CONSTRUCTING MULTIPLICATIVE GROUPS MODULO N WITH IDENTITY DIFFERENT FROM ONE

By: AlaEddin Douba – 35697

Advisor: Dr. Ayman Badawi

MTH 490: Senior Project

INTRODUCTION

The numbering system consists of different sets of numbers that are contained within each other. The most used number sets can be classified as: natural numbers, integers, rationals, irrationals, real numbers, complex numbers and many others that are defined by the cross product between these systems. This paper deals with the second set of numbers, integers. Specifically, it deals with a specific structure in integers called “integers modulo n” denoted by Z_n . The set of numbers in Z_n can be written by the residues of division by n. The following definitions hold for integers modulo n:

$$let\ a, b\ \in Z\ , a \equiv b\ mod\ n\ iff\ n \mid (a - b)$$

$$let\ a, b \in Z\ , a \equiv b\ mod\ n\ is\ equivelant\ to\ a = kn + b\ where\ 0 \leq k < b$$

$$ax \equiv b\ mod\ n\ has\ a\ solution\ iff\ \gcd(a, n) \mid b$$

Arithmetic procedures are carried out in Z_n in a similar manner to Z. Multiplication and addition are denoted by $+_n\ and\ *_n$ to differentiate the domain of these functions. The modular n is applied to the image of these operations as illustrated below. For simplicity, these operation will be referred to by the regular + and * signs since we are only dealing with Z_n.

$$(10 +_n 8) mod\ 12 \equiv 18\ mod\ 12 \equiv 6\ mod\ 12$$

$$note\ that\ 18 = 12(1) + 6\ where\ 6\ is\ the\ residue$$

$$(10 *_n 8)\ mod\ 12\ \equiv 80\ mod\ 12\ \equiv 8\ mod\ 12$$

$$Similarly, 80 = 12(6) + 8$$

In order to demonstrate the results of any linear operations on a set of numbers, Cayley's table can be constructed. This table can help illustrating properties such as identity, closure, inverse, and associativity that will be discussed later on. Cayley's table can be constructed in a similar manner to the following example:

$$for\ the\ set\ H = \{A, B, C, D\}, cayley's\ table\ for\ H\ under\ addition\ is:$$

	A	B	C	D
A	A+A	A+B	A+C	A+D
B	B+A	B+B	B+C	B+D
C	C+A	C+B	C+C	C+D
D	D+A	D+B	D+C	D+D

Group is a term which was firstly used by Galois around 1830 to describe sets of one-to-one functions on finite sets that could be grouped together to form a closed set under composition. The field of groups have grown ever since. Now, a complete definition describing groups is as follows:

$let\ G\ be\ a\ set\ together\ with\ binary\ operation\ \nabla\ that\ assigns\ to\ eacher\ orderd\ pair\ (a, b)\ where\ a, b\ \in G\ an\ element\ a \nabla b\ \in G. G\ is\ a\ said\ to\ be\ a\ group\ under\ this\ operation\ if\ the\ following\ three\ properties\ are\ satisdied$

$let\ a, b\ c\ and\ e\ \in G\ with\ binary\ operation\ \nabla$

1. *Associativity:*

$$(a \nabla b) \nabla c = a \nabla (b \nabla c)$$

2. *Identity:*

$$let\ e\ be\ the\ identity\ of\ G\ then,$$

$$a \nabla e = e \nabla a = a$$

3. *Inverse:*

$$\forall\ a\ \in G\ \exists\ b\ \in G\ where\ a \nabla b = b \nabla a = e$$

The three requirements and closure, which is implied in the definition, are the general requirements for a set to form a group under a binary operation ∇. G is said to be Abelian iff for every $a, b \in G,\ a\nabla b = b\nabla a$. If there exist one pair that doesn't satisfy this property then G is non-Abelian. Groups of integers under multiplication or addition are among the most common examples of Abelian groups.

Sometimes, groups with different elements or binary operations might be the same but have different names. When there's a map that respects the structure the group structure between G and $\overline{G}$ we say they hold they have homomorphism. Note that both sets must have the same size (order). If this mapping holds bijection property, we say G and $\overline{G}$ are isomorphic, denoted as $G \cong \overline{G}$.

Homomorphism:

$A\ homomorphism\ \emptyset\ from\ a\ group\ (G,*)\ to\ a\ group\ (\bar{G},\hat{})\ is\ a\ mapping\ from\ G$

$into\ \bar{G}\ \ that\ preserves\ the\ group\ operation;\ that\ is,$

$$\emptyset(a * b) = \emptyset(a)\hat{}\emptyset(b) forall\ a, b\ \in G$$

Isomorphism:

$$(G, \nabla) is\ said\ to\ be\ isomorphic\ to\ (\overline{G},*) if\ there\ exists\ a\ one - to$$

$$-one\ mapping\ or\ a\ function\ \mathrm{f} from\ G\ onto\ \overline{G}$$

$$that\ preserves\ the\ group\ operation:$$

$$f(a\nabla b) = f(a) * f(b) \quad \forall a, b\ \in G$$

Euler described and defined the set of relatively prime integers $U(x)\ to\ be\ as:$ $U(l) = \{1 \leq a < x | \gcd(a, x) = 1\}$. The order of such set is also defined using Euler's Phi

function (totient function). This function is important for calculating the order of multiplicative groups of integers modulo n. $U(l)$ is useful in determining when a group under both addition and multiplication will form a field.

