ON RING HOMOMORPHISMS AND SOME PROPERTIES AMONG INTEGER RINGS

Mohammed Faisal Alrashdi
Department of Mathematics, Faculty of Sciences, King Abdulaziz University, KSA.
mfrshedi@gmail.com

Abstract

The principle propose of this paper is to give some solutions of $Lcm(u, n) \equiv 0 \bmod m$ and determine the number of ring homomorphisms from Z_n to Z_m as additive groups and as rings by using elementary results of number theory. We also introduce and investigate some properties of the class of ring homomorphisms from Z_n to Z_m.

Keywords: ring; homomorphism; ideal.

AMS classification: Primary 08E20, 19L20; 20M12.

1 Introduction

Algebraic number theory is a branch of number theory that uses the techniques of abstract algebra to study the integers, rational numbers, and their generalizations. Number-theoretic questions are expressed in terms of properties of algebraic objects such as algebraic number fields and their rings of integers,homomorphisms, finite fields, and function fields. These properties, such as whether a ring admits unique factorization, the behavior of ideals, and the Galois groups of fields, can resolve questions of primary importance in number theory, like the existence of solutions to Diophantine equations. Gallian and James in 1984, [5], studied and introduced the number of ring homomorphisms from Z_n to Z_m as additive groups and as rings by using elementary results of number theory. In order to determine the number of homomorphisms, we do not need to assume previous knowledge from group theory or ring theory, except for the definition of group and ring homomorphism. With respect to number theory, we use some elementary facts on congruences, which can be found on any introductory book such as [7]. Also, although our results are basically the same as those in [5, 1], our proofs are much more basic.

2 Prelimeries

Definition 2.1. *According to Rotman and Joseph [8], a ring R is a triple* $(R, +, \bullet)$ *consisting of a non-empty set* R *together with two binary operations of addition and multiplication such that*

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

(2) Multiplication is associative i.e $\forall a, b, c \in R,\ a(b+c) = ab + ac$ *and*

$$a(b+c) = ab + ac. \textit{ The left and right distributive laws respectively.}$$

Definition 2.2. *A commutative ring is a ring* R *in which* $\forall a, b \in R,\ ab = ba$.

Definition 2.3. *A division ring is a ring* R *with identity and every non zero element is a unit. A unit is an element* $r \in R$ *that is invertible.*

Definition 2.4. *An ideal of a ring* R *is a subring* I *such that* $r \in R$ *and* $a \in I$, $ar,\ ra \in I$. *It is a left (right) ideal if* $ra \in I (ar \in I)$ *for all* $r \in R$ $a \in I$

Definition 2.5. *Maximal ideal* I *of a ring* R *is an ideal that is not properly contained in any other ideal of* R. *If* J *is another ideal of* R, *then* $J \subset I \subset R,\ J = I$ *or* $I = J$.

Definition 2.6. *A principal ideal is an ideal generated by a single element.*

Definition 2.7. *Let* R *and* S *be rings, a ring homomorphism is a mapping* $\phi : R \to S$ *such that* $\forall r_1, r_2 \in R,\ \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ *and* $\phi(r_1 r_2)\phi(r_1)\phi(r_2)$. *A monomorphism is a homomorphism that is injective (one to one).*

An epimorphism is a homomorphism that is surjective (onto). An isomorphism is a bijective homomorphism (both one to one and onto). An endomorphism is a homomorphism from a ring R into a ring itself $\phi : R \to R$ The kernel of a homomorphism $\phi : R \to S$, denoted ker ϕ is the set of elements of R mapped onto the identity element of S by ϕ, [9].

3 Some solutions of $lcm(u, n) \equiv 0 \bmod m$

In the section we will to find the solutions of $lcm(u, n) \equiv 0 \bmod m$. Suppose $lcm(u, n) \equiv 0 \bmod m$. Since $m\ lcm(u, n)$, then

$$m\ un \Leftrightarrow m | lcm(\frac{m}{gcd(m, n)}, n).$$

That means

$$m\ lcm(\frac{m}{gcd(m, n)} \cdot gcd(\frac{m}{gcd(m, n)}, n), n).$$

Therefore, the solutions given by:

$$u = \frac{m}{gcd(m, n)} \cdot gcd(\frac{m}{gcd(m, n)}, n) \cdot r$$

where

$$0 \leqslant r \leqslant \frac{gcd(m, n)}{gcd(\frac{m}{gcd(m,n)} \cdot gcd(\frac{m}{gcd(m,n)}, n), n)}$$

and n, m any number in N.

