Investigation of solutions to the equation $x^{\ell+1} \equiv x \pmod{n}$

Jung Hyo Koo

May 6, 2011

1 Abstract

This paper will study the solutions to the equation $x^{\ell+1} \equiv x \pmod{n}$. The topic will be approached in three ways. First, we will fix $\ell = 1$ and study the characteristics of idempotents. Secondly, we will let ℓ vary within the positive integers and find characteristics of the roots to the equation. Lastly, we will use the previous results to study subsets of $\mathbb{Z}_n$ that are cyclic groups under multiplication having powers of odd primes as orders and show exactly how many such subsets qualify as groups.

2 Introduction

The paper will be divided into three main parts: The study of Idempotents which are solutions to the equation when $\ell = 1$, the study of $E(n)$ which are solutions to the equation for any $\ell \in \mathbb{Z}^+$, and the analysis of $C(n, q)$, the number of subsets which are cyclic groups under multiplication of order q. The first section will start by fixing $\ell = 1$ and studying the idempotents in $\mathbb{Z}_n$. A method will be generated in which every single idempotent for any given positive integer can be found and operations that preserve idempotents will be studied. Furthermore, idempotents will be generalized from context of $\mathbb{Z}_n$ to Boolean rings to arrive at the result that every finite Boolean ring is isomorphic to a chain of $\mathbb{Z}_2$s, i.e. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$. Then, letting ℓ vary among postive integers, a relationship between the number of solutions to the equation and the Euler ϕ function will be explored. This will be further studied to give two major characterics for solutions to the equation. The last section will be devoted to analyzing the subsets of $\mathbb{Z}_n$ that are groups of a given order. The analysis will end with a final theorem

showing exactly how many subsets of $\mathbb{Z}_n$ are groups of order q^f for an odd prime q and a positive integer f.

3 Preliminaries, fundamentals and notation

The reader is assumed to have moderate knowledge and understanding in number theory and abstract algebra. To aid the reader, here are a list of definitions and theorems that will be vital in understanding this paper. These will be applied and referred to frequently.

Theorem 1. *(Fundamental Theorem of Arithmetic) Any positive integer can be uniquely represented as a product of primes, i.e.* $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ *where* p_i *is a prime and* e_i *is a positive integer for* $1 \leq i \leq k$. [1]

As will be discussed later in this section, Theorem 1 will be of enormous importance when it is used with the Chinese Remainder Theorem.

Theorem 2. *(Chinese Remainder Theorem) Let* $k = mn$ *where* $m, n, k \in \mathbb{Z}^+$ *and* $(m, n) = 1$. *Then there exists a ring isomorphism from* $\mathbb{Z}_k$ *to the cartesian product of* $\mathbb{Z}_m$ *and* $\mathbb{Z}_n$, *namely* $f(x) = (|x|_m, |x|_n)$.

Proof. To prove the Chinese Remainder Theorem it is sufficient to show for all a and b, there exist an x that satisfies $a = |x|_n$ and $b = |x|_m$ and that this x is unique. To prove the existence, let us start by noting that since m and n are relatively prime, there exist integers ℓ and k that satisfy $m\ell + nk = 1$. Observe that $m\ell = 1 \pmod{n}$ and $nk = 1 \pmod{m}$. From this it follows that $am\ell + bnk$ is $a \pmod{n}$ and $b \pmod{m}$. Thus we can conclude that such an x exists. To prove the uniqueness, let us assume c and d both satisfy as x. Since both c and d are $a \pmod{n}$ and $a \pmod{m}$. We know that $n \mid c - d$ and $m \mid c - d$. Since n and m are relatively prime we know that $mn \mid c - d$. Thus $c - d \equiv 0 \pmod{k}$ and $c \equiv d \pmod{k}$. □

Definition 1. *(Group) A group is defined as a set with a binary operation that satisfies three axioms:*
1) The operation is associative;
2) These exist an identity element;
3) Every element has an inverse.

[1] Refer to page 51 of "An Introduction to Higher Mathematics" by Patrick Keef, David Guichard and Russ Gordon for a proof of this theorem[2]

A group is called abelian if any two elements commute, ie, for any $a, b \in G$, $ab = ba$.

Notice that $\mathbb{Z}, \mathbb{Z}_n$ are groups under addition and $\mathbb{U}_n, \mathbb{Z}_n^*$ are groups under multiplication. All of these groups are abelian. All of the groups that will be considered in the paper will be abelian groups.

Definition 2. *(Ring) A ring is defined as a set with two operations called addition and multiplication which follow the following three axioms:*
1) It is an abelian group under addition;
2) Multiplication is associative;
3) Multiplication is distributive over addition.

Definition 3. *(Subring) A non-empty subset A of R is called a subring if it satisfies the following conditions:*
1) A is closed under addition;
2) A is closed under multiplication;
3) A is closed under negatives.

Conditions 1) and 3) can be combined to say that A is closed under subtraction. Thus A is a subring if it is closed under subtraction and multiplication.

In particular, we call a ring containing a multiplicative identity a ring with unity. In addition, if every element commutes under multiplication we call it a communitive ring. This paper will only be concerned with communitive ring with unity. Notice that $\mathbb{Z}, \mathbb{Z}_n$ are commutative rings with unity.

Definition 4. *(Isomorphism) An isomorphism is a bijective function from one group or a ring to another that preserves the operations of the group or the ring. Notation for an isomorphism is $\cong$. For example, if a ring H is isomorphic to a ring G, it is written as $H \cong G$*

The Fundamental Theorem of Arithemetic and the Chinese Remainder Theorem play a big role in this paper. From Theorem 1 we know that any positive integer n can be uniquely prime decomposed into $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where p_i is a prime and e_i is a positive integer for $1 \leq i \leq k$. Then from Theorem 2 we know there exist a ring isomorphism between $\mathbb{Z}_n$ and the cartesian products of $\mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$. This tells us that any x will satisfy $x^{\ell+1} \equiv x \pmod{n}$ if and only if it satisfies $x^{\ell+1} \equiv x \pmod{p_i^{e_i}}$ for

each $i = 1, 2 \cdots k$. Thus, prime decomposing n, we can look at the roots one prime at a time and then use the Chinese Remainder Theorem to combine all the roots mod n.

4 Introduction to E and σ notation and their basic properties

We will now consider some notation that will be important for our investigations.

Definition 5. *For a positive integer n, let $E(n, \ell)$, $E(n)$, $\sigma(n, \ell)$ and $\sigma(n)$ be defined as follows:*
For a given $\ell \in \mathbb{Z}^+$ we let, $E(n, \ell) = \{x \in \mathbb{Z}_n : x^{\ell+1} \equiv x \ (mod\ n)\}$
Similarly, let $E(n) = \{x \in \mathbb{Z}_n : x^{\ell+1} \equiv x \ (mod\ n)$ for some $\ell \in \mathbb{Z}^+\}$
To represent the size of these sets, we use the following notation
$\sigma(n, \ell) = |E(n, \ell)|$ and $\sigma(n) = |E(n)|$.