Fields:

$let\ (H,+,*) be\ a\ set\ with\ two\ binary\ operations; addition\ and\ multiplication$

$H\ is\ said\ to\ be\ a\ field\ if\ the\ following\ requrements\ are\ met:$

a) $(H,+) is\ an\ abelian\ group$

b) $(H^*,*)\ is\ an\ abelian\ group$

c) $\forall\ a,b,c\ \in G\ a*(b+c)=(a*b)+(a*c)$

In this paper, some key theorems have been used in relation to Arithmetic, integers modulo n, groups, isomorphism, Euler Phi function, and many more:

1. Fundamental Theorem of Prime Factorization

   $Every\ integer\ greater\ than\ 1\ either\ is\ prime\ itself\ or\ is\ the\ product\ of\ prime\ numbers, and\ that, although\ the\ order\ of\ the\ primes\ in\ the\ second\ case\ is\ arbitrary, the\ primes\ themselves\ are\ not.$

2. $let\ a>1,\ a\in Z, then\ \gcd(a,a-1)=1$

3. Let G be a group with linear operation * and identity e then, the order of $a \in G$ denoted by |a| is defined as:

   $$|a|=w\ iff\ a^w=e\ for\ w\ the\ smallest\ integer\ , i.e:$$

   $$if\ a^s=e\ then\ w|s$$

4. Euler Phi function:

   Let $U(x)$ be defined as the set of all integers relatively prime to x.

$$U(x) = \{1 \leq a < x | \gcd(a, x) = 1\}$$

$$The\ order\ of\ U(x) = |U(x)| = \emptyset(x)$$

$$for\ x = p_1^{\propto_1}.p_2^{\propto_2}.\ldots\ p_n^{\propto_n}$$

$$\emptyset(x) = p_1^{\propto_1 - 1}(p_1 - 1).p_2^{\propto_2 - 1}(p_2 - 1).\ldots\ p_n^{\propto_n - 1}(p_n - 1)$$

$$or\ \emptyset(x) = x\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_n}\right)$$

5. Well defined function:

$A\ function\ f\ is\ said\ to\ be\ well - defined\ if\ it\ gives\ the\ same\ result\ when$

$the\ form\ but\ not\ the\ value\ of\ an\ input\ is\ changed.$

6. First isomorphism Theorem:

$$let\ f: G \to H\ be\ a\ group\ homomorphism\ from\ G\ into\ H$$

$$G/Ker(f)\ \cong\ Range\ (f) <\ H$$

7. Kernel:

$$let\ f: G \to H\ be\ a\ group\ homomorphism$$

$$The\ kernel\ of\ f\ (\ker(f))is\ defined\ as:$$

$$\ker(f) = \{g \in G : f(g) = e_H\}\ where\ e_H is\ the\ identity\ in\ H$$

8. $(U(x) \cup \{0\}, +, *)\ is\ a\ field\ iff\ x\ is\ a\ prime$
9. $if\ k|n\ and\ l|k\ then\ l|n\ .Also, if\ a|m, b|n\ and \gcd(m, n) = 1$

$$then \gcd(a, b) = 1$$

10. Subgroups:

$$if\ D\ is\ a\ finite\ abelian\ group\ and\ m|\ |D|,\ then$$

$D\ has\ a\ subgroup\ of\ order\ m$

PROBLEM STATEMENT

Theorem 1:

1. Let m $\in Z^+, m \geq 2$. Suppose that D is a group under multiplication with the multiplicative identity m under multiplication modulo n where D $\subset Z_n$. Then,
   a) $m^2 - m \geq n > m$
   b) $n = kl \; for \; k|m \, , l|(m-1)$
   c) If $x \in D$, then x = $m * w \;\; for \;\; some \;\; w < l \; such \; that \gcd(w, l) = 1$ $(i.e.,$ $w \in U(l))$.
   d) $D \; is \; a \; group \; isomorphic \; to \; a \; subgroup \; of \; U(l)$
2. Let $m \in Z^+ , n, k \; and \; l$ be as 1.b then $D = \{kc \mid \gcd(c, l) = 1, 1 \leq c \leq l\}$ is a multiplicative group with multiplicative identity m under multiplication modulo n where D is a subset of Z_n
3. Let $m \in Z^+ , n, k \; and \; l$ be as 1.b. Then, D is a field iff l is prime

Corollary 2: Let D be the group in theorem 1 and let |D| denotes the order (the size) of D. Then |D| | $\emptyset(l) \; where \; n, k \; and \; l \; as \; in \; 1.b$.

Theorem 3: let $m, n \in Z^+ \; such \; that \gcd(m, n) = 1. Then, D = m.U(n) is \; a \; group$ $modulo \; mn \; with \; identity \; e = mc \; for \;\; mc \equiv 1 \; mod \; (n), c \in U(n)$

PROOF

Theorem 1:

1. **Let m $\in Z^+, m \geq 2$. Suppose that D is a group under multiplication with the multiplicative identity m under multiplication modulo n where D $\subset Z_n$. Then,**

   a) $\boldsymbol{n > m}$

$if\ n < m, then\ m \notin Z_n$

$if\ n = m\ then\ m \equiv 0\ mod\ n$

$$a * m \equiv 0\ mod\ n\ \forall\ a \in Z_n$$

$$Then, n > m$$

   b) $\boldsymbol{n = kl\ for\ k|m\ , l|(m-1)}$

$let\ m\ be\ the\ multiplicative\ identity\ for\ a\ set\ D \subset Z_n\ under\ multiplication\ modulo\ n$

$$m * m \equiv m\ mod\ n$$

$$n|\ (m^2 - m) \rightarrow n \mid m * (m-1)$$

$$By\ the\ Fundamental\ Theorem\ of\ Prime\ Factorization,$$

$$write\ n = k * l\ where\ \gcd(k, l) = 1.$$

$$since\ n\ |m * (m-1)\ and\ n = k * l,\ k * l\ |m * (m-1)\ .$$

$Since\ \gcd(k, l) = \gcd(m, m-1) = 1,$

$we\ may\ assume\ that\ k|m, l|(m-1),\ \text{and}\ \gcd(k, m-1) = \gcd(l, m) = 1.$

   c) $\boldsymbol{If\ x\ in\ D, then\ x = m * w\ for\ some\ w < l\ such\ that\ gcd(w, l) = 1}$

$$a * m \equiv a \bmod n \; \forall \; a \in D \rightarrow n \mid ((a * m) - a)$$

$$n \mid a(m-1)$$

$$since \; n = k, l \rightarrow k * l \mid a(m-1)$$

$$Since \;\; l \mid \; (m-1) \; and \; \gcd(k, m-1) = 1, we \; have \; k \mid a.$$

$$Hence \;\; a = k * c \;\; where \;\; c < l \; .$$

Now, we show that $\gcd(c, l) = 1$.