Lemma 3.1. *The solution of* $lcm(u, n) \equiv 0 \bmod m$ *is given by*

$$u = \frac{m}{gcd(m, n)} \cdot gcd(\frac{m}{gcd(m, n)}, n) \cdot r$$

where

$$0 \leqslant r \leqslant \frac{gcd(m,n)}{gcd(\frac{m}{gcd(m,n)} \cdot gcd(\frac{m}{gcd(m,n)}, n), n)}$$

and n, m *any number in* N.

Example 3.2. *The solution of* $lcm(u, 12) \equiv 0 \bmod 30$ *is given by*

$$u = r \cdot (\frac{30}{gcd(30,12)}) \cdot gcd(12, \frac{30}{gcd(30,12)}) = r \cdot 5 \cdot 1 = 5r$$

where $0 \leqslant r \leqslant \frac{gcd(12,30)}{gcd(5,30)}$. *Therefore, the solutions are* $\{0, 5, 10, 15, 20, 25, 30\}$.

Example 3.3. *To solve* $lcm(u, 30) \equiv 0 \bmod 140$, *note that* $30u \equiv 0 \bmod 140$. *It clearly* $u = 14$,*then* 14 *is a solution. But is not solution of* $lcm(u, 30) \equiv 0 \bmod 140$. *This will make it easier for us in the next sections.*

$$u = r \cdot (\frac{140}{gcd(30,140)}) \cdot gcd(30, \frac{140}{gcd(30,140)}) = r \cdot 14 \cdot 2 = 28r$$

where $r \leqslant \frac{gcd(140,30)}{gcd(28,30)}$.*Therefore, The solutions are* $\{0, 28, 56, 84, 20, 112, 140\}$.

Example 3.4. *The solution of* $lcm(u, 12) \equiv 0 \bmod 28$ *is given by* $k = \frac{28}{gcd(28,12)} \cdot gcd(7, 12) = 7$. *Hence,* $0 \leqslant r \leqslant 4$ *Therefore, The solutions are*$\{0, 7, 14, 21, 28\}$.

Now let $\phi : Z_n \to Z_m$ be a ring homomorphism and it is clear that ϕ is a group homomorphism such that $\phi(x) = ux, u \in Z_m$. So we will show the following.

Theorem 3.5. *The mapping is* $\phi_u : Z_n \to Z_m$ *such that* $\phi_u(x) = ux : u \in Z_m$ *is a ring homomorphism if and only if Lcm(u,n)* $\equiv 0 \bmod m$.
$u \equiv u^2 \bmod m$.

Proof. Let ϕ_u is a ring homomorphism we need show :

$$Lcm(u, n) \equiv 0 \bmod m.$$
$$u \equiv u^2 \bmod m.$$

Since ϕ_u is a ring homomorphism then u=$\phi_u(1) = \phi_u(1^2) = (\phi_u(1))^2 = u^2$. Therefore, $u = u^2$. Suppose $m \nmid lcm(u, n)$ and since $u = u^2$ then $m \nmid lcm(u^2, n)$. Hence, $m \nmid un : u \in Z_m$. This is contradiction because ϕ is a ring homomorphism. Therefore, $Lcm(u, n) \equiv 0 \bmod m$.

Conversely, let $a, b \in Z_n$ then $\phi_u(a + b) = (a + b)u = ua + ub = \phi_u(a) + \phi_u(b)$. Second let $a, b \in Z_n$ such that $ab = nq + r, where, 0 \leqslant r < n$ then $\phi_u(ab) = u(nq + r) = u^2(nq + r) = u^2nq + u^2r = u^2(ab - nq) = u^2(ab) = ua \cdot ub = \phi_u(a)\phi_u(b)$. Therefore, ϕ_u is a ring homomorphism. □

Example 3.6. *A function* $\phi : Z_{12} \to Z_{30}$ *with* $phi(x) = 10x$ *is ring homomorphism. Note that* $Lcm(10, 12) = 60$. *and* $100 \equiv 10 \bmod 30$.