Theorem 3. *If $k = mn$ and m and n are relatively prime, that is $(m, n) = 1$, then $E(k, \ell)$ is in one-to-one correspondence with $E(n, \ell) \times E(m, \ell)$*

Proof. This directly follows from the Chinese Remainder Theorem. The theorem states that there exist an isomorphism between $\mathbb{Z}_k$ and $\mathbb{Z}_n \times \mathbb{Z}_m$, namely the function that takes an element of $\mathbb{Z}_k$ and reduces it mod n and mod m. It follows that any x that satisfies $x^{\ell+1} \equiv x \pmod{k}$ will satisfy the same equation mod n and m. And if x satisfies $x^{\ell+1} \equiv x \pmod{m}$ and $\pmod{n}$, x will satisfy $x^{\ell+1} \equiv x \pmod{k}$ □

Corollary 4. *If $k = mn$ and m and n are relatively prime positive integers then*

$$\sigma(k, \ell) = \sigma(m, \ell)\sigma(n, \ell)$$

Proof. This follows trivially from Theorem 3. From Theorem 3, there exist a function that maps every element in $E(k, \ell)$ to an unique element in $E(m, \ell) \times E(n, \ell)$ and vice versa. It follows that the sizes of these two sets are the same. It can be concluded that $\sigma(k, \ell) = \sigma(n, \ell)\sigma(m, \ell)$. □

Similarly, if the conditions in Theorem 3 are met, $\sigma(k) = \sigma(n)\sigma(m)$. Generalizing Theorem 3 and Corollary 4 when $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ shows that $E(n)$ is in one-to-one correspondence with $E(p_1^{e_1}) \times E(p_2^{e_2}) \times \cdots \times E(p_k^{e_k})$ and $\sigma(n) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_k^{e_k})$. From here on, $\simeq$ will be used to indicate that two sets are in one-to-one correspondence.

5 Study of Idempotents

This section will be dedicated to examining properties of solutions to the equation when ℓ is fixed at 1. Analyzing solutions to $x^2 \equiv x \pmod{n}$ will show that roots to this particular equation has many interesting properties. Let us begin with a definition.

Definition 6. *(Idempotent) An element of $\mathbb{Z}_n$ is an itempotent if it is a root to the equation $x^{\ell+1} \equiv x \pmod{n}$ when $\ell = 1$. The collection of idempotents can be written as $E(n, 1)$*

For examples if $n = 12$, then there are 4 idempotents.
In $\mathbb{Z}_{12}$;

$0^2 = 0$ $1^2 = 1$ $2^2 = 4$ $3^2 = 9$
$4^2 = 4$ $5^2 = 1$ $6^2 = 0$ $7^2 = 1$
$8^2 = 4$ $9^2 = 9$ $10^2 = 4$ $11^2 = 1$

So there are 4 idempotents: 0,1,4,9.

Lemma 5. *Let $n = p^e$ for a prime p and a positive integer e. Then there are two idempotents in $\mathbb{Z}_n$, namely 0 and 1.*

Proof. To find solutions to $x^2 \equiv x \pmod{n}$, we first use algebra to show that the congruence is equivalent to $x(x-1) \equiv 0 \pmod{n}$. Notice that x and $x-1$ is relatively prime. Thus it cannot be the case that $p|x$ and $p|x-1$. It follows that either $p^e|x$ or $p^e|x-1$. Thus the only possible solutions to the equation are 0 and 1. □

Thus this lemma shows that $E(p^e, 1) = \{0, 1\}$ and $\sigma(p^e, 1) = 2$. Now, recall that from Theorem 4 we have concluded that $\sigma(n) = \sigma(p_1^{e_1}) \cdots \sigma(p_k^{e_k})$. With the knowledge that $\sigma(p_i^{e_i}, 1) = 2$ we can find out exactly how many idempotents n would have.

Theorem 6. *If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then $\mathbb{Z}_n$ has 2^k idempotents.*

Proof. We know that $\sigma(n, 1) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \ldots \sigma(p_k^{e_k})$, since primes to different powers are relatively prime to each other. Also from Lemma 5, we know that $E(p^e, 1) = \{0, 1\}$ thus $\sigma(p^e, 1) = 2$. Thus $\sigma(n, 1) = 2^k$. □

Let us take $n = 12$, for example. Prime decomposition gives us $12 = 2^2 * 3$. Thus $\sigma(12, 1) = \sigma(2^2, 1)\sigma(3, 1) = 2*2 = 4$. We also know that $E(12, 1) = E(2^2, 1) \times E(3, 1)$. From the Lemma 5 we know that both 2^2 and 3 have two idempotents, 1 and 2. Thus $E(12, 1) = E(2^2, 1) \times E(3, 1) = \{0, 1\} \times \{0, 1\}$. Thus the four idempotents are (0,0), (0,1), (1,0) and (1,1) (mod 4, mod 3).

(0,0) corresponds to 0, (1,0) corresponds to 9, (0,1) corresponds to 4, and (1,1) corresponds to 1. This is in accordance with 0,1,4 and 9 that we have found to be idempotents of 12 in the beginning of the section. The same method can be generalized for when $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.

$$\begin{aligned} E(n,1) &= E(p_1^{e_1}) \times E(p_2^{e_2}) \times \cdots \times E(p_k^{e_k}) \\ &= \{0,1\} \times \{0,1\} \times \cdots \times \{0,1\} \\ &\simeq \{(0,0\cdots 0),(0,0\cdots 1),\cdots,(1,0\cdots 1),(1,1\cdots 1)\} \end{aligned}$$

Recall that the Chinese Remainder Theorem describes the isomorphism between the cartesian products of $\mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$ and $\mathbb{Z}_n$. Let us do another example and let $n = 30$. We know 30=2*3*5

$$\begin{aligned} E(30,1) &= E(2,1) \times E(3,1) \times E(5,1) \\ &= \{0,1\} \times \{0,1\} \times \{0,1\} \\ &\simeq \{(0,0,0),(1,0,0),(0,1,0)(0,0,1),(1,1,0),(1,0,1),(0,1,1),(1,1,1)\} \end{aligned}$$

From the Chinese Remainder Theorem (0,0,0)↔1, (1,0,0)↔15, (0,1,0)↔10, (0,0,1)↔6, (1,1,0)↔25, (1,0,1)↔21, (0,1,1)↔16. Thus it can be concluded that $E(30,1) = \{0,1,6,10,15,16,21,25\}$. Likewise, idempotents for any n can be found through this process.

Definition 7. *Let, $x, y, z \in \mathbb{Z}_n$, then define three operations, $x \wedge y$, $x \vee y$ and x^c to be the following.*

$x \wedge y = x * y \qquad x \vee y = x + y - xy \qquad x^c = 1 - x$

With some algebra it can be proven that these operations preserve idempotents.

Theorem 7. *If x and y are idempotents $x \wedge y$, $x \vee y$ and x^c are also idempotents.*

Proof. If $x, y \in E(n,1)$ then we know that $x^2 = x$ and $y^2 = y$ in $\mathbb{Z}_n$. From this we know that $xy = x^2y^2 = (xy)^2$. Thus we know that $x \wedge y$ is an element of $E(n,1)$. Also, $1 - x = 1 - 2x + x^2$ is true since $x = x^2$. Thus x^c is an element of $E(n,1)$. Proving $x \vee y \in E(n,1)$ will use the facts that $x \wedge y$ and x^c preserves idempotents. Since x and y are elements in $E(n,1)$ the above statements tell us that $1 - x$ and $1 - y$ are elements in $E(n,1)$. Also if this is true, from above we know $(1-x)(1-y)$ is in $E(n,1)$. If this is true from above we know $1-(1-x)(1-y)$ is in $E(n,1)$. $1-(1-x)(1-y) = x+y-xy$ thus $x \vee y$ is in $E(n,1)$.

□

To use the example of $E(30,1) = \{0,1,6,10,15,16,21,25\}$. It can be observed that in $\mathbb{Z}_{30}$

$$1-6=-5=25 \qquad 1-10=-9=21$$
$$1-15=-14=16 \qquad 6*10=60=0$$
$$15*21=315=15 \qquad 15+25-15*25=-335=25$$
$$6+10-6*10=-44=16 \qquad 16*21=336=6$$

Likewise, going through all the possible combinations could also show that these operations preserve idempotents.