Since k|m and $\gcd(m, l) = 1$, $we \; have \;\; m = \; k * h \; where \;\; h < l \;\; and \;\; gcd(h, l) = 1$.

$Since \; D \; is \; a \; group \; and \; a \; \in D, a \; has \; an \; inverse \; say \; b \; \in D. Thus,$

$a \; * \; b \; = k * c * b \; \equiv \;\; m \; = k * h \; mod(n = kl). \; Hence, \;\; c \; * \; b \; \equiv h \; mod \; (l).$ Since $gcd(h, l) \; = \; 1, \; we \; have \;\; gcd(c \; * \; b, l \;) \; = \; 1 \;\; and \; thus \;\; gcd(c, l) \; = \; 1.$

Thus $\;\; a = k * c, \; where \; \gcd(c, l) = 1.$

$Since \; m = k * h \;\; where \;\; h < l \; and \; \gcd(h, l) = 1 \; then \; h \in U(l),$

$h^{-1} \;\; in \;\; U(l). \; Thus \;\; a \; = \;\; k * c = k * h * h^{-1} * c$

$= m * h^{-1} * c \;\;\; in \;\;\; D \; .$

$Since \;\; h^{-1}, c \;\;\; in \;\; U(l) \;\; and \;\; U(l) \; is \; a \; group \; under \; multiplication \; modulo \;\; l, \;\; we \;\; have$

$$(h^{-1} * c) \; \in U(l). \;\; Thus \;\;\; a \; = \;\;\; m * j \;\; in \;\;\; D \;\;\;\; where \;\;\; j \;\;\; in \;\;\; U(l).$$

d) <u>*D is a group isomorphic to a subgroup of $U(l)$*</u>

$Recall \;\;\; U(l) = \{b \mid 1 \leq b < l \; and \; \gcd(b, l) = 1\} \; is \; a \; group \; under \; multiplication \; modulo \; l.$

$let\ f\colon D \to U(l),\ and\ x\ in\ D.\ Then\ x = m * z\ where\ z\ in\ U(l).\ Define\ f(x) = f(m * z) = z\ in\ U(l).$ Clearly f is well-defined.

Note that $f(m) = f(m * 1) = 1.$

Let a, b in D. We show $f(a * b) = f(a) * f(b).$

$Since\ a, b \in D. we\ have\ a = m * y\ and\ b = m * w\ for\ some\ y, w\ in\ U(l).$

Hence $f(a * b) = f(m * y * m * w) = f(m * y * w) = y * w = f(a) * f(b).$

$Thus\ f\ is\ a\ group - homorphism\ from\ D\ to\ U(l).$

By construction of f, $we\ see\ that\ f(x) = 1\ iff\ x = m\ in\ D.\ Thus\ Ker(f) = \{m\}.$ Hence by the first isomorphic Theorem we have

$D = \frac{D}{Ker\{f\}}\ is\ isomorphic\ to\ Range(f)\ that\ is\ a\ subgroup\ of\ U(l).$

2. **Let m, n, k and l be defined as previous and let $D = \{kc \mid \gcd(c, l) = 1, 1 \leq c \leq l\}$. Then, D is a multiplicative group with multiplicative identity m under multiplication modulo n where D is a subset of Z_n**

$The\ following\ four\ requirements\ must\ be\ met:$

a) **Closure:**

$let\ a, b \in D, show\ that\ a * b \in D.\ Then\ a = k * c\ and\ b = k * g\ where\ c,$

$g\ in\ U(l).\ Since\ \gcd(k, l) = 1,\quad we\ have\ k * c * g = v\ in\ U(l).$

Hence $a * b = k * c * k * g = k * v\ in\ D.$

b) **Identity:**

$Since\ \ m = k * h\ \left(as\ \ it\ \ is\ \ shown\ \ in\ \ (1.c)\right)\ \ where\ h < l\ \ and\ gc\,d(h,l) =$

1, $we\ \ have\ \ m\ \ in\ \ D$. Since $l \mid (m-1)$, $we\ \ have\ \ m \equiv 1\ \ mod\ \ l$.

$let\ x = \ k * c\ \ in\ \ D\ \ where\ \ c\ \ in\ \ U(l),\ then\ x * m = \ k * c * m \equiv k * c\ mod\ (kl = n)$

$Thus\ \ m = k * h\ \ \ \ is\ the\ identity\ \ in\ \ D$.

c) <u>Inverse:</u>

$let\ \ a \in D,\ \ find\ \ \ b \in D\ \ \ such\ that\ \ \ b * a \equiv m\ mod\ n.$

Since a in D, we have $a = k * c\ \ where\ \ c\ \ in\ \ U(l)$.

$Since\ \ gcd(k,l) = \gcd(c,l)$

$= 1\ \ and\ \ \ U(l)\ \ is\ \ a\ group\ \ under\ multiplication\ \ modulo\ \ \ l,$

$there\ is\ \ a\ \ \ y\ \ \ in\ \ \ U(l)\ \ such\ \ that\ \ \ \ k * c * y \equiv h\ \ mod\ (l)$. Thus $k * c * k * y \equiv k * h = m\ \ mod(n).\ \ \ Hence\ \ n = k * y\ \ \ in\ \ D\ is\ the\ inverse\ \ of\ \ \ a$

d) <u>Associative:</u>

$Z_n\ is\ \ associative\ \ under\ \ multiplication\ \ modulo\ \ n\ \ \ and$ D $\subset Z_n$.

