MULTIPLICATIVE GROUPS IN $\mathbb{Z}_m$

BRIAN SLOAN

1. Abstract

Our goal will be to find subsets of $\mathbb{Z}_m$ that form groups under the operation of multiplication modulo m. By utilizing the isomorphism $\mathbb{Z}_m \cong \mathbb{Z}_n \oplus \mathbb{Z}_k$, we will find multiplicative groups contained in $\mathbb{Z}_n \oplus \mathbb{Z}_k$ and then map these back to $\mathbb{Z}_m$. In particular, if $m = nk$ with $\gcd(n, k) = 1$, our objective is to find particular multiplicative subsets of $\mathbb{Z}_n \times \mathbb{Z}_k$ that are groups and whose first coordinate is a projection onto $U(n)$. We will give a method to calculate the total number of these subsets, and identify the elements of which they are composed.

2. Preliminaries - Notation and the Chinese Remainder Theorem

We will be examining subsets of $\{0, 1, 2, ...m - 1\}$, $m \in \mathbb{Z}^+$, that when paired with the operation of multiplication modulo m, are closed, have a multiplicative identity element, and have a multiplicative inverse for each element. Thus we will be examining groups that consist of a binary operation of multiplication modulo m on finite sets of positive integers.

Definition 2.1 (Binary Operation)**.** *Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.*

Definition 2.2 (Group)**.** *Let G be a nonempty set together with a binary operation that assigns to each ordered pair (a,b) of elements of G an element in G denoted by ab. We say G is a group under this operation if the following three properties are satisfied.*

1. ***Associativity.*** *The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G*
2. ***Identity.*** *There is an element e (called the identity) in G, such that $ae = ea = a$ for all a in G.*
3. ***Inverses.*** *For each element a in G, there is an element b in G (called an inverse of a) such that $ab = ba = e$.*

The topics dealt with will all be familiar to anyone that has taken a first course in Abstract Algebra. The notation will be the same as that which is used in Gallian's *Contemporary Abstract Algebra*[1]. We will expect the reader to have familiarity with common group theoretic topics, including cyclic groups, finite Abelian groups, rings, and fields. However, those theorems and concepts which are integral to the development of splittings will be restated and recalled as necessary.

Because the group operation will always be either addition or multiplication modulo n, the groups we examine will also all be *Abelian*. That is, for all $a, b \in G$, $ab = ba$. Also, many of the groups we will examine will be *cyclic*, meaning that

multiples of some element will generate the entire group. When a cyclic group A is generated by an element a we write $\langle a \rangle = A$.

Generalized Chinese Remainder Theorem for Groups

When dealing with an integer, it is often helpful to know its prime factorization. Breaking something into its smaller component parts allows further insight into how each part functions and contributes to the behavior of the whole. When working with finite Abelian groups, an analogous process allows us to decompose complex groups into simpler parts. We accomplish this decomposition with the help of the First Isomorphism Theorem, found in [1].

Theorem 2.1 (First Isomorphism Theorem)**.** *Let Φ be a group homomorphism from G_1 to G_2. Then the mapping from $G/Ker\Phi$ to $\Phi(G)$, given by $gKer\Phi \to \Phi(g)$, is an isomorphism. In symbols, $G/Ker\Phi \cong \Phi(G)$.*

Now we are ready to show how $\mathbb{Z}_m$ can be equivalently expressed in terms of its simpler parts.

Theorem 2.2 (Generalized Chinese Remainder Theorem for Groups)**.** *Suppose some positive integer $m = nk$ where $gcd(n, k) = 1$. Then*

$$\mathbb{Z}_m \cong \mathbb{Z}_n \oplus \mathbb{Z}_k$$

Proof. Let $m = nk$ where $(n, k) = 1$. Consider the homomorphism $\phi|\mathbb{Z} \to \mathbb{Z}_n \oplus \mathbb{Z}_k$ given by $\phi(x) = ([x]_n, [x]_k)$ [where $[x]_n$ denotes the remainder of x upon division by n]. The kernel of this homomorphism will be the set of all elements $x \in \mathbb{Z}$ such that $\phi(x) = ([0]_n, [0]_k)$. Then in order to be in the kernel, it must be divisible by both n and k. As n and k are relatively prime, $\text{lcm}(n, k) = nk$. The least common multiple of two numbers has the property that any common multiple of two numbers is also divisible by their lcm. Then the set $\langle nk \rangle =$ Ker ϕ. We know from the First Isomorphism Theorem that, $\mathbb{Z}/\langle nk \rangle \cong \phi(\mathbb{Z})$.

The group $\mathbb{Z}/\langle nk \rangle$ is also isomorphic to $\mathbb{Z}_{nk}$ (Also a consequence of the First Isomorphism Theorem considering the mapping $\Phi|\mathbb{Z} \to \mathbb{Z}_{nk}$ given by $\Phi(x) = [x]_{nk}$). Therefore $\mathbb{Z}_{nk} \cong \mathbb{Z}/\langle nk \rangle \cong \phi(\mathbb{Z})$ where $\phi(\mathbb{Z}) \subseteq \mathbb{Z}_n \oplus \mathbb{Z}_k$. As $\mathbb{Z}_n \oplus \mathbb{Z}_k$ has only nk elements, and it is isomorphic to $\mathbb{Z}_{nk}$ which also has nk elements, $\phi(\mathbb{Z}) = \mathbb{Z}_n \oplus \mathbb{Z}_k$. Hence $\mathbb{Z}_m \cong \mathbb{Z}_n \oplus \mathbb{Z}_k$.

□

3. Introduction

Given a particular $\mathbb{Z}_m$, how can we find subsets of it that will form a group with the operation of multiplication modulo m?. Simply taking the whole set will evidently not work. Suppose we look at the set of integers $S = \{0, 1, 2, 3, ...39\}$ with the operation multiplication modulo 40. This set is not a group, although it satisfies almost all of the necessary criteria. The operation is associative. Clearly, the set is also closed under the operation. Applying the modulo 40 to any integer will yield an integer n, $0 \leq n \leq 40$ contained in the set. Furthermore, the standard multiplicative identity 1 is contained in the set, such that for all a in S, $1a = a1 = a$.

All that remains to be verified are inverses, and this is precisely where it fails to be a group. The element 0 can never have an inverse (i.e. a solution to the equation $x \cdot 0 = 1 \bmod 40$). However, if we discard 0, there are still other elements that fail to have an inverse. If we take the element 20 and multiply it by any other

member of the group, the result modulo 40 will be either 0 or 20, neither of which is the identity.

One method is to take a simply take a subset of S that consists only of *units*, that is, only those elements in S that have an inverse. In this case, the set of units is denoted $U(40)$. U-groups will be important to splittings, and we shall examine them in more detail in the next section.

Other than $U(40)$, will there be any other subsets of S that form a group? At first glance it seems likely that we will at least need the element 1 to act as the identity. This turns out to be false. Consider the subset $\{5, 15, 25, 35\}$. With these elements we form a *Cayley Table*, a table used for displaying every possible multiplication in a group in an analogous manner to a multiplication table.

	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

Notice that the element 25 behaves as the identity element in this set. Also, each row and column contains 25, thus each element has some inverse element. With closure, associativity, an identity element, an inverses, it satisfies the group criteria. Despite the fact that none of the elements of the group are units of $\mathbb{Z}_{40}$, and despite lacking the expected identity 1, the set forms a group with the operation multiplication modulo 40.

These numbers were obviously not chosen at random. If one attempted to form a group by picking and choosing elements randomly S they would quickly see the futility of the endeavor. How can we make sense of this? We will investigate the behavior of this set and apply this knowledge to see how we might construct other similar sets.

4. The group of units $U(n)$ and its structure

We now return to our first example of a set of integers that was closed under the operation of multiplication modulo 40, $\{5, 15, 25, 35\}$. Note that each of these terms is divisible by 5. If we divide each member as well as the modulus by 5, we obtain the set of integers $\{1, 3, 5, 7\}$ under multiplication modulo 8. We form another Cayley table with this set and binary operation and see that, interestingly enough, it also forms a group.

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Those familiar with group theory will immediately recognize this group as the group of units $U(8)$. The group of units $U(n)$ is a common group studied in an introductory abstract algebra class. It is the set of numbers less than n and relatively prime to n under the operation multiplication modulo n.

It is well known and easy to verify that one may choose any $n \in \mathbb{Z}^+$ and $U(n)$ will be a group. It may be helpful to do a few calculations with the following U-groups to see that they satisfy the properties of a group (closure, identity, inverses) $U(5) = \{1, 2, 3, 4\}$, $U(10) = \{1, 3, 7, 9\}$, $U(13) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

An examination of the structure and behavior of $U(n)$ will be necessary for further insight into the original set $\{5, 15, 25, 35\}$ and in order to understand how we might construct other similar sets.