Lemma 3.7. *The number of ring homomorphism* $\phi : Z_n \to Z_m$ *less than* $\frac{gcd(n,m)}{gcd(n,k)}$ *such that* $gcd(n, m) > 1$

Proof. Since the solutions in $< k = t >= \{kr : r \in Z_m\}$ As you can see in the Figure(1). The number of ring homomorphism less than $| < t > |$, that means

$$\frac{m}{k} = \frac{m}{\frac{m \cdot gcd(k,n)}{gcd(n,m)}} = \frac{gcd(n,m)}{gcd(n,k)}.$$

Therefore, $\frac{gcd(n,m)}{gcd(n,k)} \cdot t = m$. Then the number of ring homomorphism less than $\frac{gcd(n,m)}{gcd(n,k)}$. □

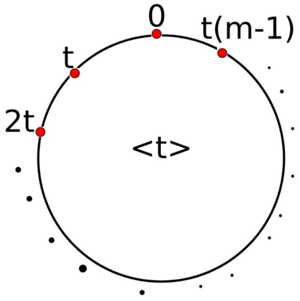

Figure 1: generated by t

Example 3.8. *In example 3.6, we have $< k = 5 >= \{0, 5, 10, 20, 15, 25\}$, it's clearly that, then the number of ring homomorphism less than $\frac{30}{5} = \frac{gcd(12,30)}{gcd(12,5)} = 6$*

Lemma 3.9. *If $gcd(n, m) = 1$, then the number of ring homomorphism $\phi : Z_n \to Z_m$ is one ring homomorphism*

Proof. By Theorem(3.5) $Lcm(a, n) \equiv 0 \bmod m$. Since $gcd(n, m) = 1$, then the solution is $a = 0$ that means there is one ring homomorphism (trivial ring homomorphism) ϕ_0. □

Theorem 3.10. *Let $\phi : Z_n \to Z_m$, such that ϕ_a and ϕ_b are ring homomorphism, then $\phi_a \circ \phi_b = \phi_c$ is a ring homomorphism.*

Proof. Let $\phi : Z_n \to Z_m$ with $\phi(x) = ax$ and there are two ring homomorphism ϕ_a and ϕ_b such that $\phi_a(x) = ax$, $\phi_b(x) = bx$ then $(\phi_a \circ \phi_b)(x) = \phi_c(x) = abx$, By Theorem (3.5), since $Lcm(a, n) \equiv 0 \bmod m$ *and* $Lcm(b, n) \equiv 0 \bmod m$ then $Lcm(ab, n) \equiv 0 \bmod m$. Since $a \equiv a^2 \bmod m$ *and* $b \equiv b^2 \bmod m$,then $ab \equiv a^2b^2 \equiv (ab)^2 \bmod m$. Thus ϕ_c is a ring homomorphism. □

As seen in Theorem 3.5 and you have provided examples. It can be difficult to say whether $u^2 = u \bmod m$ is true, especially when dealing with large numbers. Therefore, we will focus on this part to find a solution to the problem.

Theorem 3.11. *Let ϕ be a ring homomorphism from a ring R to a ring S. Then For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$.*

Proof. Let ϕ be a ring homomorphism from $R \to S$. Hence,

$$\phi(\underbrace{r \cdot r \cdot r ... \quad \cdot r}_{n-times}) = \phi(nr) = \underbrace{\phi(r)\phi(r)\phi(r)... \quad \phi(r)}_{n-times} = n\phi(r).$$

Thus $\phi(nr) = n\phi(r)$. □

Corollary 3.12. *Let ϕ be a ring homomorphism from $R \to S$. Hence, $\phi(-r) = -\phi(r) : \forall r \in R$.*

Corollary 3.13. *$\phi_a : Z_n \to Z_m$, $\phi(x) = ax$ is a ring homomorphism then $\overline{a(n-1)} = \overline{-a}$, where $\forall a \in Z_m$.*

In Theorem 3.5, It is easy to find solutions of $Lcm(a,n) \equiv 0 \bmod m$. But not easy to find solutions of $a^2 \equiv a \bmod m$. We know that if t is a solution of $Lcm(a,n) \equiv 0 \bmod m$ and $a^2 \equiv a \bmod m$, then $t = a$ is a solution of $Lcm(a,n) + a \equiv 0 + a^2 \bmod m$. Thus t is a solution of $Lcm(a,n) + a \equiv a^2 \bmod m$. Therefore,