3. <u>Let m, n, k, l and D be defined as previous. Then, D is a field iff l is prime</u>

$since\ D\ \ is\ a\ group\ \ under\ \ multiplication\ \ modulo\ \ \ n\ \ \ with\ \ \ m\ \ as\ \ the\ \ identity,\ \ D\ \ \ is$

$group - \ isomorphic\ to\ a\ subgroup\ of\ \ \ U(l)\ \ \ by\ \ (1d).$ By construction of D, we have $D\ \ is\ \ group - isomorphic\ \ \ to\ \ \ U(l)$. It is well-known that

$U(l)\ U\ \{0\}\ \ \ is\ \ a\ field\ \ if\ and\ only\ \ if\ \ \ l\ \ is\ \ prime.$

Corollary 2: Let D be the group in theorem 1 and let |D| denotes the order (the size) of D. Then |D| | $\emptyset(l)$ *where* n, k *and* l *as in* 1.b.

$$Since\ D\ is\ group-isomorphic\ to\ a\ subgroup\ of\ U(l)\ by\ Theorem\ 1(d)$$
$$and\ |U(l)| = \emptyset(l),$$
$$the\ claim\ is\ now\ clear\ since\ the\ order\ of\ a\ subgroup\ of\ U(l)$$
$$must\ divide\ the\ order\ of\ U(l)$$

Theorem 3: let $m, n \in Z^+ such\ that \gcd(m,n) = 1. Then, D = m.U(n) is\ a\ group$ $modulo\ mn\ with\ identity\ e = mc\ for\ mc \equiv 1\ mod\ (n), c \in U(n)$

a) Closure:

$$let\ a, b \in D \rightarrow a = m * x\ , b = m * y\ for\ x, y \in U(n)$$
$$a * b = m * x * m * y$$
$$since \gcd(m,n) = 1\ then\ x * m * y = z\ mod\ n\ for\ z \in U(n)$$
$$hence, a * b = m * z \in D$$

b) Identity:

$$for\ identity\ e\ as\ defined, show\ that\ a * e = e\ mod\ mn$$
$$for\ a \in D, a = m * x\ for\ x \in U(n)$$
$$a * e = m * x * e \equiv m * x * m * c\ mod\ (mn)$$
$$\rightarrow x * e \equiv x * m * c\ mod\ (n), since\ m * c \equiv 1 mod(n)$$
$$x * e \equiv x * 1 \equiv x\ mod(n)$$
$$then, a * e = m * x * e \equiv m * x = a$$

c) Inverse:

$$let\ a \in D, show\ that \exists\ b \in D\ such\ that\ a * b \equiv e\ mod\ mn$$

$$let\ a = m * x\ , \qquad for\ x \in U(n)$$

$$since\ \gcd(m, n) = 1\ and\ U(n) is\ group$$

$$then \exists\ w\ \in U(n)\ where\ w * m * x = c\ \in U(n)$$

$$hence, m * x * m * w \equiv m * c = e$$

$$Therefore, b = m * w\ is\ the\ inverse\ of\ a$$

d) Associativity:

$$D\ C\ Z_{mn}\ which\ is\ associative\ under\ multiplication\ mod\ mn$$

EXAMPLES

Example 1:

Let m = 5

$$m - 1 = 4 = 2^2 \rightarrow k = 5 \; and \; l = \{2,4\}$$

Then, $n_1 = 5 \, . \, 2 = 10 \, , n_2 = 5 \, . \, 4 = 20$

5 is the multiplicative identity for some group D ∈ Z_n under multiplication modulo n where n = {10, 20}

Check:

$$5^2 mod \; 10 \; \equiv 5$$

$$5^2 mod \; 20 \; \equiv 5$$

a) $D \; \in Z_{10}$

$n = 10 = 5 \, . \, 2 = k \, . \, l \; for \; k | \; 5 \; and \; l | 4 \rightarrow k = 5, l = 2$

$D = \{ \, 5c \mid \gcd(c, 2) = 1, 1 \leq c \leq 2\}$

$\rightarrow D = \{5\}$

b) $D \; \in \; Z_{20}$

$n = 20 = 5 \, . \, 4 = k \, . \, l \; for \; k | 5 \; and \; l | 4 \rightarrow k = 5, l = 4$

$D = \{5c \mid \gcd(c, 4) = 1, 1 \leq c \leq 4\}$

$\rightarrow D = \{ \, 5(1), 5(3)\} = \{5 \, , 15\}$

To show that these are the only groups, Cayle's table is used for $(Z_{20},*)$. Cayley's table for the Z_{20} is constructed in this example only to show that D is the only set that forms a group. In the other examples, Cayley's table will be used to show that D satisfies the group requirements.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	2	4	6	8	10	12	14	16	18	0	2	4	6	8	10	12	14	16	18
3	3	6	9	12	15	18	1	4	7	10	13	16	19	2	5	8	11	14	17
4	4	8	12	16	0	4	8	12	16	0	4	8	12	16	0	4	8	12	16
5	5	10	15	0	5	10	15	0	5	10	15	0	5	10	15	0	5	10	15
6	6	12	18	4	10	16	2	8	14	0	6	12	18	4	10	16	2	8	14
7	7	14	1	8	15	2	9	16	3	10	17	4	11	18	5	12	19	6	13
8	8	16	4	12	0	8	16	4	12	0	8	16	4	12	0	8	16	4	12
9	9	18	7	16	5	14	3	12	1	10	19	8	17	6	15	4	13	2	11
10	10	0	10	0	10	0	10	0	10	0	10	0	10	0	10	0	10	0	10
11	11	2	13	4	15	6	17	8	19	10	1	12	3	14	5	16	7	18	9
12	12	4	16	8	0	12	4	16	8	0	12	4	16	8	0	12	4	16	8
13	13	6	19	12	5	18	11	4	17	10	3	16	9	2	15	8	1	14	7
14	14	8	2	16	10	4	18	12	6	0	14	8	2	16	10	4	18	12	6
15	15	10	5	0	15	10	5	0	15	10	5	0	15	10	5	0	15	10	5
16	16	12	8	4	0	16	12	8	4	0	16	12	8	4	0	16	12	8	4
17	17	14	11	8	5	2	19	16	13	10	7	4	1	18	15	12	9	6	3
18	18	16	14	12	10	8	6	4	2	0	18	16	14	12	10	8	6	4	2
19	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Note that only the set {5, 10, 15} satisfies 5 as the multiplicative identity. Then, in order to maintain closure, we need to check 10*10, 10*15, and 15*10. Since 10*10= 0 mod 20, and $0 \notin Z_{20}$, 10 is eliminated from the set. The set now becomes {5, 15}. Now 15*15=5 mod 20 therefore, 15 is the inverse of itself. Since the set {5, 15} maintains closure, inverse, associativity and identity for multiplication modulo 20. Then {5, 15} is a group.