For which n is $U(n)$ cyclic?

Some of the U-groups are cyclic, such as $U(5)$ and $U(10)$. (consider $\langle 2\rangle = U(5)$ and $\langle 3\rangle = U(10)$). In the case of $U(8)$, we find that every element is its own inverse, and no element generates all of $U(8)$. Hence $U(8)$ is not cyclic. For what positive integers n is $U(n)$ cyclic? It is precisely those n which have a *primitive root modulo* n, defined to be the specific integer $g \in U(n)$ that generates $U(n)$. Here is what we will be proving:

Theorem 4.1 (Primitive Root Theorem)**.** *$U(n)$ is cyclic if and only if n is $1, 2, 4, p^k$, or $, 2p^k$, where p is an odd prime and $k \geq 1$.*

Before getting started, we need to recall some concepts from number theory and familiar theorems from group theory that will be necessary for the proof.

How many elements will $U(n)$ have? Given an integer n, the number of elements less than and relatively prime to n is given by $\Phi(n)$, where Φ is the Euler phi-function. Consider the case of $U(p)$ for a prime p. Every integer less than p is relatively prime to p, therefore $U(p)$ will have $p - 1$ elements. Also, note that for $U(p^k)$, $\Phi(p^k) = p^k - p^{k-1}$ (to see this, consider the number of integers that are multiples of p between 1 and p^k).

We now remind the reader of two familiar theorems from group theory.

Theorem 4.2 (Fundamental Theorem of Cyclic Groups)**.** *Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n: and, for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k—namely, $\langle a^{n/k}\rangle$.*

To apply this theorem consider the cyclic group $\mathbb{Z}_6$. The divisors of 6 are $6, 3$, and 2. Hence there will be exactly one subgroup each of orders 6, 3, 2, and 1, generated as follows.

$$\langle 1\rangle = \langle 5\rangle = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6$$
$$\langle 2\rangle = \langle 4\rangle = \{2, 4, 0\}$$
$$\langle 3\rangle = \{3, 0\}$$

Another important theorem allows for the decomposition of any finite Abelian group into simpler parts.

Theorem 4.3 (Fundamental Theorem of Finite Abelian Groups)**.** *Every finite Abelian group is isomorphic to a direct product of cyclic groups of prime-power order. Moreover, the factorization is unique except for rearrangement of the factors.*

Because each $U(n)$ is finite and Abelian, it has the unique representation

$$U(n) \cong \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_2^{a_2}} \oplus ... \oplus \mathbb{Z}_{p_n^{a_n}}$$

for not necessarily distinct primes p_1 to p_n and $a_i \geq 1$. The representation as a direct product of cyclic groups is the *isomorphism class* of $U(n)$. For now we will not examine the method of finding these isomorphism classes. That they exist will be sufficient. Only note that when $U(n)$ is cyclic with order $\Phi(n)$, the isomorphism class of $U(n)$ is $\mathbb{Z}_{\Phi(n)}$. As an example, in the context of the U-groups we have been using, the isomorphism classes of $U(8)$ and $U(5)$ are

$$U(5) \cong \mathbb{Z}_4$$
$$U(8) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Now we can begin to approach the topic of when $U(n)$ will be cyclic. The proof will be broken into several cases, each examining a part of the Primitive Root Theorem. It is easy to write out and verify that for $n = 1, 2, 4$, $U(n)$ is cyclic. We will first show that $U(p)$ is cyclic for any odd prime p. Next we will show that this implies both $U(p^2)$ and $U(p^k)$ are cyclic. Finally, we show that when n is divisible by more than one distinct odd prime, or by 2^k for $k \geq 2$, $U(n)$ is not cyclic.

The first task is to show that $U(n)$ is cyclic for an odd prime p. We begin with a definition and two lemmas.

Definition 4.1. *The least common multiple of a set of positive integers $\{a_1, a_2, ..., a_m\}$, denoted $lcm(a_1, a_2...a_m)$, is the smallest positive integer b such that $a_i|b$ for $1 \leq i \leq m$. It follows*[1] *that if for some positive integer c, $a_i|c$ for $1 \leq i \leq m$, then $b|c$.*

Lemma 4.4. *If $x = lcm(a_1, a_2, ..., a_m)$, $y = lcm(b_1, b_2, ..., b_m)$ with $b_i|a_i$ for $1 \leq i \leq m$ then $y|x$.*

Proof. If $b_i|a_i$ then $b_ic_i = a_i$, so that $x = \text{lcm}(b_1c_1, b_2c_2, ..., b_mc_m)$. By definition each $b_ic_i|x$, and furthermore, $b_i|x$ for $1 \leq i \leq m$. Therefore $y|x$. □

Lemma 4.5. *Let G be a finite Abelian group and m be an element of maximal order contained in G. Then for every element $b \in G$, the order of g divides the order of m.*

Proof. If G is a finite Abelian group, then it is isomorphic to

$$\mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus .... \oplus \mathbb{Z}_{p_k^{n_k}}$$

where the p_i's are not necessarily distinct primes. We know from [1] that an element $g = (g_1, g_2, ..., g_k)$ has order $\text{lcm}(|g_1|, |g_2|, ..., |g_k|)$. An element of maximal order will be generated by a k-tuple of the form $(1, 1, ..., 1,)$. As each entry is a generator for its respective $\mathbb{Z}_{p_i^{n_i}}$, each will have order $p_i^{n_i}$. Thus $|m| = lcm(p_1^{n_1}, p_2^{n_2}, ..., p_k^{n_k})$. Let b be some element in G. It has the form $b = (b_1, b_2, ..., b_k)$ where each b_i is a member of $\mathbb{Z}_{p_i^{n_i}}$. Lagrange's Theorem states that the order of an element of a group divides the order of the group, so for $1 \leq i \leq k$

$$|b_i| \mid |p_i^{n_i}|$$

The order of b is $lcm(|b_1|, |b_2|, ...|b_k|)$ and the order of m is $\text{lcm}(p_1^{n_1}, p_2^{n_2}, ..., p_k^{n_k})$. Then by the previous lemma, the order of b divides the order of m.

□

[1] See definition of $\text{lcm}(a, b)$ given by [2].

We proceed by examining $U(n)$ for particular cases of n.

Case 1: $U(n)$ is cyclic when $n = p$ for a prime p.

The proof will assume that the reader is familiar with the concepts of fields, and polynomials defined over a field.

Proof. The group $U(p)$ has order $p-1$ given by $\Phi(p)$. Each non-identity element of $U(p)$ has some order less than or equal to $p-1$ and greater than 1. Let m be an element of order n with maximal order in $U(p)$. We proceed by contradiction. Assume $U(p)$ is not cyclic. Then n is strictly less than $p-1$. Observe that the elements of $U(p)$ are contained in the field $\mathbb{Z}_{p-1}$. Define a polynomial $P(x) = x^n - 1$ over $\mathbb{Z}_{p-1}$. Then

$$P(m) = m^n - 1 = 1 - 1 = 0$$

and m is a root of $P(x)$. Let g be any other element of $U(p)$. By Lemma 1.3, the order of g divides the order of m. Then for each g, there exists a positive integer a such that $a|g| = n$, so that

$$P(g) = g^n - 1 = (g^{|g|})^a - 1 = 1^a - 1 = 0$$

Therefore all $p-1$ elements of $U(p)$ are roots of $P(x)$, but $P(x)$ is a polynomial of degree n and can thus have at most n roots. This contradicts the hypothesis $n < p-1$, therefore $n = p-1$ and $U(p)$ is cyclic.

□

Case 2: $U(n)$ is cyclic when $n = p^2$ for a prime p

Proof. As $U(p)$ is cyclic, there exists $g \in U(p)$ such that $\langle g \rangle = U(p)$. We will show that $U(p^2)$ is cyclic by showing that either the element g or $g+p$ has an order of (p^2-p). Let h_t be the order of $g+tp$ where t is equal to 0 or 1. Then by definition, $(g+tp)^{h_t} \equiv 1 \mod p^2$ and $(g+tp)^{h_t} \equiv 1 \mod p$. So,

$$\begin{aligned} 1 &\equiv (g+tp)^{h_t} (\mathrm{mod} p), \\ &\equiv g^{h_t} + \binom{h_t}{1} g^{h_t - 1}(tp) + \binom{h_t}{2} g^{h_t - 2}(tp)^2 + ... + (tp)^{h_t} (\mathrm{mod} p), \\ &\equiv g^{h_t}, \end{aligned}$$

and $g^{h_t} = 1$. For any element a of a group G, with identity e, if $a^k = e$ then $|a| \big| k$. Because g is a generating element of $U(p)$ it has order $(p-1)$, so $(p-1)|h_t$. Recall the corollary to Lagrange's theorem that states that the order of each element of a group divides the order of the group. Therefore h_t divides $p^2 - p$, the order of $U(p^2)$, or equivalently, $h_t | p(p-1)$. Thus there exists positive integers a and b such that $(p-1)a = h_t$ and $bh_t = p(p-1)$. Combining the equations yields $ab(p-1) = p(p-1)$, or $ab = p$. Therefore either $a = 1$ or $b = 1$. We conclude that either $h_t = p-1$ or $h_t = p(p-1)$.