Note that these operations are very reminiscent of set operations: union, intersection, complements among sets. It is because these operations are very similar to set operations with sets that have two elements, 0's and 1's. To proceed by example, let $n = 30$. As shown above,
$E(30, 1) = \{0, 1, 6, 10, 15, 16, 21, 25\}$ which translates to the cartesian product of $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ in the respective order as

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

We know that the complement of a set consists of everything that is not in the set. In this case, we only have two elements, 0s and 1s. Notice, that 1=(1,1,1) when written in $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. When subtracting anything from (1,1,1), subtracting 1 will give us 0 and subtracting 0 will leave us with 1. It follows that this operation $1-x$ is essentially the same as taking the complement of a set. All the 1's in the cartesian product of x will turn to 0s and 0s will turn to 1s. Similarly, when multiplying, notice that 1*1=1, 0*1=1*0=0 and 0*0=0. It follows that this is very similar to taking the intersection of sets. Unless both x and y have 1's in the $\mathbb{Z}_{p_i^{e_i}}$ the result of multiplication will be 0. Lastly, union of two sets consists of the elements that are contained in either set. 1+1-1*1=1, 1+0-1*0=0+1-0*1=1 and 0+0-0*0=0. This shows that unless both x and y have 0's in the same $\mathbb{Z}_{p_i^{e_i}}$, the result will be 1. Now that we have shown that $1-x$, xy and $x+y-xy$ are similar in structure to taking the complement, intersection and union of sets, we can show that these operations follow some rules we have seen before.

It should also be noted that these operations follow the rules that govern set operations. We know that if x, y and z are sets, the following are true:
$(x^c)^c = x \qquad x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$
$x \cup (y \cap z) = (x \cup y) \cap (x \cup z) \qquad (x \cup y)^c = x^c \cap y^c \qquad (x \cap y)^c = x^c \cup y^c.$
It is also the case that these operations as we have defined them, follow the exact same rules.

Theorem 8. *The operations defined in definition 7 satisfy the set operation rules*

Proof. Let x, y, z be idempotents.
Notice $(x^c)^c = (1-x)^c = 1-(1-x) = x$. Thus $(x^c)^c = x$.
With some algebra we can see that $x \wedge (y \vee z) = x \wedge (y+z-yz) = xy + xz - xyz = xy + xz - x^2yz = xy \vee xz = (x \wedge y) \vee (x \wedge z)$. Thus intersection is distributive over union.
Because $(x \vee y) \wedge (x \vee z) = (x+y-xy) \wedge (x+z-xz) = x^2+xz-x^2z+xy+yz-xyz-x^2y-xyz+x^2yz = x^2+yz-xyz = x+yz-xyz = x \vee yz = x \vee (y \wedge z)$, the union is distributive over intersection.
Notice $(x \vee y)^c = 1-(x+y-xy) = 1-x-y+xy = (1-x)(1-y) = x^c \wedge y^c$.
Thus $(x \vee y)^c = x^c \wedge y^c$
Finally, notice $(x \wedge y)^c = 1-xy = 1-x+1-y-(1-x)(1-y) = x^c \vee y^c$.
Thus $(x \wedge y)^c = x^c \vee y^c$. □

Now let us consider idempotents in a general ring. In this section, we will focus on special kind of rings.

Definition 8. *(Boolean ring) A Boolean ring is a ring in which all the elements are idemptents, i.e. R is a Boolean ring if for all x in R, $x^2 = x$.*

Also, we say a commutative, unitary ring R is *decomposable* if there is a ring isomorphism $R \cong S \times T$, where S and T are non-zero, commutative unitary rings. If R cannot be decomposed we say it is indecomposable.

Lemma 9. *If R is decomposable then R has an idempotent e other than 0 and 1.*

Proof. This almost directly follows from the definition of an isomorphism. If R is decomposable, R is isomorphic to the cartesian product of two non-zero communitive unitary rings. Then we know that the ordered pairs $(0,0), (0,1), (1,0), (1,1)$ are all idempotents. □

Next, we will verify that if e is an idempotent of a ring R, then $Re = \{xe : x \in R\}$ is a subring of R. A subring has to be closed under subtraction and multiplication. It is easy to see that Re is non-empty since the additivive identity, 0, will always be in the subring since $0e = 0$. For any $x, y \in Re$ we know $x = x'e$ and $y = y'e$ for some $x', y' \in R$. Since $xy = x'y'e^2 = x'y'e$ we conclude that $xy \in Re$. We also know $x - y = x'e - y'e = (x' - y')e$; since $x' - y' \in R$ we conclude that $x - y \in Re$ thus Re is a subring of R.

Let, R be a commutative unitary ring and e an idempotent of R that is neither 0 nor 1. From Theorem 7 we know that if e is an idempotent,

$e^c = 1 - e$ is an idempotent. Let's call this idempotent f. Since e is neither 0 nor 1, f will not be 0 or 1. Then from what we have proved directly above, we know Re and Rf are both subrings and thus rings. With little algebra, we can show that R is isomorphic to $Re \times Rf$.

Lemma 10. *If $e \in R$ is an idempotent, $e \neq 0, 1$ let $f = 1 - e, S = Re, T = Rf$. Then, $\phi : R \to S \times T$ given by $\phi(x) = (xe, xf)$ is a ring isomorphism.*

Proof. To prove that it is a ring isomorphism we need to prove that it is a bijective homomorphism. To show that it is bijective, we can show that it has an inverse function. Let $\sigma(x, y) = x + y$ for $x \in S$ and $y \in T$ then $\sigma(\phi(x)) = \sigma(xe, xf) = xe + xf = x(e + f) = x$, since $f = 1 - e$. Composing the other way we have, $\phi(\sigma(x, y)) = \phi(x + y) = ((x + y)e, (x + y)f) = (xe + ye, xf + yf)$. Notice that any $x \in S$ can be written as es for some $s \in R$ and any $y \in T$ as tf for some $t \in R$. It follows that $xe = ees = es = x$ and $ye = tfe = t(1 - e)e = t(e - e^2) = t(e - e) = 0$ and that $xe + ye = x$. Similarly $xf + yf = f$, thus it can be concluded that $\phi(\sigma(x, y)) = (x, y)$. For it to be a ring homomorphism it needs to preserve both multiplication and addition, i.e. $\phi(xy) = \phi(x)\phi(y)$ and $\phi(x + y) = \phi(x) + \phi(y)$. Observe that $\phi(xy) = (xye, xyf) = (xye^2, xyf^2) = (xe, xf)(ye, yf) = \phi(x)\phi(y)$ show that it preserves multiplication. $\phi(x + y) = ((x + y)e, (x + y)f) = (xe + ye, xf + yf) = (xe, xf) + (ye, yf) = \phi(x) + \phi(y)$. Thus it is shown that ϕ is a ring isomorphism. □

From these two Lemmas, we conclude that R is decomposable if and only if it has an idempotent e other than 0 and 1.

Theorem 11. *R is decomposable if and only if it has an idempotent e other than 0 and 1.*

Proof. Lemma 9 proves that if R is decomposable, then R has an idempotent e other than 0 or 1. Lemma 10 proves that if R has an idempotent other than 0 and 1, there exist an isomorphism, namely ϕ that makes $R \cong S \times T$ for two rings S and T. From these two lemmas, it follows that R is decomposable if and only if it has an idempotent e other than 0 and 1.

□

From this directly follows the fact that any indecomposable Boolean ring is isomorphic to $\mathbb{Z}_2$. Indecomposable ring has only two idempotents, 0 and 1. Thus an indecomposable Boolean ring has two elements, 0 and 1. Any ring with 2 elements is isomorphic to $\mathbb{Z}_2$. It follows that any indecomposable Boolean ring is isomorphic to $\mathbb{Z}_2$.