$\in Z_{20}$, $l = 4 \; and \; D = \{5, 15\}$,

$$U(l) = \{1, 3\} \; since \; l \; is \; not \; a \; prime \; , then \; D \; is \; not \; a \; field:$$

$D \; is \; not \; closed \; under \; addition \; since \; 5 + 5 = 10 \notin D.$

$Whereas, in\ Z_{10}, l = 2\ and\ D = \{5\}$ $abelian\ group\ under\ multiplication$

$now\ D\ U\ \{0\} = \{0,5\}$ $abelian\ group\ under\ addition\ (Trivial)$

$Distributive\ property\ of\ multiplication\ over\ addition\ is\ true\ for\ all\ integers\ Z$

$since\ Z_n is\ a\ subset\ of\ Z\ then\ it\ holds\ the\ same\ property.$

$Then\ D\ U\{0\} is\ a\ field.$

$This\ result\ is\ also\ concluded\ directly\ by\ looking\ at\ l. l = 2\ is\ a\ prime.$

$Therefore, D\ U\ \{0\}\ is\ a\ field$

Example 2:

Let m = 8

$$m - 1 = 7 \rightarrow k = \{2, 4, 8\} \ and \ l = \{7\}$$

Then, $n_1 = 2 * 7 = 14$, $n_2 = \ 4 * 7 = 28$, $n_3 = 8 * 7 = 56$

8 is the multiplicative identity for some group D ∈ Z_n under multiplication modulo n where n = {14, 28, 56}

Check:

$8^2 mod\ 14 \ \equiv 8$

$8^2 mod\ 28 \ \equiv 8$

$8^2 mod\ 56 \ \equiv 8$

a) $D \ \in Z_{14}$

$n = 14 = k \,.\, l \ \rightarrow l = 7, k = 2$

$D = \{\, 2c \mid \gcd(c, 7) = 1, 1 \leq c \leq 7\}$

$\rightarrow D = \{2(1), 2(2), 2(3), \dots, 2(6)\} = \{2, 4\ , 6\ , 8, 10, 12\}$

	2	4	6	8	10	12
2	4	8	12	2	6	10
4	8	2	10	4	12	6
6	12	10	8	6	4	2
8	2	4	6	8	10	12
10	6	12	4	10	2	8
12	10	6	2	12	8	4

b) $D \ \in \ Z_{28}$

$n = 28 = 7 \ * 4 \rightarrow l = 7, k = 4$

$D = \{4c \mid \gcd(c, 7) = 1, 1 \leq c \leq 7\}$

$\rightarrow D = \{4(1), 4(2), \dots 4(6)\} = \{4, 8, 12, 16, 20, 24\}$

	4	8	12	16	20	24
4	16	4	20	8	24	12
8	4	8	12	16	20	24
12	20	12	4	24	16	8
16	8	16	24	4	12	20
20	24	20	16	12	8	4
24	12	24	8	20	4	16

c) $D \in Z_{56}$

$n = 56 = 7 * 8 \rightarrow l = 7, k = 8$

$D = \{8c \mid \gcd(c, 7) = 1, 1 \leq c \leq 7\}$

$\rightarrow D = \{8(1), 8(2), \dots, 8(7)\}$

	8	16	24	32	40	48
8	8	16	24	32	40	48
16	16	32	48	8	24	40
24	24	48	16	40	8	32
32	32	8	40	16	48	24
40	40	24	8	48	32	16
48	48	40	32	24	16	8

All three groups constructed are isomorphic to the set {1, 2, 3, 4, 5, 6,}=$U(7)$. It can be easily observed that all three sets $D\ U\ \{0\}$ form finite closed fields since 7 is prime.

Example 3:

Let m = 37

$$m - 1 = 36 \rightarrow k = 37 \ \ and \ l = \{2,3,4,6,9,12,18,36\}$$

Then, $n_1 = 37 \,.\, 2 = 74$, $n_2 = 37 \,.\, 2^2 = 148$, $n_3 = 37 \,.\, 3 = 111$, $n_4 = 37 \,.\, 3^2 = 333$,

$n_5 = 37 \,.\, 3 \,.\, 2 = 222, n_6 = 37 \,.\, 2^2 . 3 = 444$, $n_7 = 37 \,.\, 2 \,.\, 3^2 = 666$,

$n_8 = 37 \,.\, 2^2 . 3^2 = 1332$

37 is the multiplicative identity for some group D ∈ Z_n under multiplication modulo n where n = {74, 111, 148, 222, 333, 444, 666, 1332}

Check:

$37^2 mod\ 74 \ \equiv 37$

$37^2 mod\ 111 \ \equiv 37$

$37^2 mod\ 148 \ \equiv 37$

$37^2 mod\ 222 \equiv 37$

$37^2 mod\ 333 \equiv 37$

$37^2 mod\ 444 \equiv 37$

$37^2 mod\ 666 \equiv 37$

$37^2 mod\ 1332 \ \equiv 37$

a) $D \ \in Z_{74}$

$n = 74 = k \,.\, l \ \rightarrow l = 2, k = 37$

$D = \{\, 37c \mid \gcd(c, 2) = 1, 1 \le c \le 2\}$

$\rightarrow D = \{37(1)\} = \{37\}$

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(2) = \{1\}$

$D\ U\ \{0\}\ is\ a\ field$

b) $D\ \in Z_{111}$

$n = 111 = k\,.\,l\ \rightarrow l = 3, k = 37$

$D = \{\, 37c \mid \gcd(c, 3) = 1, 1 \le c \le 3\}$

$\rightarrow D = \{37(1), 37(2)\} = \{37{,}74\}$

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(3) = \{1{,}2\}$

$D\ U\ \{0\}\ is\ a\ field$

c) $D\ \in Z_{148}$

$n = 148 = k\,.\,l\ \rightarrow l = 4, k = 37$

$D = \{\, 37c \mid \gcd(c, 4) = 1, 1 \le c \le 4\}$

$\rightarrow D = \{37(1), 37(3)\} = \{37{,}111\}$

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(4) = \{1{,}3\}$

$D\ U\ \{0\}\ is\ not\ a\ field\ since\ 37 + 37 = 74 \notin D$

$\rightarrow D\ U\ \{0\}\ is\ not\ a\ closed\ group\ under\ addition$

d) $D\ \in Z_{222}$

$n = 222 = k\,.\,l\ \rightarrow l = 6, k = 37$

$D = \{\, 37c \mid \gcd(c, 6) = 1, 1 \le c \le 6\}$

$\rightarrow D = \{37(1), 37(5), \} = \{37{,}185\}$

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(6) = \{1{,}5\}$

$D\ U\ \{0\}\ is\ not\ a\ field\ since\ 37 + 37 = 74 \notin D$

$\rightarrow D\ U\ \{0\}\ is\ not\ a\ closed\ group\ under\ addition$

e) $D \in Z_{333}$

$n = 333 = k \,.\, l \;\rightarrow l = 9, k = 37$

$D = \{\, 37c \mid \gcd(c, 9) = 1, 1 \leq c \leq 9\}$

$\rightarrow D = \{37(1), 37(2), 37(4), 37(5), 37(7), 37(8)\}$

$= \{37,74, 148, 185, 259,296\}$

	37	74	148	185	259	296
37	37	74	148	185	259	296
74	74	148	296	37	185	259
148	148	296	259	74	37	185
185	185	37	74	259	296	148
259	259	185	37	296	148	74
296	296	259	185	148	74	37

Note that D is isomorphic to a subgroup in $U(9) = \{1,2,4,5,7,8\}$

$D\ U\ \{0\}$ *is not a field since* $37 + 74 = 111 \notin D$

$\rightarrow D\ U\ \{0\}$ *is not a closed group under addition*

f) $D \in Z_{333}$

$n = 333 = k \,.\, l \;\rightarrow l = 9, k = 37$

$D = \{\, 37c \mid \gcd(c, 9) = 1, 1 \leq c \leq 9\}$

$\rightarrow D = \{37(1), 37(8)\} = \{37,296\}$

D is isomprphic to a subgroup in $U(9) = \{1,8\}$

$D\ U\ \{0\}$ *is not a field since* $37 + 74 = 111 \notin D$

$\rightarrow D\ U\ \{0\}$ *is not a closed group under addition*

g) $D \in Z_{444}$

$n = 333 = k \,.\, l \;\rightarrow l = 12, k = 37$

$D = \{\, 37c \mid \gcd(c, 12) = 1, 1 \leq c \leq 12\}$

$\rightarrow D = \{37(1), 37(5), 37(7), 37(11)\} = \{37,185,259, 407\}$

	37	185	259	407
37	37	185	259	407
185	185	37	407	259
259	259	407	37	185
407	407	259	185	37

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(12) = \{1,5,7,11\}$

$D\ U\ \{0\}\ is\ not\ a\ field\ since\ 37 + 37 = 74 \notin D$

$\rightarrow D\ U\ \{0\}\ is\ not\ a\ closed\ group\ under\ addition$

h) $D\ \in Z_{444}$

$n = 333 = k\ .\ l\ \rightarrow l = 12, k = 37$

$D = \{\ 37c \mid \gcd(c, 12) = 1, 1 \leq c \leq 12\}$

$\rightarrow D = \{37(1), 37(11)\} = \{37, 407\}$

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(12) = \{1,11\}$

$D\ U\ \{0\}\ is\ not\ a\ field\ since\ 37 + 37 = 74 \notin D$

$\rightarrow D\ U\ \{0\}\ is\ not\ a\ closed\ group\ under\ addition$

i) $D\ \in Z_{666}$

$n = 666 = k\ .\ l\ \rightarrow l = 18, k = 37$

$D = \{\ 37c \mid \gcd(c, 18) = 1, 1 \leq c \leq 18\}$

$\rightarrow D = \{37(1), 37(5), 37(7), 37(11), 37(13), 37(17)\}$

$= \{37,185,259, 407,481, 629\}$

	37	185	259	407	481	629
37	37	185	259	407	37	185
185	185	37	407	259	185	37
259	259	407	37	185	259	407
407	407	259	185	37	407	259
481	37	185	259	407	37	185
629	185	37	407	259	185	37