By way of contradiction, assume that $h_t = p-1$ for both $t = 1$ and $t = 0$ for the element $g + tp$. Then $g^{p-1} \equiv 1 \mod p^2$ and $(g+p)^{p-1} \equiv 1 \mod p^2$, and

$$\begin{aligned} 1 &\equiv (g+p)^{p-1} (\mathrm{mod} p^2) \\ &\equiv g^{p-1} + \binom{p-1}{1} g^{p-2}(p) + \binom{p-1}{2} g^{p-3}(p)^2 + ... + (p)^{p-1} (\mathrm{mod} p^2) \\ &\equiv 1 + \binom{p-1}{1} g^{p-2}(p) + 0 + 0 ... (\mathrm{mod} p^2) \\ &\equiv 1 + (p-1) g^{p-2} p (\mathrm{mod} p^2) \\ &\equiv 1 - g^{p-2} p (\mathrm{mod} p^2) \end{aligned}$$

Therefore $p^2 | (1 - (1 - g^{p-2}p)$, that is, $p^2 | pg^{p-2}$. But the element g^{p-2} is an element of $U(p^2)$, and $\gcd(g^{p-2}, p) = 1$, so it is not possible for p^2 to divide pg^{p-2} because it has at most one factor of p in its prime factorization. Therefore the original assumption is false, and one of the elements g or $g+p$ has order $p^2 - p$. Thus $U(p^2)$ is cyclic.

□

Case 3: $U(n)$ is cyclic when $n = p^k$ for an odd prime p.

Proof. Proceeding by induction we begin with the hypothesis that $U(p^k)$ is cyclic and generated by some element g. Also by hypothesis, each $U(p^i)$ for $i = 2$ to $i = k-1$ is also cyclic, and generated by the same element g. Let h be the order of the element g in $U(p^{k+1})$, then $h | p^k(p-1)$. Observe that $g^h \equiv 1 \mod p^{k+1} \equiv 1 \mod p^k$. Therefore, $p^{k-1}(p-1) | h$, so either $h = p^k(p-1)$ or $h = p^{k-1}(p-1)$. This fact will be useful shortly.

Suppose that $h = p^{k-1}(p-1)$. In $U(p^k)$, the element g has order $p^{k-1}(p-1)$, and in $U(p^{k-1})$, the element g has order $p^{k-2}(p-1)$. Thus

$$g^{p^{k-2}(p-1)} \neq 1 (\mathrm{mod} p^k)$$

This is valid because when g is raised to any power less than its order in $U(p^k)$, it will not be congruent to 1 mod p^k. Therefore $g^{p^{k-2}(p-1)} = 1 + up^{k-1}$ for some integer u. Note that p does not divide u, for if it did, $g^{p^{k-2}(p-1)} \cong 1 (\mod p^k)$. Then

$$\begin{aligned} \left(g^{p^{k-2}(p-1)}\right)^p &= (1 + up^{k-1})^p \\ &= 1 + \binom{p}{1} up^{k-1} + \binom{p}{2} (up^{k-1})^2 + \binom{p}{2} (up^{k-1})^2 + ... + (up^{k-1})^p (\mathrm{mod} p^{k+1}) \\ &\equiv 1 + pup^{k-1} (\mathrm{mod} p^{k+1}) \\ &= 1 + up^k (\mathrm{mod} p^{k+1}) \end{aligned}$$

So we have $(g^{p^{k-2}(p-1)})^p = 1 + up^k$, which is equivalent to $g^{p^{k-1}(p-1)} = 1 + up^k$ where p does not divide u. Then $g^{p^{k-1}(p-1)} \neq 1 (\mathrm{mod} p^{k+1})$ so h,the order of g, is not $p^{k-1}(p-1)$ and therefore it must be the other option, $h = p^k(p-1)$, and $\langle g \rangle = U(p^{k+1})$. Hence $U(p^{k+1})$ is cyclic.

□

Case 4: $U(n)$ is not cyclic when n is a product of distinct odd primes.

So far we have concluded that $U(n)$ is cyclic for n equal to $1, 2, 4$, p^2, and q^k for odd primes q. We consider the case when n is a product of more than one odd prime. An isomorphism exists to decompose U-groups in much the same way we decompose $\mathbb{Z}_n$. Given two relatively prime positive integers s and t, we may write

$$U(st) \cong U(s) \oplus U(t)$$

An isomorphism Φ from $U(st)$ to $U(s) \oplus U(t)$ is given by $\Phi(x) = (x \bmod s, x \bmod t)$. That this mapping is operation preserving, one to one, and onto is not hard to verify. Given any n, it is also not hard to see that using this method $U(n)$ can be expressed as a direct product of U-groups of prime power order. A theorem from [1] then tells us exactly when this direct product will be cyclic.

Theorem 4.6 (Criterion for $G_1 \oplus G_2 \oplus ... \oplus G_n$ to Be Cyclic)**.** *An external direct product $G_1 \oplus G_2 \oplus ... \oplus G_n$ of a finite number of finite cyclic groups is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime when $i \neq j$*

From this, the fact that $U(n)$ is not cyclic for n that are products of distinct odd primes.

Proof. Suppose that the prime factorization of n is $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where each p_i is distinct and $k \geq 2$. Then $U(n)$ may be written as an external direct product in terms of its relatively prime parts.

$$U(\Pi_{i=1}^{k} p_i^{a_i}) \cong U(p_1^{a_1}) \oplus ... \oplus U(p_k^{a_k})$$

The order of $U(p_k^{a_k})$ is $\Phi(p_k^{a_k}) = p_k^{a_k} - p_k^{a_k - 1}$ which is always an even number (note that both terms will always be odd). Then each member of the external direct product has even order, and their orders are not pairwise relatively prime, implying $U(n)$ is not cyclic.

□

Case 5: $U(n)$ is not cyclic for $n = 2^k$, $k > 2$

Proof. Consider $U(n)$ for $n = 2^k$, $k > 2$. For any cyclic group, there will be exactly one subgroup of order d for each divisor of the order of the group. Thus it is sufficient to show that $U(2^k)$ will have two distinct subgroups of order 2 to show it is not cyclic. $U(2^k)$ will contain every odd positive integer less than or equal to 2^k, thus both $2^k - 1$ and $2^{k-1} - 1$ are contained in $U(2^k)$. Observe that

$$(2^k - 1)^2 = 2^{k+1} - 2^k + 1 = 1 (\mathrm{mod} 2^k)$$
$$(2^{k-1} - 1)^2 = 2^{2k-2} - 2^k + 1 = 1 (\mathrm{mod} 2^k)$$

Then both elements generate a different subgroup of order 2, and it follows that $U(2^k)$ is not cyclic.

□

All that remains is the case when $n = 2p^k$ for $k \geq 1$. We may rewrite $U(2p^k)$ as $U(2p^k) \cong U(2) \times U(p^k)$. Because $U(2) = \{1\}$ it is trivially true that $U(2) \times U(p^k) \cong U(p^k)$. Hence

$$U(2p^k) \cong U(2) \times U(p^k) \cong U(p^k)$$

Since they are isomorphic and $U(p^k)$ is cyclic, $U(2p^k)$ is also cyclic. This completes the proof of the Primitive Root Theorem.

One last piece of information will be necessary regarding the structure of $U(n)$. So far, we have a method of breaking $U(n)$ down into simpler parts by first separating n into its prime factorization, and then recognizing that each of those odd prime power parts is isomorphic to a cyclic group. If n's prime factorization contains more than one factor of 2, then there will be some $U(2^k)$ in the initial separation of $U(n)$

$$U(\Pi_{i=1}^{k} p_i^{a_i}) \cong U(2^k) \oplus U(p_1^{a_1}) \oplus ... \oplus U(p_k^{a_k}).$$

In order to completely decompose $U(n)$ into a direct product of cyclic groups, the isomorphism class of $U(2^n)$ will be necessary.