Theorem 12. *R has a finite number of idempotents if and only if it is isomorphic to a product $S_1 \times S_2 \times \cdots \times S_j$ where each S_i is indecomposable.*

Proof. Note that R is a communitive ring with unity thus always has 0 and 1 as its elements. Also, observe that if R is isomorphic to a product $S_1 \times S_2 \times \cdots \times S_j$ where each S_i is indecomposable, R will have 2^j idempotents as each S_i has two idempotents. It follows that R will have a finite number of idempotents. Now to show that if R has a finite number of idempotents then it is isomorphic to a product $S_1 \times S_2 \times \cdots \times S_j$ where each S_i is indecomposable, we consider two cases

Case 1) R has two idempotents: If R only has two idempotents, namely 0 and 1, we know from Lemma 9 that it is indecomposable.

Case 2) R has more than two idempotents: This means that R has idempotent other than 0 and 1. Thus it is decomposable into two rings, S_1 and S_2 through the ring isomorphism given in section 3. Observe that every idempotent of R is in one-to-one correspondence to (e, f) where e is an idempotent in S_1 and f is an idempotent in S_2. Then we again consider two cases for each rings S_1 and S_2. By induction, the process can be continued until R is isomorphic to a cartesian product of indecomposable rings.

Thus, R has a finite number of idempotents if and only if it is isomorphic to $S_1 \times S_2 \times \cdots \times S_j$ where each S_i is indecomposable. □

Lemma 13. *If R is isomorphic to $S \times T$, then R is Boolean if and only if S and T are Boolean.*

Proof. R is Boolean iff every element $a \in R$ is an idempotent
iff every elements $(s, t) \in S \times T$ is an idempotent
iff every $s \in S$ and $t \in T$ is an idempotent
iff S and T are Boolean.

□

With the results from these four lemmas, we can reach a theorem

Theorem 14. *A ring is a finite Boolean ring if and only if it is isomorphic to a product $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$*

Proof. Trivially, any finite Boolean ring will have finite idempotents. Thus, applying Theorem 12, we have that any finite Boolean ring, R, is isomorphic to $S_1 \times S_2 \times \cdots \times S_j$ where each S_i is indecomposable. From Lemma 13, we know that if R is isomorphic to any cartesian product of a set of rings, these rings all have to be Boolean, thus we conclude that S_i is a indecomposable

Boolean ring. From Lemmas 9 and 10 we have derived that any indecomposable Boolean ring is isomorphic to $\mathbb{Z}_2$. Thus S_i is isomorphic to $\mathbb{Z}_2$. This proves that any finite Boolean ring is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$. □

This concludes our investigation of idempotents. We have provided a method in which every idempotent can be generated for any given positive integer. We also examined operations resembling set operations of unions, intersections and complements that preserved idempotents. Lastly, we studied characteristics of Boolean rings and concluded that every Boolean ring is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$.

6 Study of $E(n)$

In the previous section, we looked at the roots to $x^{\ell+1} \equiv x \pmod{n}$ by letting $\ell = 1$. In this section, we will broaden our range of ℓ and let it vary within the positive integers. This will let us examine the properties of $E(n)$ and $\sigma(n)$ and find characteristics that elements of $E(n)$ will possess. In order to do so, it is imperative that the reader have an understanding of Euler's phi function, notated as ϕ.

Definition 9. *(Euler phi function) $\phi(n)$ counts the number of elements in $\mathbb{Z}_n$ that are relatively prime to n.*

Note that $\mathbb{U}_n$ is the collection of units in the ring R_n. Thus, letting $R_n = \mathbb{Z}_n$ it is the case that $\mathbb{U}_n$ is the set of all the elements in $\mathbb{Z}_n$ that are relatively prime to n. Thus it follows that $\phi(n) = |\mathbb{U}_n|$.

Lemma 15. *$\phi(p^e) = p^e - p^{e-1}$ when p is a prime and e is a postive integer.*

Proof. The numbers that are not relatively prime to p^e are the multiples of p. The number of multiples of p under p^e were p^{e-1} thus the number of numbers relatively prime to p^e are $p^e - p^{e-1}$. □

For example, let $p^3 = 3^3$. Notice that the numbers that are not relatively prime to $3^3 = 27$ are the multiples of 3, namely 3,6,9,12,15,18,21,24 and 27. Observe that there are nine of them or 3^{3-1} of them. It follows that $\phi(3^3) = 3^3 - 3^2 = 18$.

Lemma 16. *If $m, n \in \mathbb{N}$ and are relatively prime then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. It is sufficient to prove that $\mathbb{U}_m \times \mathbb{U}_n \cong \mathbb{U}_{mn}$. Now let us assume $a \in \mathbb{U}_m$ and $b \in \mathbb{U}_n$. From the Chinese Remainder Theorem we know that the direct product of $\mathbb{Z}_n$ and $\mathbb{Z}_m$ are isomorphic to $\mathbb{Z}_{mn}$. Since a and b are elements of $\mathbb{Z}_n$ and $\mathbb{Z}_m$ that have inverses we know that the ordered pair (a, b) transforms to in $\mathbb{Z}_{mn}$ will have an inverse too which shows that it is in $\mathbb{U}_{mn}$. Also for any element in $\mathbb{U}_{mn}$, we know that since the element is relatively prime to mn, it has to be relatively prime to m and n. Thus any element in $\mathbb{U}_{mn}$ will correspond to (a, b) where a and b are elements of $\mathbb{U}_m$ and $\mathbb{U}_n$ respectivley. Thus the phi function is multiplicative if m and n are relatively prime. □

Combining Lemmas 15 and 16, we can generalized to an arbitrary positive integer n. Note that from the Fundamental Theorem of Arithematic, n can be uniquely prime factored into $n = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$.

Theorem 17. *If* $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ *then*

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$$

Proof. This follows directly from Lemma 15 and Lemma 16. Since we know the phi function is multiplicative for relatively prime numbers and $p_i^{e_i}$ and $p_j^{e_j}$ are relatively prime for all i and j between 1 and k we know $\phi(n) = \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k})$. Then using the Lemma 15, we can compute each $\phi(p_i^{e_i})$ to get $\phi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$. □

Note that we can play around with the equation to get

$$\begin{aligned}\phi(n) &= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= p_1^{e_1-1} p_2^{e_2-1} \cdots p_k^{e_k-1}(p_1 - 1)(p_2 - 1) \cdots (p_k - 1).\end{aligned}$$

Theorem 18. *If* n *is a natural number,* $n = \sum_{d|n} \phi(d)$

Proof. Let us define a function f such that $f : \mathbb{Z}_n \to \{d; d|n\}$ given by $f(x) = \frac{n}{(n,x)}$ where $0 \leq x \leq n-1$ and x is an integer. From this we know that for f to map multiple elements to the a single d, the elements need to satisfy $\frac{n}{(n,x)} = d$. Since n is a constant, we need to find the number of x's that satisfies $(x, n) = k$ where k satisfies $\frac{n}{k} = d$. We know $(n, x) = k$ shows $(\frac{n}{k}, \frac{x}{k}) = 1$ and we can easily see that the easiest x that satisfies this is $x = k$. All the other x's must be some multiple of k, so there exist an integer y that satisfies $ky = x$ and consequently $y = \frac{x}{k}$. Since from above we know $(\frac{n}{k}, \frac{x}{k}) = 1$, y has to be relatively prime to $\frac{n}{k}$ which is d. Since the number of relatively prime numbers to d that are less than d is given by $\phi(d)$

so the function f maps all the numbers in $\mathbb{Z}_n$ to $\{d; d|n\}$ and the number of numbers that gets map to each d is exactly $\phi(d)$, thus $\sum_{d|n} \phi(d) = n$. □

With the basics of the ϕ function covered, we can move to generate a relationship between the ϕ function and $\sigma(n)$. A vital theorem that will help us bridge the gap between ϕ function and $\sigma(n)$ is the Euler's theorem.