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(18) = \{1,5,7,11,13,17\}$

$D\ U\ \{0\}\ is\ not\ a\ field\ since\ 37 + 37 = 74 \notin D$

$\rightarrow D\ U\ \{0\}\ is\ not\ a\ closed\ group\ under\ addition$

j) $D\ \in Z_{1332}$

$n = 1332 = k\ .\ l\ \rightarrow l = 36, k = 37$

$D = \{\ 37c \mid \gcd(c, 36) = 1, 1 \leq c \leq 36\}$

$\rightarrow D$

$$= \begin{Bmatrix} 37(1), 37(5), 37(7), 37(11), 37(13), 37(17), 37(19), 37(23), 37(25), \\ 37(29), 37(31), 37(35) \end{Bmatrix}$$

$$= \{37,185,259,407,481,629,703,851,925,1073,1147,1295\}$$

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(36)$

$$= \{1,5,7,11,13,17,19,23,25,29,31,35\}$$

$D\ U\ \{0\}\ is\ not\ a\ field\ since\ 37 + 37 = 74 \notin D$

$\rightarrow D\ U\ \{0\}\ is\ not\ a\ closed\ group\ under\ addition$

	37	185	259	407	481	629	703	851	925	1073	1147	1295
37	37	185	259	407	481	629	703	851	925	1073	1147	1295
185	185	925	1295	703	1073	481	851	259	629	37	407	1147
259	259	1295	481	185	703	407	925	629	1147	851	37	1073
407	407	703	185	481	1295	259	1073	37	851	1147	629	925
481	481	1073	703	1295	925	185	1147	407	37	629	259	851
629	629	481	407	259	185	37	1295	1147	1073	925	851	703
703	703	851	925	1073	1147	1295	37	185	259	407	481	629
851	851	259	629	37	407	1147	185	925	1295	703	1073	481
925	925	629	1147	851	37	1073	259	1295	481	185	703	407
1073	1073	37	851	1147	629	925	407	703	185	481	1295	259
1147	1147	407	37	629	259	851	481	1073	703	1295	925	185
1295	1295	1147	1073	925	851	703	629	481	407	259	185	37

Note that in every Cayley's table for D, every element appears only once in each raw/column. Also, since multiplication is abelian, the table is symmetric around the diagonal

(for previous example, the diagonal is from (37,37) to (1295,1295)). Also, for every number, we can find the inverse of that number by locating the identity in its raw/column. The number corresponding to that raw/column is the inverse. Since every element appears once, the inverse is unique.

Also, note that the order of D, |D|, is given by $\emptyset(l)$

For example,

$$for\ D\ \in Z_{1332}, l = 36\ = 2^2 * 3^2 \rightarrow\ \emptyset(36) = 36\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 12$$

$$|D| = |\{37,185,259,407,481,629,703,851,925,1073,1147,1295\}| = 12$$

$$for\ D\ \in Z_{333}, l = 9 = 3^2 \rightarrow\ \emptyset(9) = 9\left(1-\frac{1}{3}\right) = 6$$

$$|D| = |\{37,74,148,185,259,296\}| = 6$$

Example 4:

Let m = 16

$$m - 1 = 15,$$

now for l & k we can use prime factorization instead of the previous method:

$m(m-1) = 16 * 15 = 2^4 * 3 * 5$

$K = \{2, 4, 8, 16\}\ and\ L = \{3, 5, 15\}$

$now\ \ n = k * l\ for\ k \in K\ and\ l \in L\ where\ n > m$

Then, $n_1 = 2 * 15 = 30, n_2 = 4 * 5 = 20, n_3 = 4 * 15 = 60, n_4 = 8 * 3 = 24,$

$n_5 = 8 * 5 = 40\ , n_6 = 8 * 15 = 120, n_7 = 16 * 3 = 48, n_8 = 16 * 5 = 80,$

$n_9 = 16 * 15 = 240$

$Note\ that\ although\ 2 \in K\ and\ 3 \in L\ but\ 16\ \notin Z_6$

16 is the multiplicative identity for some group D ∈ Z_n under multiplication modulo n where n = {20, 21, 30, 40, 48, 60, 80, 120, 240}

Check:

$16^2 mod\ 20\ \equiv 16$

$16^2 mod\ 24\ \equiv 16$

$16^2 mod\ 30\ \equiv 16$

$16^2 mod\ 40 \equiv 16$

$16^2 mod\ 48 \equiv 16$

$16^2 mod\ 60 \equiv 16$

$16^2 mod\ 80 \equiv 16$

$16^2 mod\ 120 \equiv 16$

$16^2 mod\ 240 \equiv 16$

a) $D \in Z_{20}$

$n = 20 = k\,.\,l \rightarrow l = 5, k = 4$

$D = \{\, 4c \mid \gcd(c,5) = 1, 1 \leq c \leq 5\}$

$\rightarrow D = \{4(1), 4(2), 4(3), 4(4)\} = \{4,8,12,16\}$

	4	8	12	16
4	16	12	8	4
8	12	4	16	8
12	8	16	4	12
16	4	8	12	16

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(5) = \{1,2,3,4\}$

$D\ U\ \{0\}\ is\ a\ field\ since\ l\ is\ a\ prime$

b) $D \in Z_{24}$

$n = 24 = k\,.\,l \rightarrow l = 3, k = 8$

$D = \{8c \mid \gcd(c,3) = 1, 1 \leq c \leq 3\}$

$\rightarrow D = \{8(1), 8(2)\} = \{8,16\}$

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(3) = \{1,2\}$

$D\ U\ \{0\}\ is\ a\ field$

c) $D \in Z_{30}$

$n = 30 = k\,.\,l \rightarrow l = 15, k = 2$

$D = \{\, 2c \mid \gcd(c,15) = 1, 1 \leq c \leq 15\}$

$\rightarrow D = \{2(1), 2(2), 2(4), 2(7), 2(8), 2(11), 2(13), 2(14)\}$

$D = \{2, 4\ 8, 14, 16, 22, 26, 28\}$

	2	4	8	14	16	22	26	28
2	4	8	16	28	2	14	22	26
4	8	16	2	26	4	28	14	22
8	16	2	4	22	8	26	28	14
14	28	26	22	16	14	8	4	2
16	2	4	8	14	16	22	26	28
22	14	28	26	8	22	4	2	16
26	22	14	28	4	26	2	16	8
28	26	22	14	2	28	16	8	4