Lemma 4.7. *If $n \geq 2$, $5^{2^{n-2}} = 1 + u_n 2^n$, where u_n is odd.*

Proof. We proceed by induction. For $n = 2$ observe that

$$5^{2^{2-2}} = 5 = 1 + (1)(2^2).$$

Assume that for $n = k$, $5^{2^{k-2}} = 1 + u_k(2^k)$ where u_k is odd. Then for $n = k + 1$

$$\begin{aligned} 5^{2^{(k+1)-2}} &= 5^{2^{(k-1)}} \\ &= 5^{2^{(k-2)}} 5^{2^{(k-2)}} \\ &= (1 + u_k(2^k))(1 + u_k(2^k)) \\ &= 1 + 2u_k 2^k + u_k^2 2^{2k} \\ &= 1 + u_k 2^{k+1} + u_k^2 2^{2k} \\ &= 1 + 2^{k+1}(u_k + u_k^2 2^{k-1}) \end{aligned}$$

Since $(u_k + u_k^2 2^{k-1})$ will always be odd, we may write $5^{2^{(k+1)-2}} = 1 + u_{k+1} 2^{k+1}$ for some odd number u_{k+1}. This completes the proof.

□

With this lemma, we may proceed to find the isomorphism class of $U(n)$ when n contains a factor of 4 or some higher power of 2.

Theorem 4.8. *For $n \geq 2$, $U(2^n)$ is isomorphic to $\mathbb{Z}_{2^{n-2}} \oplus \mathbb{Z}_2$*

Proof. We know by from Euler Phi function that $U(2^n)$ has order $2^n - 2^{n-1} = 2^{n-1}$. By the Fundamental Theorem of Finite Abelian Groups, $U(2^n)$ will be isomorphic to some direct product of cyclic groups. Because the order of $U(2^n)$ is 2^{n-1}, each cyclic group in the direct product must be some power of 2 less than or equal to $n - 1$. Also, since it is not cyclic, it cannot be isomorphic to $\mathbb{Z}_{2^{n-1}}$.

Note that if an element with order 2^k exists in $U(2^n)$, then at least one member of the direct product of cyclic groups will also have an order of at least 2^k. We will show that $U(n)$ contains an element of order 2^{n-2}, implying $\mathbb{Z}_{2^{n-2}}$ is a member of the external direct product of cyclic groups to which $U(2^n)$ is isomorphic. If $\mathbb{Z}_{2^{n-2}}$ is a member of this direct product, the remainder of the product must be a cyclic group of order 2 such that

$$U(2^n) \cong \mathbb{Z}_{2^{n-2}} \oplus \mathbb{Z}_2$$

as this gives $U(2^n)$ its appropriate order 2^{n-1}.

From the previous lemma, we know that 5 has an order that divides 2^{n-2}. In order to show that 2^{n-2} is the order of 5 we also have to show that it is the smallest

number m such that $5^m = 1 \bmod 2^n$. As 5 must have an order that is a power of 2 it is sufficient to show that

$$5^{2^{n-3}} \neq 1 \bmod 2^n.$$

From the previous lemma, $5^{2^{n-3}} = 1 + u2^{n-1}$ for some positive odd integer u. By way of contradiction, we suppose that $5^{2^{n-3}} = 1 + q2^n$ for a positive integer q. Thus

$$1 + u2^{n-1} = 1 + q2^n, \text{ and}$$
$$u2^{n-1} = q2^n.$$

As u is odd, the previous statement must be false. Thus the order of the element 5 in $U(2^n)$ is 2^{n-2}. This completes the proof.

□

5. $kU(n)$ and Splittings of $\mathbb{Z}_m$

As we saw earlier, we were able to take $U(8)$, multiply each element as well as the multiplication modulus by 5, and the resulting set formed a group. We denote this group $5U(8)$. Alternatively, consider the set $8U(5) = \{8, 16, 24, 32\}$ with operation multiplication modulo 40. Constructing a Cayley Table demonstrates this is also a group.

	8	16	24	32
8	24	8	32	16
16	8	16	24	32
24	32	24	16	8
32	16	32	8	24

Table 1. $8U(5)$

Also consider $3U(8) = \{3, 9, 15, 21\}$. The operation will be multiplication modulo 24. We again construct a Cayley Table and verify that it is also a group (Refer to Table 2).

	3	9	15	21
3	9	3	21	15
9	3	9	15	21
15	21	15	9	3
21	15	21	3	9

Table 2. $3U(8)$

Will it be the case that $kU(n)$ is a group for any positive integer k? Examining $2U(8) = \{2, 6, 10, 14\}$ quickly reveals that it is not the case. We need only consider the multiplication $(2)(6) = 12$ to see that the group is not closed under multiplication modulo 16.

It may be shown that $kU(n)$ is only a group when $\gcd(n, k) = 1$. To see why this is the case, we return to the first example. Recall that if $\gcd(n, k) = 1$, $\mathbb{Z}_{nk} \cong \mathbb{Z}_n \oplus \mathbb{Z}_k$. Thus we may write $\mathbb{Z}_{40} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_5$. As $kU(8)$ is a subset of the

ring $\mathbb{Z}_{nk}$, we may find the isomorphic subset of $\mathbb{Z}_8 \oplus \mathbb{Z}_5$ given by the isomorphism $\phi(x) = (x \mod 8, x \mod 5)$. For example, $\phi(5) = (5 \mod 8, 15 \mod 5) = (5, 0)$. Continuing with the other elements, $\phi(15) = (7, 0)$, $\phi(25) = (1, 0)$, $\phi(35) = (3, 0)$. Thus $kU(8) \cong \{(1, 0), (3, 0), (5, 0), (7, 0)\}$.

When presented in this manner, it is easy to see why $5U(8)$ is a group. When the ordered pairs are multiplied together component-wise, with their respective operations multiplication modulo 8 and multiplication modulo 5, $5U(8)$ behaves exactly the same as $U(8)$ and is in fact isomorphic to $U(8)$, as the 0 in the second position has no effect on the multiplication.

This presents us with a method for finding other splittings of Z_{40}. If we can construct subsets of $\mathbb{Z}_8 \oplus \mathbb{Z}_5$ that are groups, they will necessarily be groups when we map the elements back to $\mathbb{Z}_{40}$. Using this strategy, we create another similar subset, but replace 1 with 0 in the second component.

$$\{(1, 1), (3, 1), (5, 1), (7, 1)\}$$

Clearly this also will be isomorphic to $U(8)$. If we map these elements back into Z_{40}, we find that this subgroup corresponds to the set $\{1, 11, 21, 31\}$.

We now turn our attention to just those subsets of Z_{kn} that when mapped to $\mathbb{Z}_k \oplus \mathbb{Z}_n$ contain all of $U(n)$ in the first component. We define this precisely as follows:

Definition 5.1. *Let $k, n \in \mathbb{N}$ with $gcd(k, n) = 1$. A subset $G \subseteq \mathbb{Z}_n \oplus \mathbb{Z}_k$ is said to be splitting if it is a group under multiplication (mod n, mod k) and if $\pi : \mathbb{Z}_n \oplus \mathbb{Z}_k \to \mathbb{Z}_n$ given by $\pi(x, y) = x$ restricts to a group isomorphism from G to $U(n)$.*

Thus any splitting of $\mathbb{Z}_8 \oplus \mathbb{Z}_5$ will have the form $\{(1, a), (3, b), (5, c), (7, d)\}$ for $a, b, c, d \in \mathbb{Z}_5$.

If we preserve the first coordinate, such that the some member of the set contains each member of $U(8)$, the set will necessarily be isomorphic to $U(8)$, as the operation is multiplication modulo 8 in that coordinate. There are obviously conditions under which a, b, c, and d may be chosen to ensure it is a splitting. For example, the set $\{(1, 1), (3, 1), (5, 1), (7, 2)\}$ is not a splitting, as the product $((3, 1))((7, 2)) = (5, 2)$ is not contained in the set. We will show what conditions on the second coordinate entries ensure that we generate a splitting.

6. Commutative Monoid Homomorphisms and Splittings

Our objective now is to identify all splittings for any given $\mathbb{Z}_n \oplus \mathbb{Z}_k$. Generally, a splitting of $\mathbb{Z}_n \oplus \mathbb{Z}_k$ will have the form

$$\{(a_1, b_1), (a_2, b_2), ..., (a_k, b_k)\}$$

where $a_1, ..., a_k$ is an exhaustive list of the elements of $U(n)$, and $b_1, ..., b_k$ are elements of Z_k that are not necessarily distinct (note that they were all 0's or 1's in the previous examples).