Theorem 19. *(Euler's Theorem) If n is a positive integer and $gcd(u, n) = 1$, then $u^{\phi(n)} \equiv 1$ (mod n).* [2]

Now with the Euler's theorem, we have the tools for the following theorem.

Theorem 20. *If p is a prime and e a positive integer, then $E(p^e) = \{0\} \cup \mathbb{U}_{p^e}$ and thus it follows that $\sigma(p^e) = 1 + \phi(p^e)$*

Proof. We know that everything that is relatively prime to p^e is in $E(p^e)$ from Euler's theorem. We also know that any positive power of 0 is 0 thus 0, although it is not relatively prime to p^e is in $E(p^e)$. We now must show that these are the only elements of $E(p^e)$ thus verifying the equation above. To prove this, we need to prove that all the multiples of ps do not satisfy the equation. Let us say $x = yp^j$ where $j < e$ and $(y, p) = 1$. Let us assume that there exists an ℓ that satisfies $x^{\ell+1} \equiv x \pmod{p^e}$. This is same as saying $(yp^j)^{\ell+1} \equiv yp^j \pmod{p^e}$. We know that $k^{j(\ell+1)}p^{j(\ell+1)}$ is divisible by $p^{j(\ell+1)}$ and since $j(\ell + 1) > j$ and $j < e$, $(yp^j)^{\ell+1}$ cannot be equivalent to $yp^j \bmod p^e$. Thus it follows that $\sigma(p^e) = 1 + \phi(p^e)$ □

Moving to generalize this result to $n = p_1^{e_1} p_2^{e_2} .....p_k^{e_k}$. Let us start by introducing a new definition: the unitary divisor.

Definition 10. *(Unitary divisor) We write $d||n$ and call d an unitary divisor of n if $d|n$ and $(d, \frac{n}{d}) = 1$.*

Theorem 21. *If $n = p_1^{e_1} p_2^{e_2} .....p_k^{e_k}$, $\sigma(n)$ can be represented as below*

$$\sigma(n) = \sum_{d||n} \phi(d)$$

[2] Refer to page 87 of "An Introduction to Higher Mathematics" by Patrick Keef, David Guichard and Russ Gordon for a proof of this theorem[2].

Before moving on to the proof of the theorem, observe the similarity betwen Theorem 21 and 18. n is the sum of $\phi(d)$ for all divisors d of n whereas $\sigma(n)$ is the sum of $\phi(d')$ for all unitary divisors d' of n. Let $n = 12$, we have $n = 12 = \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12)$ and $\sigma(12) = \phi(1) + \phi(4) + \phi(3) + \phi(12) = 9$. Now, let us prove Theorem 21.

Proof. Let us start with the Theorem 20 which states that $\sigma(p^e) = 1+\phi(p^e)$. From this it is clear that $\sigma(p_1^{e_1}p_2^{e_2}.....p_k^{e_k}) = (1 + \phi(p_1^{e_1}))(1 + \phi(p_2^{e_2}))....(1 + \phi(p_k^{e_k}))$ since σ is multiplicative. If we write this out we know that there will be 2^k terms since there are k terms multiplied together with each term consisted of two terms added together. Every term in the sum can be represented as $\phi(p_1^{e_1f_1}p_2^{e_2f_2}.....p_k^{e_kf_k})$ where $f_1, f_2.....f_k$ are either 0 or 1. Notice that whether f_i for any $1 \leq i \leq n$ is 0 or 1, $p_1^{e_1f_1}p_2^{e_2f_2}.....p_k^{e_kf_k}$ is always an unitary divisor of n and all the possible combinations of f_is cover all the unitary divisors of n thus it follows that $\sigma(n) = \sum_{d||n} \phi(d)$ □

To give an example of Theorem 21, let $n = 2^2 \times 3 \times 5 = 60$. Note that the unitary divisors of 60 are 1,3,4,5,12,15,20 and 60. It follows that

$$\begin{aligned}\sigma(60) &= \phi(1) + \phi(3) + \phi(4) + \phi(5) + \phi(12) + \phi(15) + \phi(20) + \phi(60)\\ &= 1 + 2 + 2 + 4 + 4 + 8 + 8 + 16\\ &= 45\end{aligned}$$

Let $n = p_1^{e_1}p_2^{e_2}.....p_k^{e_k}$ and $m \in \mathbb{Z}_n$ where the ps are primes and es are positive integers. From Theorem 21, it follows that $m \in E(n)$ if and only if each $p_i^{e_i}$ when $i = \{1, 2, \cdots k\}$ either divides m or is relatively prime to it. Note that every unitary divisor on n is a divisor of n. It follows that Theorem 21 is equivalent to the statement $m \in E(n)$ if and only if the greatest common divisor of m and n is an unitary divisor of n, i.e. $m \in E(n)$ if and only if $gcd(m, n)||n$.

So far in this section, we have analyzed $E(n)$ and $\sigma(n)$ by using the ϕ function. The ϕ function is very useful in discribing $\sigma(n)$, the size of $E(n)$. Moreover, using unitary divisors, we have explored a property of elements in $E(n)$. For the remainder of the section, we will look at an alternate way to think of the elements of $E(n)$ involving groups and investigate another characteristic of elements in $E(n)$.

Definition 11. *(Finite Cyclic Group) A finite Group G is called cyclic if there exist an element, g, such that $G = \{g, g^2, g^3 \cdots, g^{n-1}, g^n\}$ for some positive integer n. Such elements are called generators.*

There are infinite cyclic groups in which every g^n for $n \in \mathbb{Z}^+$ is different, however, in this paper, we will only be concerned with finite cyclic groups. Thus, cyclic groups in this paper will mean finite cyclic groups. In addition we write $< g >$ to represent the set generated by g, i.e. $< g >= \{g, g^2, g^3, g^4 \cdots\}$. With this notation, we say a group, G, is cyclic if and only if there exist some element $g \in G$ such that $< g >= G$.

Theorem 22. *$x \in E(n)$ if and only if $< x >$ (mod n) forms a group under multiplication.*

Proof. This is a biconditional proof, let us start with the proof that if $x \in E(n)$, then $< x >$ is a group under $\mathbb{Z}_n$. Recall from Definition 1 that for $< x >$ to be group it needs to have three properties: associativity, existence of an identity element and existence of inverses for every element in the group. Associativity holds generally for multiplication in $\mathbb{Z}_n$ thus there is no need for a proof. To prove that $< x >$ has the identity we need to use the fact that $x \in E(n)$ thus there exist an ℓ that satisfies $x^{\ell+1} \equiv x \pmod{n}$. We will show that x^ℓ is an identity element. For $i = 1$ multiplying x^ℓ gives $x^{\ell+1} = x$ thus we know that for any element in $< x >$, multiplying x^ℓ bring the element back to itself thus x^ℓ is the identity element. With this, let us assume x^i for some positive integer i, if i is greater than 1 multiplying x^ℓ we have $x^{\ell+i} \equiv x^{i-1}x^{\ell+1} \equiv x^{i-1}x \equiv x^i$. Lastly, for x^i where $i \in \mathbb{Z}^+$, we can find a positive integer j that satisfies $i + j = k\ell$ for some positive integer k. Then $x^{i+j} = x^i x^j = x^{k\ell} = x^\ell$. Thus x^j is the inverse of x^i and thus $< x >$ is closed under inverses. It follows that $< x >$ is a group if $x \in E(n)$.