$$\frac{a \cdot n + a \cdot gcd(a,n)}{gcd(a,n)} \equiv a^2 \bmod m$$

$$\frac{a \cdot n + a \cdot gcd(a,n) - a^2 \cdot gcd(a,n)}{gcd(a,n)} \equiv 0 \bmod m$$

$$k(n + gcd(a,n) - a \cdot gcd(a,n)) \equiv 0 \bmod m$$

$$k(n + gcd(a,n) + a(n-1) \cdot gcd(a,n)) \equiv 0 \bmod m$$

$$k \cdot n + k \cdot gcd(a,n) + k \cdot a(n-1) \cdot gcd(a,n) \equiv 0 \bmod m$$

$$gcd(a,n)(k + k \cdot a \cdot n - a \cdot k) \equiv 0 \bmod m$$

$$k \cdot gcd(a,n)(1-a) \equiv 0 \bmod m$$

Therefore, $a = t$ is a solution of $k \cdot gcd(a,n)(1-a) \equiv 0 \bmod m$, $\forall t = a \in Z_m$.

Theorem 3.14. *The mapping is $\phi : Z_n \to Z_m$ such that $\phi(x) = ax : a \in Z_m$ is a ring homomorphism if and only if*

$$\begin{gathered} Lcm(a,n) \equiv 0 \bmod m. \\ k \cdot gcd(a,n)(1-a) \equiv 0 \bmod m \, : \, k = \tfrac{m}{gcd(n,m)} \cdot gcd(\tfrac{m}{gcd(n,m)}, n). \end{gathered}$$

Example 3.15. *Let $\phi : Z_{1976} \to Z_{2022}$ with $\phi(x) = ax$. Note that $lcm(u,1976) \equiv 0 \bmod 2022. k = \frac{2022}{gcd(2022,1976)} = 1011$, and $gcd(1011,1976) = 1$. Hence, $< 1011 >= \{1011 \cdot r : 0 \leqslant r < 2\}$ Therefore, the solutions of $lcm(u,1976) \equiv 0 \bmod 2022$ are$\{0,1011\}$. Now must we check By $k \cdot gcd(a,n)(1-a) \equiv 0 \bmod m$.*
$(1011) \Rightarrow 1011 \cdot gcd(1011,1976)(1-1011) \equiv 0 \bmod 2022 = 2022 \cdot -505 \equiv 0 \bmod 2022$. *Thus, ϕ_{1011} is ring homomorphism. Therefore, the ring homomorphism are $\{\phi_0, \phi_{1011}\}$.*

Corollary 3.16. *The mapping is $\phi : Z_n \to Z_m$, such that $\phi(x) = ax : a \in Z_m$ is a ring homomorphism if and only if*

$$k|a \text{ and } k \cdot gcd(a,n)(1-a) \equiv 0 \bmod m \, : \, k = \tfrac{m}{gcd(n,m)} \cdot gcd(\tfrac{m}{gcd(n,m)}, n).$$

Corollary 3.17. *The mapping is $\phi : Z_n \to Z_m$ such that $\phi(x) = ax : a \in Z_m$ is a ring homomorphism if and only if*

$$k|a \text{ and } gcd(a,n)(1-a) \equiv 0 \bmod \tfrac{m}{k} \, : \, k = \tfrac{m}{gcd(n,m)} \cdot gcd(\tfrac{m}{gcd(n,m)}, n).$$

Example 3.18. *Let* $\phi : Z_{1998} \to Z_{45660}$ *with* $\phi(x) = ax$*. Note that* $lcm(u, 1998) \equiv 0 \bmod 45660.k = \frac{45660}{gcd(1998,45660)} \cdot gcd(\frac{45660}{gcd(1998,45660)}, 1998) = 15220$*. Hence,* $< 15220 >= \{15220 \cdot r : 0 \leqslant r < 3\}$ *Therefore, the solutions of* $lcm(u, 1998) \equiv 0 \bmod 45660$ *are*$\{0, 15220, 30440\}$*. Now must, we check By* $k \cdot gcd(a, n)(1 - a) \equiv 0 \bmod m$*.*
$(15220) \Rightarrow 15220 \cdot gcd(15220, 1998)(1 - 15220) \equiv 0 \bmod 45660 = 45660 \cdot 2 \cdot -5073 \equiv 0 \bmod 45660$*. Thus,* ϕ_{15220} *is ring homomorphism.*
$(30440) \Rightarrow 15220 \cdot gcd(30440, 1998)(1 - 30440) \equiv 0 \bmod 45660 = 45660 \cdot 2 \cdot -30139 \not\equiv 0 \bmod 45660$*. Thus,* ϕ_{15220} *is not ring homomorphism. Therefore, the ring homomorphism are* $\{\phi_0, \phi_{15220}\}$*.*