Given a splitting, consider the function $f : U(n) \to \mathbb{Z}_k$ defined by by $f(a_j) = b_j$. Thus the function assigns to each member of $U(n)$ the corresponding element in $\mathbb{Z}_k$ as designated by the splitting. Applying this to the first example, $\{5, 15, 25, 35\}$,

that corresponds to the splitting $\{(5,0),(7,0),(1,0),(3,0)\}$, the function $f : U(8) \to \mathbb{Z}_k$ is defined by

$$f(1) = 0,\ f(3) = 0,\ f(5) = 0,\ f(7) = 0.$$

A function $f : A \to B$ is said to be operation preserving if $f(a)f(b) = f(ab)$ for all a in A and b in B. We will show that any $f : U(n) \to \mathbb{Z}_k$ that is defined by a splitting is operation preserving, and conversely, given any operation preserving function $f : U(n) \to \mathbb{Z}_k$ the ordered pairs that define the function correspond to a splitting of $\mathbb{Z}_n \oplus \mathbb{Z}_k$.

Let $S(n,k)$ be the total number of splittings of $\mathbb{Z}_n \oplus \mathbb{Z}_k$ and let $\mathrm{Hom}(U(n), \mathbb{Z}_k)$ denote the set of operation preserving functions $f : U(n) \to \mathbb{Z}_k$ (More generally $Hom(A,B)$ is the set of operation preserving functions between two sets of elements, A and B, on which a binary operation is defined).

Theorem 6.1. $S(n,k) = |Hom(U(n), \mathbb{Z}_k)|$

Proof. We will first show that any operation preserving function corresponds to a splitting, and then that any splitting corresponds to an operation preserving function.

Suppose $f : U(n) \to \mathbb{Z}_k$ is operation preserving. Then the set of ordered pairs $H = \{(z, f(z)) : z \in U(n)\}$ is a subset of $\mathbb{Z}_n \oplus \mathbb{Z}_k$. Let $x, y \in U(n)$. Thus $(x, f(x)), (y, f(y))$ are elements of H and

$$\begin{aligned}(x, f(x))(y, f(y)) &= (xy, f(x)f(y)) \\ &= (xy, f(xy)) \in H.\end{aligned}$$

Hence H is closed under multiplication. We now need to show that H has an identity and inverses. For $x \in U(n)$, the identity and inverse in H are analogous to their $U(n)$ counterparts. For $(x, f(x)) \in H$

$$(1, f(1))(x, f(x)) = (x, f(x)f(1)) = (x, f(x))$$
$$(x^{-1}, f(x^{-1}))(x, f(x)) = (1, f(1)) = e$$

Clearly the function $\pi : H \to U(n)$ given by $\pi(x, y) = x$ is a group isomorphism. Thus H is a splitting.

Now consider some splitting $H \subseteq \mathbb{Z}_n \oplus \mathbb{Z}_k$, and let $f : U(n) \to \mathbb{Z}_k$ be the function defined by the set of all ordered pairs of G (formed in the same manner as the first example at the beginning of section 6). Then f maps all of $U(n)$ to a subset of $\mathbb{Z}_k$. Let $(x, f(x)), (y, f(y)) \in G$. Because G is a group and closed,

$$(x, f(x))(y, f(y)) = (xy, f(x)f(y)) \in H$$

By the definition of the function, the elements $(xy, f(x)f(y))$ and $(xy, f(xy))$ are in fact the same element. Hence $f(x)f(y) = f(xy)$. Therefore any splitting G corresponds to an operation preserving function $f : U(n) \to \mathbb{Z}_k$.

So each splitting G of $\mathbb{Z}_n \oplus \mathbb{Z}_k$ corresponds to some operation preserving function $f : U(n) \to \mathbb{Z}_k$ and each operation preserving f corresponds to some splitting G. Therefore an exhaustive list of the operation preserving functions f will also yield a list of all the splittings of $\mathbb{Z}_n \oplus \mathbb{Z}_k$, and $|S(n,k)| = |\mathrm{Hom}(U(n), \mathbb{Z}_k)|$.

□

In order to find operation preserving functions it will be necessary to characterize them. Because the set of elements $Z_k = \{0, 1, 2, ..., k-1\}$ under multiplication modulo k is not always a group, the operation preserving functions are not group homomorphisms. Although $\mathbb{Z}_k$ is not a group, it satisfies several of the required conditions. Namely the set is closed, it contains an identity element, and it is associative. Furthermore, the operation is commutative. Therefore both it and $U(n)$ satisfy the definition of a *commutative monoid*.

Definition 6.1 (Commutative Monoid (CM))**.** *A commutative monoid is a set that is closed under an associative and commutative operation and has an identity element.*

With this in mind, we will call an operation preserving function between two commutative monoids a *CM-homomorphism* and given two CM's A and B, the set of all CM-homomorphisms from A to B is the set $\mathrm{Hom}(A, B)$. The problem now is to find the size of $\mathrm{Hom}(U(n), \mathbb{Z}_k)$, which will correspond to the number of splittings.

Before attempting to count the number of elements in $\mathrm{Hom}(U(n), \mathbb{Z}_k)$ (and thus, the number of splittings), we will simplify the task by showing that one need only consider n and k that are primes or powers of primes. Our goal in the following section will be to show that if n or k is a not a prime or a power of a prime, $\mathrm{Hom}(U(n), \mathbb{Z}_k)$ may be broken into smaller parts utilizing the isomorphisms $U(n) \cong U(s) \oplus U(t)$ and $\mathbb{Z}_k \cong \mathbb{Z}_\ell \oplus \mathbb{Z}_j$.

Commutative Monoid Homomorphisms

Given CM's A and B where $A \cong A_1 \oplus A_2 \oplus ... \oplus A_m$ and $B \cong B_1 \oplus B_2 \oplus .... \oplus B_n$, our objective is to show that

$$|\mathrm{Hom}(A, B)| = \Pi_{i=1}^{n} \Pi_{j=1}^{m} |\mathrm{Hom}(A_j, B_i)|$$

by which we reduce the problem of finding the number of elements in $\mathrm{Hom}(U(n), \mathbb{Z}_k)$ to finding the number of elements for only prime power n and k.

Given CM's $A_1, A_2, ..., A_n$ it is clear that the Cartesian product

$$A_1 \oplus A_2 \oplus ... \oplus A_n$$

will also be a CM, if the operation is defined component-wise. If 1_{A_k} is the identity element of A_k then the identity element of the Cartesian product is $(1_{A_1}, 1_{A_2}, ..., 1_{A_n})$ and it is not hard to show it will be closed, commutative, and associative.

Now suppose that the sets A, B_1, and B_2 are CM's and there exist functions $f : A \to B_1$ and $g : A \to B_2$ that are CM-homomorphisms. Define a function $h : A \to B_1 \oplus B_2$ by

$$h(a) = (f(a), g(a))$$

Then for every $a_1, a_2 \in A$,

$$h(a_1)h(a_2) = (f(a_1), g(a_1))(f(a_2), g(a_2)) = (f(a_1a_2), g(a_1a_2)) = h(a_1a_2)$$

Thus h is operation preserving, and is a CM-homomorphism from A to $B_1 \oplus B_2$

Conversely, if $h : A \to B_1 \oplus B_2$ is a CM-homomorphism where $h(a) = (f(a), g(a))$ then for all $a_1, a_2 \in A$

$$(f(a_1), g(a_1))(f(a_2), g(a_2)) = h(a_1)h(a_2) = h(a_1a_2) = (f(a_1a_2), g(a_1a_2))$$

So f and g are operation preserving, and thus are CM-homomorphisms.