Going the other way, proving that if $< x >$ is group under multiplication then $x \in E(n)$, we start by noting that every group has an identity element. It follows that the identity element of $< x >$ is x^ℓ for some $\ell \in \mathbb{Z}^+$. The identity element maps every element to itself thus $x \times x^\ell = x^{\ell+1} = x \pmod{n}$. We can conclude that $x \in E(n)$ thus $x \in E(n)$ if and only if $< x > \pmod{n}$ make a group under multiplication. □

Theorems 21 and 22 can be used to generalize the characteristics of solutions to the equation $x^{\ell+1} \equiv x \pmod{n}$ when ℓ varies. Before we move on to do so, it is important to recognize that we are not assuming these groups to be subgroups of $\mathbb{U}_n$. In fact, most of these groups are not subgroups of $\mathbb{U}_n$. With that in mind, let us generalize our results. Theorem 21 tells us that $m \in E(n)$ is equivalent to saying that the greatest common divisor of m and n is an unitary divisor of n. Theorem 22 tells us that it is also equivalent to saying that $< m >$ is a cyclic group under multiplication.

It can be concluded that all three statements are equal as is summarized by the following theorem.

Theorem 23. *Let $n \in \mathbb{N}$ and $m \in \mathbb{Z}_n$ then the following are equivalent:*
1) $m \in E(n)$.
2) If $(m, n) = g$, then $g||n$.
3) $< m >$ is a cyclic group under multiplication.

7 Analysis of $C(n, q)$

In previous sections, we studied characteristics of elements of $E(n, \ell)$. We first fixed $\ell = 1$ and examined idempotents. Then, by letting ℓ to be any positive integer, we analyzed $E(n)$ and $\sigma(n)$. Now, we will move on to analyze cyclic groups of a given order in $\mathbb{Z}_n$.

Definition 12. *Let $C(n, q)$ be the number of subsets S of $\mathbb{Z}_n$ that are groups of order q under the operation of multiplication.*

The remainder of this paper will be mainly concerned with cases in which q is either an odd prime or an odd prime to some power. Before we move on to analyze $C(n, q)$ in detail, let us go through theorems that will serve as fundamentals.

Theorem 24. *(Lagrange's Theorem) The order of any subgroup divides the order of the group.* [2]

From Lagrange's Theorem follows one important corollary.

Corollary 25. *Any group of order q when q is an odd prime is a cyclic group.*[3]

Theorem 26. *(Primitive Root Theorem) $\mathbb{U}_n$ is cyclic if and only if n is 1,2,4,p^k, or $2p^k$, where p is an odd prime and $k \geq 1$*

Proof. The proof of this will be done through cases. The trivial cases, 1,2 and 4 can be easily shown and will thus be omitted in the proof.

First, we prove that $\mathbb{U}_{2^k}$ when $k > 2$ is not cyclic. From the Fundamental theorem of cyclic groups, for $\mathbb{U}_{2^k}$ to be cyclic, it must have only one subgroup of order 2. This means that there is only one element other than the identity element in $\mathbb{U}_{2^k}$ that is its own inverse. However, both $2^k - 1$

[2]Refer to page 129 of "A Book of Abstract Algebra" by Charles C.Pinter for a proof[1]

and $2^{k-1}-1$ are their own inverses: $(2^k-1)^2 \equiv 2^{2k}-2^{k+1}+1 \equiv 1(\text{mod } 2^k)$ and $(2^{k-1}-1)^2 \equiv 2^{2k-2}-2^k+1 \equiv 1(\text{mod } 2^k)$, observe that there are two distinct elements greater than 1 since $k>2$ that are its own inverses. Thus $\mathbb{U}_{2^k}$ cannot be cyclic.

Secondly, we prove that $\mathbb{U}_{p^k}$ is cyclic where p is an odd prime. Induction will be used to prove this. When $k=1$, let us proceed by proof by contradiction, assume $\mathbb{U}_p$ is not cyclic and that an element of the maximum order is m and has order $n<p-1$. The order of every element divides the order of m and $m^n \equiv 1 \pmod p$[4]. Let us assume a polynominal $f(x)=x^n-1$ over the field $\mathbb{Z}_n$ we know this polynominal has maximum of n roots. We know that since order of every element divides n , every element of $\mathbb{U}_n$ is a root of the polynominal and thus there are $p-1$ roots. This contradicts the statement that $n<p-1$ thus $\mathbb{U}_p$ is cyclic.

In the case $k=2$, we know $\mathbb{U}_p$ is cyclic, thus there exists an element a that satisfies $<a>=\mathbb{U}_p$. Now, look at a and $a+p$. Let ℓ and ℓ_1 be the order for $<a>$ and $<a+p>$ in $\mathbb{U}_{p^2}$ respectively. It follows that $a^\ell \equiv (a+p)^{\ell_1} \equiv 1 \pmod{p^2}$ and is also 1 (mod p). Then writing out $(a+p)^{\ell_1}=a^{\ell_1}+\binom{\ell_1}{1}a^{\ell_1-1}p+\binom{\ell_1}{2}a^{\ell_1-2}p^2+...+p^{\ell_1}$ shows us that $a^{\ell_1} \equiv 1 \pmod p$ since $\binom{\ell_1}{1}a^{\ell_1-1}p+\binom{\ell_1}{2}a^{\ell_1-2}p^2+...+p^{\ell_1}$ is a multiple of p. The order of a in $\mathbb{U}_p$ is $p-1$ thus $p-1$ divides ℓ and ℓ_1. Also from Lagrange's theorem, order of each element divides the order of the group thus ℓ and ℓ_1 divide $\phi(p^2)=p^2-p$. Now by proving that it is impossible for both ℓ and ℓ_1 to be $p-1$, it can be shown that at least one has to be p^2-p. Let us assume both are $p-1$, then $(a+p)^{p-1}=a^{p-1}+\binom{p-1}{1}a^{p-2}p+\binom{p-2}{2}a^{p-3}p^2+...+p^{p-1} \equiv 1 \pmod{p^2}$. We know that $\binom{p-2}{2}a^{p-3}p^2+\binom{p-3}{3}a^{p-4}p^3+...+p^{p-1}$ is a multiple of p^2 thus $(a+p)^{p-1} \equiv 1+\binom{p-1}{1}a^{p-2}p \equiv 1+(p-1)pa^{p-2} \equiv 1-pa^{p-2}$. Since$(a+p)^{p-1} \equiv 1$, $pa^{p-2} \equiv 0 \pmod{p^2}$ but since $a^{p-2} \in \mathbb{U}_{p^2}$, (a^{p-2},p)=1 showing that it is contradictory and thus at least one of ℓ and ℓ_1 has to be $p^2-p=\phi(p^2)$

Now, using induction, assume that $\mathbb{U}_{p^k}$ is cyclic up to $k=m$. It follows from the inductive step that proving $\mathbb{U}_{p^k}$ is cyclic for $k=m+1$ will lead us to prove that $\mathbb{U}_n$ is cyclic for $n=p^k$ every $k \in \mathbb{Z}^+$. Let us say $\mathbb{U}_{p^m}$ is generated by some element g. Let the order of g in $\mathbb{U}_{p^{m+1}}$ be h. It follows that $h|\phi(p^{m+1})=p^{m+1}-p^m$. Since g generates $\mathbb{U}_{p^m}$, $\phi(p^m)=p^m-p^{m-1}|h$. We can conclude that either $h=p^{m+1}-p^m=p^m(p-1)$ or $p^m-p^{m-1}=$