Example 3.19. *Let* $\phi : Z_6 \to Z_6$ *with* $\phi(x) = ax$*. Note that*

$$lcm(u, 6) \equiv 0 \bmod 6.k = \frac{6}{gcd(6, 6)} \cdot gcd(\frac{6}{gcd(6, 6)}, 6) = 1.$$

Hence, $< 1 >= \{1 \cdot r : 0 \leqslant r < 6\}$ *Therefore, The solutions of* $lcm(u, 6) \equiv 0 \bmod 6$ *are*$\{0, 1, 2, 3, 4, 5\}$*. Now must, we check By* $k \cdot gcd(a, n)(1 - a) \equiv 0 \bmod m$*.*

(1) $1 \cdot gcd(1, 6)(1 - 1) \equiv 0 \bmod 6 = 1 \cdot 1 \cdot 0 \equiv 0 \bmod 6$*. Thus,* ϕ_1 *is ring homomorphism.*

(2) $1 \cdot gcd(2, 6)(1-2) \equiv 0 \bmod 6 = 1 \cdot 2 \cdot -1 \not\equiv 0 \bmod 6$*. Thus,* ϕ_2 *is not ring homomorphism.*

(3) $1 \cdot gcd(3, 6)(1 - 3) \equiv 0 \bmod 6 = 1 \cdot 3 \cdot -2 \equiv 0 \bmod 6$*. Thus,* ϕ_3 *is ring homomorphism.*

(4) $1 \cdot gcd(4, 6)(1 - 4) \equiv 0 \bmod 6 = 1 \cdot 2 \cdot -3 \equiv 0 \bmod 6$*. Thus,* ϕ_4 *is ring homomorphism.*

(5) $1 \cdot gcd(5, 6)(1-5) \equiv 0 \bmod 6 = 1 \cdot 1 \cdot -4 \not\equiv 0 \bmod 6$*. Thus,* ϕ_5 *is not ring homomorphism.*

Therefore, the ring homomorphism are $\{\phi_0, \phi_1, \phi_3, \phi_4\}$*.*

Corollary 3.20. *The mapping is* $\phi : Z_n \to Z_m$ *such that* $\phi(x) = ax : a \in Z_m$ *is a ring homomorphism if and only if*

$$k \cdot \alpha^2 \equiv \alpha \mod gcd(m, n), \text{ such that } a = k \cdot \alpha. \text{ and } \alpha \in Z_{gcd(m,n)}.$$

4 Determining a ring homomorphism by modified method

Now Let $\frac{m}{k} = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a3} ... \cdot p_n^{a_n}$ consider that from Corollary 3.17 Since multiplying two numbers. Hence the number of solutions is 2^β such that $\beta \leq n$. But from Lemma 3.7 the number of rings homomorphism less than $\frac{gcd(n,m)}{gcd(n,k)}$ and then we have $2^\beta < \frac{gcd(n,m)}{gcd(n,k)}$. Since there is trivial homomorphism ϕ_0. Therefore, $0 < 2^\beta < \frac{gcd(n,m)}{gcd(n,k)} - 1$, such that $\beta \leq n$. We have proved the following theorem.

Theorem 4.1. *The number of ring homomorphisms from* $\phi : Z_n \to Z_m$ *such that* $\phi(x) = ax$ $\forall a \in Z_m$ *is* 2^n *where* $\frac{m}{k} = p_1^{a_1} ... \cdot p_n^{a_n}$*.*

Proof. By Corollary 3.16 and Theorem 4.1 that means the number of ring homomorphisms is 2^n where $\frac{m}{k} = p_1^{a_1} ... \cdot p_n^{a_n}$. □

Corollary 4.2. *The number of ring homomorphisms from* $\phi : Z_n \to Z_n$ *such that* $\phi(x) = ax$ $\forall a \in Z_m$ *is* 2^n *where* $m = p_1^{a_1} ... \cdot p_n^{a_n}$.