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(15) = \{1,2,4,7,8,11,13,14\}$

$D\ U\ \{0\}\ is\ not\ a\ field\ since\ 2 + 4 = 6 \notin D$

$\rightarrow D\ U\ \{0\}\ is\ not\ a\ closed\ group\ under\ addition$

d) $D\ \in Z_{30}$

$n = 30 = k\ .\ l\ \rightarrow l = 15, k = 2$

$D = \{\ 2c \mid \gcd(c, 15) = 1, 1 \leq c \leq 15\}$

$\rightarrow D = \{2(2), 2(8)\}$

$D = \{4,16\}$

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(15) = \{2,8\}$

$D\ U\ \{0\}\ is\ not\ a\ field\ since\ 2 + 4 = 6 \notin D$

$\rightarrow D\ U\ \{0\}\ is\ not\ a\ closed\ group\ under\ addition$

e) $D\ \in Z_{40}$

$n = 40 = k\ .\ l\ \rightarrow l = 5, k = 8$

$D = \{\ 8c \mid \gcd(c, 5) = 1, 1 \leq c \leq 5\}$

$\rightarrow D = \{8(1), 8(2), 8(3), 8(4)\} = \{8, 16, 24, 32\}$

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

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(5) = \{1,2,3,4\}$

$D\ U\ \{0\}\ is\ a\ field$

f) $D\ \in Z_{48}$

$n = 48 = k\ .\ l\ \rightarrow l = 3, k = 16$

$D = \{\ 16c \mid \gcd(c,3) = 1, 1 \leq c \leq 3\}$

$\rightarrow D = \{16(1), 16(2)\} = \{16,32\}$

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(3) = \{1,2\}$

$D\ U\ \{0\}\ is\ a\ field$

g) $D\ \in Z_{60}$

$n = 60 = k\ .\ l\ \rightarrow l = 15, k = 4$

$D = \{\ 4c \mid \gcd(c,15) = 1, 1 \leq c \leq 15\}$

$\rightarrow D = \{4(1), 4(2), 4(4), 4(7), 4(8), 4(11), 4(13), 4(14)\}$

$= \{4, 8, 16, 28, 32, 44, 52, 56\}$

	4	16	28	32	44	52	56
4	16	4	52	8	56	28	44
16	4	16	28	32	44	52	56
28	52	28	4	56	32	16	8
32	8	32	56	4	28	44	52
44	56	44	32	28	16	8	4
52	28	52	16	44	8	4	32
56	44	56	8	52	4	32	16

$Note\ that\ D\ is\ isomorphic\ to\ a\ subgroup\ \ in\ U(15) = \{1,2,4,7,8,11,13,14\}$

$D\ U\ \{0\}\ is\ not\ a\ field\ since\ 4 + 4 = 8 \notin D$

$\rightarrow D\ U\ \{0\}\ is\ not\ a\ closed\ group\ under\ addition$

h) $D \in Z_{80}$

$n = 80 = k \,.\, l \rightarrow l = 5, k = 16$

$D = \{\, 16c \mid \gcd(c, 5) = 1, 1 \leq c \leq 5\}$

$\rightarrow D = \{16(1), 16(2), 16(3), 16(4)\}$ = {16, 32, 48, 64}

	16	32	48	64
16	16	32	48	64
32	32	64	16	48
48	48	16	64	32
64	64	48	32	16

Note that D is isomorphic to a subgroup in $U(5) = \{1,2,3,4\}$

$D\ U\ \{0\}$ *is a field*

i) $D \in Z_{120}$

$n = 120 = k \,.\, l \rightarrow l = 15, k = 8$

$D = \{\, 8c \mid \gcd(c, 15) = 1, 1 \leq c \leq 15\}$

$\rightarrow D = \{8(1), 8(2), 8(4), 8(7), 8(8), 8(11), 8(13), 8(14)\}$

$D = \{8,16,32,56,64,88,104,112\}$

	8	16	32	56	64	88	104	112
8	64	8	16	88	32	104	112	56
16	8	16	32	56	64	88	104	112
32	16	32	64	112	8	56	88	104
56	88	56	112	16	104	8	64	32
64	32	64	8	104	16	112	56	88
88	104	88	56	8	112	64	32	16
104	112	104	88	64	56	32	16	8
112	56	112	104	32	88	16	8	64

Note that D is isomorphic to a subgroup in $U(15) = \{1,2,4,7,8,11,13,14\}$

$D\ U\ \{0\}$ *is not a field since* $8 + 16 = 24 \notin D$

$\rightarrow D\ U\ \{0\}$ *is not a closed group under addition*

j) $D \in Z_{240}$

$n = 240 = k \,.\, l \;\rightarrow l = 15, k = 16$

$D = \{\, 16c \mid \gcd(c, 15) = 1, 1 \leq c \leq 15\}$

$\rightarrow D = \{16(1), 16(2), 16(4), 16(7), 16(8), 16(11), 16(13), 16(14)\}$

$D = \{16, 32, 64, 112, 128, 176, 208, 224\}$

	16	32	64	112	128	176	208	224
16	16	32	64	112	128	176	208	224
32	32	64	128	224	16	112	176	208
64	64	128	16	208	32	224	112	176
112	112	224	208	64	176	32	16	128
128	128	16	32	176	64	208	224	112
176	176	112	224	32	208	16	128	64
208	208	176	112	16	224	128	64	32
224	224	208	176	128	112	64	32	16

Note that D is isomorphic to a subgroup in $U(15) = \{1,2,4,7,8,11,13,14\}$

$D \; U \; \{0\}$ *is not a field since* $16 + 32 = 48 \notin D$

$\rightarrow D \; U \; \{0\}$ *is not a closed group under addition*

REFERENCES

Gallian, J. A. (2010). Contemporary abstract algebra. Belmont: Brooks/Cole, Cengage Learning