[4]Refer to page 129 of "A Book of Abstract Algebra" by Charles C.Pinter for a proof[1]

$p^{m-1}(p-1)$. Let us assume $h = p^{m-1}(p-1)$. Observe that g also generates $\mathbb{U}_{p^{m-1}}$, and the order of g in this case would be $p^{m-2}(p-1)$. Since $p^{m-2}(p-1) < p^{m-1}(p-1)$ and the generator raised to any power less than the order or the cyclic group cannot be the identity element, we have that $g^{p^{m-2}(p-1)} \neq 1 \pmod{p^m}$ and $g^{p^{m-2}(p-1)} = 1 + up^{m-1}$ for some u. Observe that u has to be relatively prime to p as if u is not relatively prime to p then $u|p$ and thus $g^{p^{m-2}(p-1)} \equiv 1 \pmod{p^k}$. Now, let us raise both sides of the equation by p.

$$\begin{aligned}(g^{p^{m-2}(p-1)})^p &= (1 + up^{m-1})^p \pmod{p^m} \\ &= 1 + \tbinom{p}{1}up^{m-1} + \tbinom{p}{2}(up^{m-1})^2 + \cdots + \tbinom{p}{p}(up^{m-1})^p\end{aligned}$$

dividing both sides of the equation by p^{m+1} will let us look at both equations $\pmod{p^{m+1}}$. Note that every term other than the first and the second term is a multiple of p^{m+1} since $j(m-1)+1 \geq m+1$ for $j = \{2, 3, 4, \cdots\}$. Thus, we are left with the following equation.

$$\begin{aligned}(g^{p^{m-2}(p-1)})^p &\equiv 1 + pup^{m-1} \pmod{p^{m+1}} \\ &\equiv 1 + up^m \pmod{p^{m+1}}.\end{aligned}$$

This is a contradiction as it would give us $g^{p^{m-2}(p-1)} \equiv 1 \pmod{p^m}$. It can be concluded that $h = p^m(p-1)$. It follows that g is a generator for $\mathbb{U}_{p^{m+1}}$ making it cyclic. Thus, $\mathbb{U}_p^k$ is cylic for an odd prime p and all positive integers k.

Now, to complete the proof, it needs to be shown that $\mathbb{U}_{2p^k}$ for an odd prime p and any positive integer k is cyclic and that $\mathbb{U}_{pq}$ for two distinct odd primes p and q is not cyclic. However, these facts will not be used in this paper thus will not be proved.[5] □

For example, $\mathbb{U}_{81}$ is a cyclic group as $81 = 3^4$. Let us first look at $\mathbb{U}_3 = \{1, 2\}$. This is a cyclic group as $< 2 >= \{2, 2^2 = 1\}$. Now let us look at 2 and 2+3=5 in $\mathbb{U}_{3^2} = \mathbb{U}_9 = \{1, 2, 4, 5, 7, 8\}$. We know at least one of 2 or 5 has to generate $\mathbb{U}_9$. Observe that $< 5 >= \{5, 7, 8, 4, 2, 1\}$ and $< 2 >= \{2, 4, 8, 7, 5, 1\}$ thus both of them generate $\mathbb{U}_9$. In fact both 2 and 5 are both primitive roots of $3^3 = 27$ thus $< 2 >=< 5 >= \mathbb{U}_{27}$. Notice that in the inductive step we have proved that if x is a primitive root of p^k than it is also a primitive root of p^{k+1}. This example follows directly from the proof. Now, with this in mind, let us move on to how many generators there are for each subgroup of a cyclic group with order n.

Lemma 27. *If n has a primitive root, for each divisor d of $\phi(n)$ there are*

[5] Reader who are interested in the complete proof, refer to "Multiplicative Groups in $\mathbf{Z_m}$ by Brian Sloan [3]

exactly $\phi(d)$ generators of a group of order d.

Proof. Let us consider a $\mathbb{U}_n$ which is a group under multiplication. There are $\phi(n)$ elements in $\mathbb{U}_n$ and we know that the order of every subgroup divides the group thus for any subgroup S, $|S|$ divides $\phi(n)$. We also know that for every divisor, d, of $\phi(n)$ there is exactly one subgroup of that order and that subgroup of order d is isomorphic to $\mathbb{Z}_d$ under addition. In $\mathbb{Z}_d$ there are $\phi(d)$ elements that can be generators of the group. Observe that there exists an isomorphism between $\mathbb{Z}_d$ and unique subgroup of $\mathbb{U}_n$ of order d. Thus, we can conclude that a subgroup of $\mathbb{U}_n$ of order d will have $\phi(d)$ generators for the group. □

With these Theorems and Lemmas, we can show exactly how many subsets of $\mathbb{Z}_n$ are cyclic groups of order q for any odd prime q.

Theorem 28. *Let $C(n,q)$ for an odd prime q and positive integer n be the number of subsets S in $\mathbb{Z}_n$ that are groups of order q under the operation of multiplication. Then, let us suppose $n = p_1^{e_1}p_2^{e_2}..p_j^{e_j}p_{j+1}^{e_{j+1}}....p_k^{e_k}$ where ps are the primes and the es are positive integers and q is an odd prime. suppose for $i = 1, 2, ..., j$, $q|\phi(p_i^{e_i})$ and for $i = j+1, j+2, ..., k$, $q \nmid \phi(p_i^{e_i})$. Let $\ell = k-j$.*

$$C(n,q) = \frac{2^\ell((q+1)^j - 2^j)}{q-1}$$

Proof. First from the Chinese Remainder Theorem we know $\mathbb{Z}_n$ is isomorphic to the cartesian products of $\mathbb{Z}_{p_i^{e_i}}$ for all $1 \leq i \leq k$. With this knowledge, let us look at $\mathbb{Z}_{p^e}$. From Corollary 25, a group of order q has to be cyclic thus it must have a generator. Let us name the non-zero generator a. Recall from the previous section that if a is a multiple of p, it cannot be in $E(p^e)$ and that $< a >$ cannot form a group. Thus, it follows that a cannot be a multiple of p and we can conclude that $(a, p^e) = 1$. Now we have narrowed our search to look at a in $\mathbb{U}_{p^e}$.

Notice that $\mathbb{U}_{p^e}$ is a group under multiplication so we can look for subgroups of order q. Theorem 24 tells us that the order of $< a >$ has to divide the order of $\mathbb{U}_{p^e}$, i.e. $q|\phi(p^e)$, for a subgroup of order q to exist. From this, it follows that q has to be odd. Further, observe the following two facts:
1) $< a >$ is a subgroup of order q iff $a^{q+1} \equiv a \pmod{p^e}$.
2) from Lemma 27 there are exactly $\phi(q)$ elements that have order q.
When q is a prime, then $\phi(q) = q - 1$. Thus, it follows as a consequence of 2) that for every $\mathbb{Z}_{p_i^{e_i}}$ where $i = 1, 2, ..., j$, there are $q - 1$ generators for a

group of order q. We can finally conclude that
$C(n,q) = \frac{\textbf{(number of } a\textbf{s such that } a^{q+1} \equiv a\textbf{) - (number of } a\textbf{s such that } a^2 \equiv a\textbf{)}}{q-1}$.