Consider the sets $\mathrm{Hom}(A, B_1 \oplus B_2)$ and $\mathrm{Hom}(A, B_1) \times \mathrm{Hom}(A, B_2)$. Define Φ: $\mathrm{Hom}(A, B_1 \oplus B_2) \to \mathrm{Hom}(A, B_1) \times \mathrm{Hom}(A, B_2)$ such that $\Phi(h) = (f, g)$ where h, f and g are the functions defined above such that $h(a) = (f(a), g(a))$. This is valid, as (f, g) was shown to be a member of $\mathrm{Hom}(A, B_1) \times \mathrm{Hom}(A, B_2)$. By the same reasoning, Φ will be invertible such that $\Phi^{-1}((f, g)) = h$. Therefore there is a one to one correspondence between $\mathrm{Hom}(A, B_1 \oplus B_2)$ and $\mathrm{Hom}(A, B_1) \times \mathrm{Hom}(A, B_2)$. This may be extended to any number of B_k. If $A, B_1, B_2, ..., B_n$ are commutative monoids, then

$$\begin{aligned} \mathrm{Hom}(A, B_1 \oplus B_2 \oplus ... \oplus B_n) &= \mathrm{Hom}(A, B_1 \oplus ... \oplus B_{n-1}) \times \mathrm{Hom}(A, B_n) \\ &\vdots \\ &= \mathrm{Hom}(A, B_1) \times \mathrm{Hom}(A, B_2) \times ... \times \mathrm{Hom}(A, B_n) \end{aligned}$$

We then note that if $A \times B$ is a Cartesian product of two sets, $|A \times B| = |A| \cdot |B|$. Then $|\mathrm{Hom}(A, B_1 \oplus B_2 \oplus \cdots \oplus B_n)| = |\mathrm{Hom}(A, B_1)| \cdot |\mathrm{Hom}(A, B_2)| \cdots |\mathrm{Hom}(A, B_n)|$

We have shown that for a CM-homomorphism $f : A \to B$ where $B \cong B_1 \oplus B_2$, the elements of the sets $\mathrm{Hom}(A, B_1 \oplus B_2)$ or $\mathrm{Hom}(A, B_1) \times \mathrm{Hom}(A, B_2)$ are essentially equivalent. An analogous result holds when $A \cong A_1 \oplus A_2$.

Suppose that the sets A_1, A_2 and B are CM's and $f : A_1 \to B$ and $g : A_2 \to B$ are CM-homomorphisms. We define $h : A_1 \oplus A_2 \to B$ by $h((a_1, a_2)) = f(a_1)g(a_2)$. For elements $a_1, a_3 \in A_1$, and $a_2, a_4 \in A_2$

$$h((a_1, a_2)(a_3, a_4)) = h((a_1a_3, a_2a_4)) = f(a_1a_3)g(a_2a_4) = f(a_1)f(a_3)g(a_2)g(a_4)$$
$$= f(a_1)g(a_2)f(a_3)g(a_4) = h((a_1, a_2))h((a_3, a_4))$$

Therefore h is a CM-homomorphism. Note that in this case it was necessary that the elements of B commute to show the function is operation preserving.

Conversely, suppose A_1, A_2, and B are CM's, and $h : A_1 \oplus A_2 \to B$ is a CM-homomorphism and define $f : A_1 \to B$ and $g : A_2 \to B$ by $f(a_1) = h((a_1, 1_{A_2}))$, $g(a_2) = h((1_{A_1}, a_2))$. Where 1_{A_k} is the identity element of A_k. Then

$$f(a_1a_2) = h((a_1a_2, 1_{A_2})) = h((a_1, 1_{A_2})(a_2, 1_{A_2})) =$$
$$h((a_1, 1_{A_2}))h((a_2, 1_{A_2})) = f(a_1)f(a_2).$$

Hence f is a CM-homomorphism, as well as g (to show g is operation preserving is exactly the same).

Consider the sets $\mathrm{Hom}(A_1 \oplus A_2, B)$ and $\mathrm{Hom}(A_1, B) \times \mathrm{Hom}(A_2, B)$. For the same reasons Φ: $\mathrm{Hom}(A, B_1 \oplus B_2) \to \mathrm{Hom}(A, B_1) \times \mathrm{Hom}(A, B_2)$ was a one to one correspondence, $\Pi : \mathrm{Hom}(A_1 \oplus A_2, B) \to \mathrm{Hom}(A_1, B) \times \mathrm{Hom}(A_2, B)$ will be a one to one correspondence, so that there are the same number of elements in each set.

Now returning to the topic of counting splittings. We know that the total number of splittings equals the total number of operation preserving functions from $U(n)$ to $\mathbb{Z}_k$ so that $S(n, k) = |\mathrm{Hom}(U(n), \mathbb{Z}_k)|$. By extending the above results, to $U(n)$ and $\mathbb{Z}_k$ we obtain an important theorem.

Theorem 6.2. *Suppose n and k have prime factorizations $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $k = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$. Then $S(n, k) = \Pi_{i=1}^{r} \Pi_{j=1}^{s} [S(p_i^{a_i}, q_j^{b_j})]$*

Proof. The sets $U(n)$ and $\mathbb{Z}_k$ both satisfy the requirements of a CM, so the results regarding CM-homomorphisms hold for them. Suppose that k is not a power of a prime, such that $k = j\ell$ where $(j, \ell) = 1$. Then we know that $\mathbb{Z}_k$ is isomorphic to $\mathbb{Z}_j \oplus \mathbb{Z}_\ell$, so $\mathrm{Hom}(U(n), \mathbb{Z}_k) \cong \mathrm{Hom}(U(n), \mathbb{Z}_j \oplus \mathbb{Z}_\ell)$, and

$$S(n,k) = |\mathrm{Hom}(U(n), \mathbb{Z}_k)| = |\mathrm{Hom}(U(n), \mathbb{Z}_j \oplus \mathbb{Z}_\ell)| =$$

$$|\mathrm{Hom}(U(n), \mathbb{Z}_j)||\mathrm{Hom}(U(n), \mathbb{Z}_\ell)| = S(n,j)S(n,\ell).$$

And if either j or ℓ are not a power of a prime, they may be broken down into relatively prime parts by the same process, and so on until each is a power of a prime (and may be decomposed no further). As a result, it is only necessary to consider k that are powers of primes.

Suppose alternatively that $n = m\ell$ where $m(, \ell) = 1$. Then

$$U(n) \cong U(m) \oplus U(\ell)$$

and

$$S(n,k) = |\mathrm{Hom}(U(n), Z_k)| = |\mathrm{Hom}(U(m) \oplus U(\ell), Z_k)| =$$

$$|\mathrm{Hom}(U(m), Z_k)| \cdot |\mathrm{Hom}(U(\ell), Z_k)| = S(m,k)S(\ell,k).$$

Again, if m and ℓ are not powers of primes, they may be decomposed further to powers of primes, so that we need only consider $S(n,k)$ for which n is a power of a prime.

□

Example: Symbolically find the number of splittings of Z_{630} with $n = 10, k = 63$.

$$\begin{aligned} S(10,63) &= |\mathrm{Hom}(U(10), Z_{63})|, \\ &= |\mathrm{Hom}(U(10), Z_9)| \cdot |\mathrm{Hom}(U(10), Z_7)|, \\ &= |\mathrm{Hom}(U(5), Z_9)| \cdot |\mathrm{Hom}(U(2), Z_9)| \cdot |\mathrm{Hom}(U(5), Z_7)| \cdot |\mathrm{Hom}(U(2), Z_7)|, \\ &= S(5,9) \cdot S(2,9) \cdot S(5,7) \cdot S(2,7). \end{aligned}$$

Our task is reduced to finding the number of elements in the set $\mathrm{Hom}(U(p^i), Z_{q^j})$ for primes p and q and positive integers i and k. This task may be simplified further by making some simple observations about properties of CM-homomorphisms. We illustrate this with a theorem preceded by a lemma.

Lemma 6.3. *Suppose q is a prime and j is a positive integer. If $x^2 \equiv x \bmod q^j$, then $x \equiv 1 \bmod q^j$ or $x \equiv 0 \bmod q^j$.*

Proof. If $x^2 \equiv x \bmod q^j$ then $q^j | x(x-1)$. Because q is prime, and x and $(x-1)$ are relatively prime, either $q^j | x$ or $q^j | (x-1)$. If $q^j | x$ then $x \equiv 0 \bmod q^j$ and if $q^j | (x-1)$ then $x \equiv 1 \bmod q^j$ □

Theorem 6.4. *If A is an Abelian group then $Hom(A, Z_{q^j})$ consists of the function which maps all of A to 0 and the set $Hom(A, U(q^j))$, the set of group homomorphisms from A to $U(q^j)$.*

Proof. Suppose A is an Abelian group (then it is also a CM), q is a prime, and j is a positive integer. If $f : A \to Z_{q^j}$ is a CM-homomorphism, then

$$f(1_A) = f(1_A^2) = f(1_A)^2$$

and by the previous lemma either $f(1_A) = 0$ or 1.

Let a be an element of A, and suppose $f(1_A) = 0$. Then $f(a) = f(a)f(1_A) = f(a)(0) = 0$. As a is an arbitrary element of A, $f(a) = 0$ for all $a \in A$.

Now suppose $f(1_A) = 1$ and let a be an element of A. We denote the inverse of a in A by a^{-1}. Then

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) \equiv 1 \bmod q^j.$$

We know that the equation $ax \equiv 1 \bmod n$ has a solution x for integers a and n if and only if $\gcd(a, n) = 1$. Therefore $\gcd(f(a), q^j) = 1$ and by the definition of U-groups $f(a)$ is an element of $U(q^j)$ for all $a \in A$.