Proof. Clearly, it is a special case when $k = 1$.Hence, By Corollary 3.16 and Theorem 4.1 that means the number of ring homomorphisms is 2^n where $m = p_1^{a_1} ... \cdot p_n^{a_n}$. □

According to Gallian and James [5], a ring homomorphis $f : Z_m \to Z_n$ is uniquely determined by the conditions:$mf(1) = 0$ and $f(m) = f(1)$. They stated that in order to find how many ring homomorphisms are there inZ_m into Z_n , one has to count the number of elements of the set $\{e \in Z_n : e^2 = e, \ me = 0\}$.

If $r \equiv k(modm)$ where $0 \leq k \leq m$, then $r \equiv mt + k$ for some $t \in Z$. If f is a ring homomorphism $f(r) = f(mt + k)$

$$r = emt + ek. \ So \ emt = 0, \ em = me = 0 \ and \ er = ek.$$

Again $f(r_1 r_2) = f(r_1)f(r_2), \ er_1 r_2 = (er_1)(er_2) = e^2 r_1 r_2 \ and \ e = e^2, \ i.e. \ e$ is idempotent. For $me = ne = 0(modn)$ and we only check for $e^2 = e$.

Example 4.3. *To determine the number of homomorphisms in:*

(1) $f : Z_{12} \to Z_{28}$.
We have $m = 12, \ n = 28, \ e \in Z_{28}, \ 0 = me = 12e$ *in* Z_{28}. *Iff* $28|12e$ *iff* $7|e$. *So,* $f(1) \in \{0, 7, 14, 21\}$. *Only* 0 *and* 21 *are idempotent in* Z_{28}. *Thus there are* 2 *homomorphisms from* Z_{12} *to* Z_{12}.
Alternatively,
$e \in Z_{28}$ *whose idempotent elements are* $\{0, 1, 8, 21\}$. *Thus* $e \in \{0, 1, 8, 21\}$ $me = 0.e = \{0, 8\}$*, thus there are* 2 *homomorphisms in* $f : Z_{12} \to Z_{28}$.

(2) $f : Z_{12} \to Z_{30}$.
We have $m = 12, \ n = 30, \ e \in Z_{30}$ *whose idempotent elements are* $\{0, 1, 6, 10, 15, 16, 21, 25\}$ $me = 0.e = \{0, 10, 15, 25\}$ *thus there are* 4 *homomorphisms in* $f : Z_{12} \to Z_{30}$.

(3) $f : Z_{16} \to Z_{20}$.
We have $m = 16, \ n = 20$. *Idempotent elements of* Z_{20} *are* $\{0, 1, 5, 16\}, \ e \in \{0, 1, 5, 16\}$ $me = 0, \ e = \{0, 5\}$ *thus there are* 2 *homomorphisms in* $f : Z_{16} \to Z_{20}$.

Einstein [10] on the other hand dealt with finding the number of homomorphisms from a finite field into a ring Z_n . He stated that the only kernels of a ring homomorphism. $\phi : F \to R$ are 0 and F itself, hence there are 2 homomorphisms i.e. 0 map and the identity map. He goes on to explain that they may be less than 2 e.g. in the case where $F = F^2$ and R has an odd order. He further states that they may be more than 2 e.g. in the case where F alone already has a few automophisms or R contains several copies of F.

Holt and Ischwieb [11] states that there can just be the trivial homomorphisms as is the case in $F^3 \to Z$, or there could be many ring homomorphisms as it is the case with $F^2 \to \prod_{i=1}^{\infty} F^2$. They then concluded that there is not a uniform answer for all pairs of fields and rings but it depends on what one wants to get from the homomorphism. Samuel [12] states that, if 1 is mapped onto 1, we can evoke the fact that $Z[x]$ is the free commutative ring with unity on the set $[x]$ and x can be sent to anything. He cited $Z[x] \to Z_{12}$ as an example, where he stated that there are 12 possible homomorphisms with 1 mapped to 1. However, he says that there exists a homomorphism where 1 is not mapped to 1. The important thing is that $f(2)f(x) = f(x)$. If $f(1) = 0$, then $f(x) = 0$. He concluded that if $f(1) = 4,\ f(x) = 8$, and if $f(1) = 9$, then $f(x) = 0, 3, 6$ or 9. Thus, there are 8 additional possible homomorphisms. To get this, he stated that one has to find the values of y such that $f(1)y = y$. .