In counting the number of as such that $a^{q+1} \equiv a$, first, observe that $< 0 >$ and $< 1 >$ create groups of order 1 and that lcm(1,q)=q. Consequently, the generator being 0 or 1 (mod $p_i^{e_i}$) will not affect the order of the group and the order will be q. This gives $q+1$ possibilities for every $p_i^{e_i}$, giving us $(q+1)^j$ options for a. However, if the generator is 0 or 1 for every $p_i^{e_i}$ then the group will be of order 1. Thus, we have to rule this possibility out by subtracting 2^j from $(q+1)^j$, arriving at $(q+1)^j - 2^j$. Notice that since the same logic is valid for $p_i^{e_i}$ where $q \nmid \phi(p_i^{e_i})$, we can get the exact number of as by multiplying 2^ℓ, giving us $2^\ell((q+1)^j - 2^j)$ possible as. Finally, as mentioned in the above paragraph, there are $q-1$ elements that generate the same group. Thus, we conclude that the number of cyclic groups of order q is $\frac{2^\ell((q+1)^j - 2^j)}{q-1}$. □

This is a very powerful result as it lets us to calculate how many subgroups of order q there are for any given n. For example, let $n = 7 * 11^3 * 29^2 * 31^5 * 43^5$ and $q = 7$. Note that this n is a very large number, slightly bigger than 3×10^{23}. To apply this number to Theorem 28, we know that $k = 5$ as there are 5 distinct primes in the prime decomposition of n. Also, $7 \mid \phi(29^2), \phi(43^5)$ and $7 \nmid \phi(7), \phi(11^3), \phi(31^5)$. It follows that $j = 2$ and $\ell = 3$. Thus $C(n,7) = \frac{2^3(8^2-2^2)}{6} = 80$. There are exactly 80 subsets of $\mathbb{Z}_n$ that are groups of order 7.

Note that the proof specifically mentions that q has to be an odd prime. Further research can be done in case when $q = 2$ but it will not be covered in this paper. Now, let us generalize this theorem into $C(n, q^f)$ for an odd prime q and a positive integer f. First, let us start with a lemma.

Lemma 29. *For any odd prime p*

$$|\{x : x \in \mathbb{U}_{p^e}, x^k = 1\}| = (\phi(p^e), k)$$

Proof. Let us start by assuming that $(\phi(p^e), k) = g$. We know there exists an isomorphism between $\mathbb{Z}_{\phi(p^e)}$ and $\mathbb{U}_{p^e}$. From the isomorphism, it follows that $|\{x : x \in \mathbb{U}_{p^e}, x^k = 1\}| = |\{x : x \in \mathbb{Z}_{\phi(p^e)}, xk = 0\}|$. Also observe that $(\phi(p^e), k) = g$ iff $(\frac{\phi(p^e)}{g}, \frac{k}{g}) = 1$. Then it follows that $kx = 0 \Leftrightarrow \phi(p^e) | kx \Leftrightarrow \frac{\phi(p^e)}{g} | \frac{kx}{g} \Leftrightarrow \frac{\phi(p^e)}{g} | x$. this shows that x has to be a multiple of $\frac{\phi(p^e)}{g}$ to satisfy $|\{x : x \in \mathbb{Z}_\phi(p^e), xk = 0\}|$. Since there are g multiples of $\frac{\phi(p^e)}{g}$ in $\mathbb{Z}_\phi(p^e)$ it follows that $g = |\{x : x \in \mathbb{Z}_\phi(p^e), xk = 0\}| = |\{x : x \in \mathbb{U}_{p^e}, x^k = 1\}|$. □

Theorem 30. *If q is an odd prime, p a prime and $e, f \in \mathbb{N}$ then*

$$\sigma(p^e, q^f) = gcd(p^e - p^{e-1}, q^f) + 1$$

Proof. Let us suppose $x \in E(p^e, q^j)$, then we consider two cases. First, if $p|x$ then $x = 0$ since in Theorem 20 we have proved that no non-zero multiple of p can be in $E(p^e)$. Secondly, if $p \nmid x$ then $(p^e, x) = 1$ thus $x \in \mathbb{U}_{p^e}$. If $x \in \mathbb{U}_{p^e}$ then we know that $x^{qf} + 1 \equiv x \Leftrightarrow x^{pf} = 1$ since every element in $\mathbb{U}_{p^e}$ has an inverse. Then again, we consider two cases

Case 1. when p=2. $|\mathbb{U}_{p^e}| = 2^{e-1}$. Observe that q is an odd prime and thus $2^{e-1} \nmid q^f$ thus the only possible x is $x = 1$. Thus $\sigma(p^e, q^f) = (2^{e-1}, q^f) + 1 = 2$

Case 2. when p is an odd prime $|\mathbb{U}_{p^e}| = \phi(p^e) = p^e - p^{e-1}$. We know that $\mathbb{U}_{p^e}$ is cyclic. From the lemma, we know that $\sigma(p^e, q^f) = (p^e - p^{e-1}, q^f) + 1$ suffices. □

Theorem 31. *Let $n = p_1^{e_1}....p_j^{e_k}$ then*

$$C(n, q^f) = \frac{\prod_{i=1}^{k}[(p_i^{e_i} - p_i^{e_i-1}, q^f) + 1] - \prod_{i=1}^{k}[(p_i^{e_i} - p_i^{e_i-1}, q^{f-1}) + 1]}{q^f - q^{f-1}}$$

Proof. The set of all elements that generate a cyclic group of order q^f is $E(n, q^f) - E(n, q^{f-1})$ the elements that generate a group of order q^ℓ for any integer $1 \leq \ell \leq f$ given by $E(n, q^f)$ minus the elements that generate a group of order q^i for any integer $1 \leq i \leq f - 1$. It follows that the number of the generators is given by $\sigma(n, q^f) - \sigma(n, q^{f-1})$. The number of groups of order q^f will be given by dividing $\sigma(n, q^f) - \sigma(n, q^{f-1})$ by $\phi(q^f)$ as for every group of order q^f there are $\phi(q^f)$ generator for each group. From this we come to the final equation by using the multiplicativity of σ and the above equation. □

Observe that Theorem 28 is a specific case of Theorem 31 in which $f = 1$. Let $f = 1$, we have $C(n, q^f) = C(n, q) = \frac{\sigma(n,q)-\sigma(n,1)}{q-1}$. $\sigma(n, 1)$ is the number of idempotents in n and from Theorem 6, we know that to be 2^k. Furthermore, with regards to $\sigma(n, q) = \prod_{i=1}^{k}[(p_i^{e_i} - p_i^{e_i-1}, q) + 1]$ note that $(p_i^{e_i} - p_i^{e_i-1}, q)$ is 1 if $q \nmid \phi(p_i^{e_i})$ and q if $q \mid \phi(p_i^{e_i})$, arriving at Theorem 28.

8 Conclusion

This concludes our investigation of the solutions to the equation $x^{\ell+1} \equiv x \pmod{n}$. Before summerizing the results of this paper, the importance of the Chinese Remainder theorem in our investigation should be noted. The Chinese Remainder Theorem lets us examine roots modular one prime at a time and then generalize our results mod n. Our investigation showed that all the idempotents can be found for any given n and that every Boolean ring is isomorphic to chain of $\mathbb{Z}_2$s. We have also studied the characteristics of solutions to $x^{\ell+1} \equiv x \pmod{n}$ for any positive integer ℓ and concluded that three statements, $m \in E(n)$, $(m, n)||n$ and $< m >$ is a cyclic group under multiplication, are equivalent. Moreover, analyzing subsets of $\mathbb{Z}_n$ that are groups, we concluded that the exact number of subsets that are groups under multiplication and have order q^f for an odd prime q and a positive integer f can be found for any given $n \in \mathbb{Z}^+$.

References

[1] Charles C.Pinter *A Book of Abstract Algebra: Second Edition.* Dover Publications, Inc., Mineola, New York, 2010.

[2] David Guichard, Patrick Keef, Russ Gordon *An Introduction to Higher Mathematics.* Whitman College, 2010.

[3] Brian Sloan *Multiplicative Groups in* $\mathbf{Z}_m$. Whitman College, 2010.