□

This theorem tells us that the set of CM-homomorphisms $\mathrm{Hom}(U(p^i), \mathbb{Z}_{q^j})$ consists of the homomorphism that takes every element of $U(p^i)$ to 0, and the set of group homomorphisms from $U(p^i)$ to $U(q^j)$. As we know so much about the structure of $U(n)$, this task of identifying and counting these homomorphisms will be simplified greatly. Suppose that $q = 2$ and $j > 1$. Then $U(q^j) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{q^{j-2}}$ and we we may write

$$|\mathrm{Hom}(U(p^i), U(q^j))| = |\mathrm{Hom}(U(p^i), \mathbb{Z}_2 \oplus \mathbb{Z}_{q^{j-2}})| = |\mathrm{Hom}(U(p^i), \mathbb{Z}_2)| \cdot |\mathrm{Hom}(U(p^i), \mathbb{Z}_{q^{j-2}})|$$

If neither p nor q are equal to 2, both $U(p^i)$ and $U(q^j)$ are cyclic. Thus all that remains is to count the total number of group homomorphisms between two cyclic groups and add 1 (for the homomorphism that sends every element to 0) to find the total number of splittings, $S(p^i, q^j)$.

7. Counting Group Homomorphisms Between Cyclic Groups

Suppose we are given two cyclic groups A and B such that $A = \langle a \rangle$. We need to find all group homomorphisms between A and B. Recall that a group homomorphism is any mapping $f : A \to B$ that preserves the group operations of A and B. Because A and B are cyclic, there are a very limited number of homomorphisms, as the entire mapping is defined by where the generating element, a, is sent. Consider the mapping given by $f(a) = x$ (where a generates A). Because every element of A may be expressed as a^i for some positive integer i, we know where every other element of A is mapped as well, by noticing that

$$f(a^i) = \underbrace{f(a)f(a)\cdots f(a)}_{i} = f(a)^i = x^i.$$

With this in mind, we proceed with a lemma and then a theorem.

Lemma 7.1. *Suppose A and B are cyclic groups where $A = \langle a \rangle$, and $|A| = m$. Let x be an element of B with order k. Then a mapping $f : A \to B$ given by $f(a^i) = x^i$ is a homomorphism if and only if $k|m$.*

Proof. First suppose that f is a homomorphism. Recall that if $a^k = e$ then the order of a divides k. With this in mind, observe that

$$x^m = f(a^m) = f(e_A) = e_B$$

where e_A and e_B are the identities of their respective groups. Hence $k|m$.

Now suppose that $k|m$. It is easy to see that the mapping is operation preserving. For any elements a^i and a^j in A,

$$f(a^i)f(a^j) = x^i x^j = x^{i+j} = f(a^{i+j}) = f(a^i a^j)$$

It is also important that we ensure the mapping is well-defined. If $a^i = a^j$ but $i \neq j$, we must be certain that $f(a^i) = f(a^j)$. For a finite group G, $a^i = a^j$ if and only if the order of a divides $i - j$. Then $m|(i - j)$, and since $k|m$, we also have that $k|(i - j)$. Hence $x^i = x^j$, and $f(a^i) = f(a^j)$.

□

Therefore, in order to find a homomorphism, we must find $x \in B$ such that the order of x divides the order of A, and then the appropriate homomorphism will be given by $f(a^i) = x^i$. The lemma tells us that finding every x in B that satisfies this criteria will also yield an exhaustive list of the homomorphisms between A and B. We now examine how many, and precisely which x satisfy this condition.

Lemma 7.2. *If A and B are cyclic groups with orders m and n, respectively, then there are $gcd(m, n)$ elements of B that have orders that divide m.*

Proof. We will prove that every member of a particular subgroup of B has an order that divides m, and furthermore, that any element with order that divides m is also a member of the same subgroup, thus showing that the members of the subgroup are precisely the members of B that have orders that divide m. We will denote $\gcd(m, n)$ as (m, n).

Let b be a generating element of B and consider the subgroup $S = \langle b^{n/(m,n)} \rangle$. Let $j = n/(m, n)$Thus

$$S = \{b^j, b^{2j}, b^{3j}, ..., b^{(m,n)j}\}.$$

Hence S has order (m, n), and by Lagrange's Theorem, every element of S has an order that divides (m, n), and thus also divides m.

Now consider some element $x \in B$ with order dividing m. Then the subgroup $\langle x \rangle$ has an order that divides m. A property of the greatest common divisor of two numbers is that every common divisor divides the greatest common divisor. Hence $|x|\big|(m, n)$. The Fundamental Theorem of Cyclic Groups tells us that for each positive divisor k of m, there is a unique subgroup of order m . Because $|x|$ is a divisor of (m, n), there is a subgroup of S with order $|x|$. As this is the unique subgroup in B with order $|x|$, $\langle x \rangle \subseteq S$ and $x \in S$.

Therefore the elements of S are precisely those elements which have orders that divide m, and the size of S is (m, n).

□

A method for counting the number of homomorphisms from cyclic groups A to B follows easily from these two lemmas.

Theorem 7.3. *If $A = \langle a \rangle$ and $B = \langle b \rangle$ are cyclic groups with orders m and n respectively, then there are $gcd(m, n)$ homomorphisms from A to B.*

Proof. A list of the homomorphisms, denoted by which element a is mapped to is as follows:

$$\underbrace{f_1(a) = b^j, f_2(a) = b^{2j}, ..., f_{(m,n)}(a) = b^{(m,n)j}}_{(m,n)}$$

□

Corollary 7.4. *For cyclic groups A and B there are the same number of homomorphisms from A to B as there are from B to A, that is, $Hom(A, B) = Hom(B, A)$.*

Proof. From the theorem it easily follows that

$$|\mathrm{Hom}(A, B)| = \gcd(|A|, |B|) = \gcd(|B|, |A|) = |\mathrm{Hom}(B, A)|.$$

□

8. Conclusion

Returning to the topic of splittings, we finally have all the necessary information to determine the number of splittings for a given n and k, $\mathrm{S}(n, k)$. We will conclude by retracing the logic outlined in the paper to see exactly how $\mathrm{S}(n, k)$ is determined for odd n and k, and then provide two examples.

Suppose we are given $n, k \in \mathbb{N}$ such that n and k are relatively prime. The goal is to find all splittings, $\mathrm{S}(n, k)$. Recall that a splitting is a subset of $G \subseteq \mathbb{Z}_n \oplus \mathbb{Z}_k$ that is a group under multiplication ($\bmod n$, $\bmod k$) and also has the property that a function $\pi : G \to U(n)$ restricts to a group isomorphism given by $\pi(x, y) = x$. It was found that splittings could be also identified by finding all of the operation preserving functions from $U(n)$ to $\mathbb{Z}_k$. Next, the development of commutative monoid homomorphisms showed it was only necessary to consider cases where n and k are powers of primes, and furthermore, that the set of operation preserving functions from $U(n)$ to $\mathbb{Z}_k$ consists of the function that sends all of $U(n)$ to 0, and the set of group homomorphisms from $U(n)$ to $U(k)$. As n and k are powers of primes, this is simplified further to finding the number of group homomorphisms between two cyclic groups. We will expand on this with a theorem and some examples.

Theorem 8.1. *Let n and k be odd positive integers with $(n, k) = 1$, and prime factorizations $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $k = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$. Then*

$$S(n, k) = \Pi_{i=1}^{r} \Pi_{j=1}^{s} [1 + gcd(p^{a_i} - p_i^{a_i - 1}, q_j^{b_j} - q_j^{b_j - 1})].$$

Proof. Utilizing Theorem 6.2, we write $\mathrm{S}(n, k) = \Pi_{i=1}^{r} \Pi_{j=1}^{s} [\mathrm{S}(p_i^{a_i}, q_j^{b_j})]$. Then by Theorem 6.4, $\mathrm{S}(p_i^{a_i}, q_j^{b_j}) = [1 + |\mathrm{Hom}\big(U(p_i^{a_i}), U(q_j^{b_j})\big)|]$. Both $U(p^{a_i})$ and $U(q_j^{b_j})$ are cyclic with orders $(p_i^{a_i} - p_i^{a_i - 1})$ and $(q_j^{b_j} - q_j^{b_j - 1})$, respectively. From the previous section we are able to calculate the number of homomorphisms between cyclic groups. Hence

$$|Hom\big(U(p_i^{a_i}), U(q_j^{b_j})\big)| = \gcd(p_i^{a_i} - p_i^{a_i - 1}, q_j^{b_j} - q_j^{b_j - 1})$$

.

