ )p^2$$
$$= p^4 + p^2 (mod\ p^3)$$
$$\equiv p^2 (mod\ p^3)$$
$$y_2a = (p^3 - p^2 + 1)p^2$$
$$= p^5 - p^4 + p^2$$
$$\equiv p^2 (mod\ p^3)$$

For $x_3 = p^2 + p + 1$, we take $y_2 = p^3 - p + 1$, then

$$x_3y_3 = (p^2 + p + 1)(p^3 - p + 1)$$
$$= p^5 - p^3 + p^4 + p^2 - p^2 + p + p^3 - p + 1$$
$$\equiv 1 (mod\ p^3)$$

We take $a = b = p^2$, then

$$x_3a = (p^2 + p + 1)p^2$$
$$= p^4 + p^3 + p^2$$
$$= \ p^2 (mod\ p^3)$$

and $$y_3a = (p^3 - p + 1)p^2$$
$$= p^5 - p^3 + p^2$$
$$= p^2 (mod\ p^3)$$

For $x_4 = p^2 - 1$and $y_4 = p^3 - p^2 - 1$

$$x_4y_4 = (p^2 - 1)(p^3 - p^2 - 1)$$
$$= p^5 - p^4 + p^2 - p^2 - p^3 + 1$$
$$= 1 (mod\ p^3)$$

For $a = p^2$ and $b = p^3 - p^2$, we have

$$x_4a = (p^2 - 1)p^2$$
$$= p^4 - p^2$$

$$\equiv -p^2\ (mod\ p^3)$$

$$\equiv p^3 - p^2\ (mod\ p^3)$$

For $x_5 = p - 1$ and $y_5 = p^3 - p^2 - p - 1$, then

$$x_5 y_5 = (p^3 - p^2 - 1)(p^3 - p^2 - p - 1)$$

$$= p^4 - p^3 - p^2 - p - p^3 + p^2 + p + 1$$

$$\equiv 1(mod\ p^3)$$

For $a = p^2$ and $b = p^3 - p^2$, we have

$$x_5 a = (p - 1)p^2$$

$$\equiv p^3 - p^2\ (mod\ p^3)$$

$$= b$$

$$y_5 a = (p^3 - p^2 - p - 1)p^2$$

$$\equiv p^3 - p^2\ (mod\ p^3)$$

Therefore $x_1, x_2, x_3, x_4,$ and x_5 are strongly units of Z_{p^3}.

Example 2.8: Let Z_{27} be a ring, then the elements 1,2,4,5,7,8,10,11,14,13,16,17,19,20,23,25 and 26 are strongly units.

$$\mathbf{1^2 \equiv 1(\mathit{mod}\ 27)}$$

$$1.17 \equiv 17(mod\ 27)$$

$$\mathbf{2.14 \equiv 1(\mathit{mod}\ 27)}$$

$$2.18 \equiv 9(mod\ 27)$$

$$14.18 \equiv 9(mod\ 27)$$

$$\mathbf{4.7 \equiv 1(\mathit{mod}\ 27)}$$

$$4.9 \equiv 9(mod\ 27)$$

$$7.9 \equiv 9(mod\ 27)$$

$$\mathbf{5.11 \equiv 1}(\boldsymbol{mod}\ \mathbf{27})$$

$$5.9 \equiv 18(mod\ 27)$$

$$11.9 \equiv 18(mod\ 27)$$

$$\mathbf{8.17 \equiv 1}(\boldsymbol{mod}\ \mathbf{27})$$

$$8.3 \equiv 24(mod\ 27)$$

$$17.3 \equiv 24(mod\ 27)$$

$$\mathbf{10.19 \equiv 1}(\boldsymbol{mod}\ \mathbf{27})$$

$$10.3 \equiv 3(mod\ 27)$$

$$19.3 \equiv 3(mod\ 27)$$

$$\mathbf{13.25 \equiv 1}(\boldsymbol{mod}\ \mathbf{27})$$

$$13.9 \equiv 9(mod\ 27)$$

$$25.9 \equiv 9(mod\ 27)$$

$$\mathbf{16.22 \equiv 1}(\boldsymbol{mod}\ \mathbf{27})$$

$$16.18 \equiv 18(mod\ 27)$$

$$22.18 \equiv 18(mod\ 27)$$

$$\mathbf{20.23 \equiv 1}(\boldsymbol{mod}\ \mathbf{27})$$

$$20.9 \equiv 18(mod\ 27)$$

$$23.9 \equiv 18(mod\ 27)$$

$$\mathbf{26^2 \equiv 1}(\boldsymbol{mod}\ \mathbf{27})$$

$$26.3 \equiv 24(mod\ 27).$$

Remark 2.9: We obtain a result that in a ring Z_n, where

$n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}{p_3}^{\alpha_3} \ldots {p_r}^{\alpha_r}$, p_i are odd primes, for $i = 1, \ldots, r$, $\alpha \geq 2$

every unit is a strongly unit.

References:

n.d. "A.K.S .Chandra Sekhar Rou." *On Smarandache Semi Groups.*

David, M. B. 1980. *Elementary Number Theory.* USA: Carl Lindbolm.

John, B.F. 1982. *A First Course in Abstract Algebra.* USA: Canada.

Joshi, K D. 1989. *Foundation of Discrete Mathematics.* india.

پوختە

لەو ئیشەماندا ئێمە بەداداچونمان بۆ دانەی یەکانەی بەهێزمان کردووە و گفتوگۆمان لەسەر کردووە.

لە ئەڵقەکاندا ئەوەمان نیشانداوە کە لە Z_{p^2} کاتێ p زمارەیەکی خۆبەشە ژمارەیەکی یەکاکانی x ،

دەبێتە یەکەکانی بەهێزئەگەر لەسەر شێوەی $lp-1$ یان $lp+1$ کاتیک $1 \leq l \leq p-1$.