Theorem 4.4. *Let $f_1(x), f_2(x), ..., f_k(x)$ be polynomials with integral coefficients, and for any positive integer m, let $N(m)$ denote the number of solutions of the system of congruences*

$$f_1(x) \equiv 0\ mod\ m,$$

$$f_2(x) \equiv 0\ mod\ m,$$

$$\vdots$$

$$f_k(x) \equiv 0\ mod\ m.$$

If $m = m_1m_2$ where $(m_1, m_2) = 1$, then $N(m) = N(m_1)V(m2)$. If $m = \prod P^\alpha$ is the factorization of m, then $N(m) = \prod N(P^\alpha)$.

Proof. Suppose that $x \in Z_m$. If $f_1(x) \equiv 0\ mod\ m,\ \ f_2(x) \equiv 0\ mod\ m, \cdots, f_k(x) \equiv 0\ mod\ m$, with $m = m_1m_2$, then $f_1(x) \equiv 0\ mod\ m_1,\ \ f_2(x) \equiv 0\ mod\ m_1, \cdots, f_k(x) \equiv 0\ mod\ m_1$. Let a_1 be the only member of Z_{m_1} for which $x \equiv a_1\ mod\ m_1$. It follows that $f_1(a_1) \equiv 0\ mod\ m_1,\ \ f_2(a_1) \equiv 0\ mod\ m_1, \cdots, f_k(a_1) \equiv 0\ mod\ m_1$. Similarly, there is only one $a_2 \in Z_{m_2}$ such that $x \equiv a_2\ mod\ m_2$, and $f_1(a_2) \equiv 0\ mod\ m_2,\ \ f_2(a_2) \equiv 0\ mod\ m_2, \cdots, f_k(a_2) \equiv 0\ mod\ m_2$. Thus, for each solution of the system of congruences modulo m we have a pair (a_1, a_2), in which ai is a solution of the system of congruences modulo $m_i,\ for\ i = 1; 2$. Suppose now that $m = m_1m_2$, where $(m_1, m_2) = 1$, and that for $i = 1, 2$, the numbers $a_i \in Z_{m_i}$ are such that $f_1(a_i) \equiv 0\ mod\ m_i,\ \ f_2(a_i) \equiv 0\ mod\ m_i, \cdots, f_k(a_i) \equiv 0\ mod\ m_i$. By the Chinese Remainder Theorem, there is only one $x \in Z_m$ such that $x \equiv a_i\ mod\ m_i,\ for\ i = 1, 2$. Then we conclude that $f_i(x) \equiv 0\ mod\ m,\ \ i = 1; \cdots, k$. We have now established a one-to-one correspondence between the solutions x of the system of congruences modulo m and the pairs (a_1, a_2) of solutions of the system of congruences modulo m_1 and m_2. Hence, $N(m) = N(m_1)N(m_2)$. Repeatedly applying this to the prime factorization of m, we obtain the second assertion of the theorem. □

Theorem 4.5. *For any ring homomorphism $\phi : R \to S$, the ker ϕ is an ideal.*

Proof. Let $r_1, r_2 \in ker\phi,\ r \in R,\ \phi(r_1) = \phi(r_2) = 0,\ \phi(r_1 - r_2) = \phi(r_1) - \phi(r_2) = 0 - 0 = 0$ and $\phi(r_1r_2) = \phi(r_1)\phi(r_2) = \phi(r) = 0 = 0$. Thus $r_1 - r_2,\ rr_1,\ r_1r \in ker\phi\ and\ ker\phi$ is an ideal. □

Theorem 4.6. *If I is an ideal of R , then the map $\pi : R \to R/I$ denoted by $\pi(r) = r + 1$ is an epimorphism of rings with $ker\,\pi = 1$.*

Proof. Let $r_1, r_2 \in R,\ \pi : R \to R/I,\ \pi(r_1) = r_1 + 1,\ \pi(r_2) = r_2 + 1$ and and $\pi(r_1 + r_2) = \pi(r_1) + \pi(r_2)$. $\pi(r_1r_2) = \pi(r_1)\pi(r_2)$. □

Theorem 4.7. *If $n \in P^k$, the only homomorphism $\phi_m : Z_n \to Z_n$ are the trivial homomorphism ϕ_0 and ϕ_1, P is a prime.*