This completes the proof.

□

To simplify notation, the case where n or k contains a power of 2 was omitted from the theorem. If one of n or k contains a power of 2 (note that because they are relatively prime, only one or the other can be even), we make a slight modification. Recall that $U(2^m)$ is the only case when $U(p^i)$ is not cyclic, and it is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_{2^{m-2}}$. In the proof of the theorem, if some $p_i = 2$ then the value of $|\mathrm{Hom}\big(U(p^{a_i}), U(q_j^{b_j})\big)|$ would instead be $|\mathrm{Hom}\big(\mathbb{Z}_2 \oplus \mathbb{Z}_{2^{m-2}}, \mathbb{Z}_{(q^{b_j}-q^{b_j-1})}\big)| = \gcd(2, q^{b_j}-q^{b_j-1})\gcd(2^{m-2}, q^{b_j}-q^{b_j-1}) = 2\gcd(2^{m-2}, q^{b_j}-q^{b_j-1})$.

In all of the preceding arguments, n and k are interchangeable [fundamentally because $\gcd(n,k) = \gcd(k,n)$]. Thus we may switch them to obtain the following corollary.

Corollary 8.2. *There are the same number of splittings of $\mathbb{Z}_n \oplus \mathbb{Z}_k$ as of $\mathbb{Z}_k \oplus \mathbb{Z}_n$. That is, $S(n,k)$=$S(k,n)$.*

Example 1 - Finding the total number of splittings of $\mathbb{Z}_{34} \oplus \mathbb{Z}_{15}$, S(34, 15).

We need to find the number of of operation preserving functions from $U(34)$ to $\mathbb{Z}_{15}$, $\mathrm{Hom}(U(34), \mathbb{Z}_{15})$. Decomposing to prime power parts, we may write $U(34) \cong U(17) \oplus U(2)$ and $\mathbb{Z}_{15} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_3$. Hence we need to calculate the product S(17, 5)·S(17, 3·)S(2, 5)·S(2, 3).

$$S(17,5)\cdot S(17,3)\cdot S(2,5)\cdot S(2,3) = [1+\mathrm{Hom}(U(17),U(5))]\cdot[1+\mathrm{Hom}(U(17),U(3))]\cdot$$
$$[1+\mathrm{Hom}(U(2),U(5))]\cdot[1+\mathrm{Hom}(U(2),U(3))]$$

Then as the isomorphism classes of the U-groups are known, the last expression is equal to

$$[1+|\mathrm{Hom}(\mathbb{Z}_{16},\mathbb{Z}_4)|]\cdot[1+|\mathrm{Hom}(\mathbb{Z}_{16},\mathbb{Z}_2)|]\cdot[1+|\mathrm{Hom}(\mathbb{Z}_1,\mathbb{Z}_4)|]\cdot[1+|\mathrm{Hom}(\mathbb{Z}_1,\mathbb{Z}_2)|].$$

Because we know the amount of homomorphisms between cyclic groups, this expression is equal to

$$[1+(16,4)]\cdot[1+(16,2)]\cdot[1+(1,4)]\cdot[1+(1,2)] = (5)(3)(2)(2) = 60$$

Therefore there are a total of 60 splittings.

Recall that the first splitting we examined was $\{(1,0),(3,0),(5,0),(7,0)\}$ where $n = 8$ and $k = 5$. This corresponded to the set $\{5, 15, 25, 35\} \in \mathbb{Z}_{40}$. We saw that there was also the splitting $\{(1,1),(1,3),(1,5),(1,7)\}$ that corresponded to the set $\{1, 11, 21, 31\}$. Using the method we have developed, we can systematically discover if there are more than these two splittings. This will be illustrated in the following example.

Example 2 - Find the splittings of $\mathbb{Z}_8 \oplus \mathbb{Z}_5$ and their corresponding sets in $\mathbb{Z}_{40}$

Splittings will correspond to operation preserving functions $f : U(8) \to \mathbb{Z}_5$. One of these is the function that sends each element of $U(8)$ to 0, $\{(1,0),(3,0),(5,0),(7,0)\}$.

The rest will correspond to group homomorphisms from $U(8) \to U(5)$, or equivalently, the group homomorphisms from $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ to $\mathbb{Z}_4$. In Table 3 we define both the isomorphism from $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ to $U(8)$ and the isomorphism $\mathbb{Z}_4$ to $U(5)$ so that after finding the appropriate homomorphisms, we may translate them back into $\mathbb{Z}_8 \oplus \mathbb{Z}_5$.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$U(8)$	$\mathbb{Z}_4$	$U(5)$
(0,0)	1	0	1
(0,1)	3	1	2
(1,0)	5	2	4
(1,1)	7	3	3

TABLE 3

From the discussion of CM-homomorphisms, we know that in order to find the homomorphisms from $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ to $\mathbb{Z}_4$ we need to find homomorphisms from $\mathbb{Z}_2$ to $\mathbb{Z}_4$. (Recall that for $A_1 \oplus A_2 \to B$, if $f_1 : A_1 \to B$ and $f_2 : A_2 \to B$ are homomorphisms, then $h : A_1 \oplus A_2 \to B$ is a homomorphism defined by $h(a_1, a_2) = f(a_1)f(a_2)$).

To find the homomorphism between two cyclic groups $\mathbb{Z}_2$ and $\mathbb{Z}_4$, we follow the procedure outlined in the previous section. Since 1 is the generating element of both, the possible homomorphisms are defined by $f_1(1) = 1^{4/(2,4)} = 1^2 = 2$ and $f_2(1) = 1^{(2)4/(2,4)} = 1^4 = 0$. Thus there will be a total of four possible homomorphisms h from $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ to $\mathbb{Z}_4$, defined as follows, for $(a_1, a_2) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$:

$$h_1((a_1, a_2)) = f_1(a_1)f_1(a_2);$$
$$h_2((a_1, a_2)) = f_1(a_1)f_2(a_2);$$
$$h_3((a_1, a_2)) = f_2(a_1)f_1(a_2);$$
$$h_4((a_1, a_2)) = f_2(a_1)f_2(a_2).$$

Note that h_4 is the homomorphism that sends all of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ to the identity element (f_2 just sends every element to 0). For the others, we will plug in values to calculate where individual elements are mapped. We will demonstrate the process for finding the mapping h_1:

$$h_1(0, 0) = f_1(0)f_1(0) = 0 + 0 = 0;$$
$$h_1(0, 1) = f_1(0)f_1(1) = 0 + 2 = 2;$$
$$h_1(1, 0) = f_1(1)f_1(0) = 2 + 0 = 2;$$
$$h_1(1, 1) = f_1(1)f_1(1) = 2 + 2 = 0.$$

The others may be found in the same manner. All the homomorphisms are listed in Table 4

	h_1	h_2	h_3	h_4
(0,0)	0	0	0	0
(0,1)	2	0	2	0
(1,0)	2	2	0	0
(1,1)	0	2	2	0

TABLE 4

Now that we have the homomorphisms from $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ to $\mathbb{Z}_4$ we may map them back to $U(8)$ and $U(5)$ using Table 3 to find the splittings. The following splittings are listed as they corresponded to the homomorphisms.

$$h_1 \to \{(1,1),(3,4),(5,4),(7,1)\};$$
$$h_2 \to \{(1,1),(3,1),(5,4),(7,4)\};$$
$$h_3 \to \{(1,1),(3,4),(5,1),(7,4)\};$$
$$h_4 \to \{(1,1),(3,1),(5,1),(7,1)\}.$$

These four plus the original splitting $\{(1,0),(3,0),(5,0),(7,0)\}$ are the five total splittings. Each member of the splittings exist in $\mathbb{Z}_8 \oplus \mathbb{Z}_5$. To finish, we utilize the isomorphism from $\mathbb{Z}_8 \oplus \mathbb{Z}_5$ to $\mathbb{Z}_{40}$ to find the splittings that these correspond to.

$$h_1 \to \{1,19,29,31\};$$
$$h_2 \to \{1,11,29,39\};$$
$$h_3 \to \{1,19,21,39\};$$
$$h_4 \to \{1,11,21,31\}.$$

Using the splitting corresponding to h_3, we demonstrate with a Cayley table that this is in fact a group under the operation multiplication mod40.

	1	19	29	31
1	1	19	29	31
19	19	1	31	29
29	29	31	1	19
31	31	29	19	1

References

(1) Gallian, Joseph A. Contemporary Abstract Algebra: Fourth Edition. Boston, MA: Houghton Mifflin Co., 1998.
(2) "Least Common Multiple." <http://planetmath.org/encyclopedia/LeastCommonMultiple.html >. Planet Math.