Proof. Let $m \in Z_n$ such that $m^2 = m(mod\, n)$. Then $m^2 - m = 0$, $m(m-1) = 0$, $m = 0$ $m-1 = 0$, $m = 1m$ and $(m-1)$ are relatively prime. Hence either $P^k \mid m$ or $P^k \mid (m-1)$. Since $0 < m < P^k = n$, P^k does not divide m and P^k does not divide $(m-1)$. $E(n) = \{0, 1\}$, $\sigma(n) = 2$, meaning there are 2 homomorphisms from $_n$ to Z_n when $n = P^k$ i.e. ϕ_0 and ϕ_1 are the only homomorphism. □

Theorem 4.8. *If $n = P_1^{k_1} P_2^{k_2}$ where p_1 and p_2 are distinct primes, then there are $2^2 = 4$ homomorphisms $\phi_m : {}_n \to {}_n$ namely, $\phi_{(0,0)}, \phi_{(0,1)}, \phi_{(1,0)}, \phi_{(1,1)}$.*

Proof. Let $n = P_1^{k_1} P_2^{k_2}$, for all P_1, P_2 prime and $k_1, k_2 \in Z_n$,.

$$E(n) = E(P_1^{k_1})E(P_2^{k_2}) = \{(0,0), (0,1), (1,0), (1,1)(mod\, P_1^{k_1}, mod\, P_2^{k_2})\}$$

$$\sigma(n) = \sigma(P_1^{k_1})\sigma(_2^{k_2}) = 2 \times 2 = 2^2 = 4.$$

Thus, there are 4 homomorphisms i.e.

$$\phi_{(0,0)}, \phi_{(0,1)}, \phi_{(1,0)}, \phi_{(1,1)}.$$

□

Theorem 4.9. *If $n = P_1^{k_1} P_2^{k_2} P_3^{k_3}$, then there are 2^3 homomorphisms $\phi_m : Z_n \to Z_n$.*

Proof. Let $n = P_1^{k_1} P_2^{k_2} P_3^{k_3}$, for all P_1, P_2, P_3 are distinct prime numbers and $k_1, k_2, k_3 \in Z_n$.

$$E(n) = E(P_1^{k_1})E(P_2^{k_2})E(P_3^{k_3}) = \{0, 0\} \times \{0, 1\} \times \{1, 0\} \cong$$

$$\{(0,0,0), (0,0,1), (0,1,0), (0,1,1) \times (1,0,0), (1,0,1), (1,1,0), (1,1,1)$$

$$(mod\, P_1^{k_1}, mod\, P_2^{k_2}, mod\, P_3^{k_3})\}$$

$$\sigma(n) = \sigma(P_1^{k_1})\sigma(P_2^{k_2})\sigma(P_3^{k_3}) = 2 \times 2 \times 2 = 2^3 = 8.$$

Thus, there are 8 homomorphisms. □

References

[1] Diaz-Vargas, Javier, and G. Vargas de los Santos, The number of homomorphisms from *Z_n to Z_m*, Abstraction Appl 13, (2015): 1–3.

[2] Joseph A Gallian (2021), temporary abstract algebra, Chapman and Hall/CRC.

[3] Wekesa, Jordinah N (2018), The Number of ring homomorphisms from $Z_n \to Z_n$. Diss, Kenyatta University.

[4] Rotman and Joseph J. (2006), A first course in abstract algebra with applications, N.J Pearson, Upper Saddle River.

[5] Joseph A. Gallian and James Van Buskirk, The number of homomorphisms from $Z_m \rightarrow Z_n$, American Mathematical Monthly, 91 (1984): 196–197.

[6] Niven I., Zuckerman H. S. and Montgomery H. L.(1991), An Introduction to the Theory of Numbers, Fifth Edition, John Wiley and Sons, Inc.

[7] I. Niven, H. S. Zuckerman and H. L. Montgomery, An Introduction to the Theory of Numbers, Fifth Edition, John Wiley and Sons, Inc., 1991.

[8] Rotman and Joseph J. (2006), A first course in abstract algebra with applications, N.J Pearson, Upper Saddle River.

[9] John B. F. (1984), A first course in abstract Algebra ($2^{nd}ed$), Addison, U.S.A.

[10] Hagen Van Einstein (2004), Number of homomorphism from a finite field into a ring, MSE.

[11] Derik H. (2014), Number of homomorphism from a finite field into a ring, Math stack exchange.

[12] Matt Samuel (2013), Number of homomorphisms from $Z_n \rightarrow Z_n$, pacific journal of mathematics, MSE vol. 2.