Results and Problems on Constructing Multiplicative Groups in Modular Arithmetic

Purwanto*, Indriati Nurul Hidayah, Dahliatul Hasanah
Department of Mathematics,
Universitas Negeri Malang,
Jalan Semarang 5, Malang, 65145,
Indonesia
*Email: purwanto.fmipa@um.ac.id

Abstract

It is known that groups occur in modular arithmetic, including multiplicative groups. It is well known that for each integer $n > 1$, the set of all positive integers less than n and relative prime to n is a group under multiplication modulo n. Many authors have studied multiplicative groups in modular arithmetic, and many multiplicative groups in modular arithmetic each of which has an identity element which is not necessarily 1 have been constructed. In this paper we review some of the constructions, and show that there still exists a problem to find other constructions.

Key words: problem, construction, group, multiplicative, modular arithmetic

1. Introduction

It is known that groups occur in modular arithmetic, including multiplicative groups. It is well known (see Gallian [1] p.44) that for each integer $n \geq 1$, the set of all positive integers less than n is a group under addition modulo n; and the set of all positive integers less than n and relative prime to n is a group under multiplication modulo n. Many authors have studied these groups, for example, McLean [2], Denniss [3], Brakes [4], and Hidayah and Purwanto [5]. Many groups in modular arithmetic each of which has an identity element which is not necessarily 1 have been constructed. The question is "Are there any other construction?"

Before we continue our discussion, we recall some notation and terminology. For the most part of our notation and terminology we follow that of Gallian [1]. Let n be a fixed positive integer, and a and b be any integers. We write $a \equiv b \bmod n$ when n divides $a - b$. We also write modulo n as $\bmod n$. The arithmetic modulo n (operations addition and multiplication modulo n) is defined as follows. A number $a + b \equiv c \bmod n$ when n divides $a + b - c$. Similarly, a number $a \times b \equiv c \bmod n$ when n divides $a \times b - c$. We write $a \times b$ as ab. For example,

$$27 \equiv 3 \bmod 12 \text{ since } 12 \text{ divides } 27 - 3,$$

$$11 + 17 \equiv 4 \bmod 12 \text{ since } 12 \text{ divides } 11 + 17 - 4,$$

$$5 \times 7 \equiv 11 \bmod 12 \text{ since } 12 \text{ divides } 5 \times 7 - 11.$$

Modular arithmetic is very useful for studying other topic in mathematics. For example, in [6], Hidayah and Purwanto use modular arithmetic to construct graphs.

A nonempty set *G* with a binary operation on *G* is a group if it satisfies the following three properties:

(1) $\forall a, b, c \in G, (ab)c = a(bc)$, i.e., the operation is associative,

(2) $\exists e \in G, \forall a \in G, \ni ae = ea = a$, i.e., there exists an identity element e in *G*,

(3) $\forall a \in G, \exists a^{-1} \in G \ni aa^{-1} = a^{-1}a = e$, i.e., each element of *G* has an inverse in *G*.

For an integer $n \geq 1$, the set of integers modulo n, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, is a group under addition modulo *n*. For $n > 1$, the set of all positive integers less than *n* and relative prime to n, $\mathbb{U}_n = \{a \in \mathbb{Z}_n | (a, n) = 1\}$, is a group under multiplication modulo n, the identity element is 1.For examples, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ and $\mathbb{U}_5 = \{1, 2, 3, 4\}$ are groups under addition modulo 5 and under multiplication modulo 5, respectively.

We can use Cayley table to describes the structure of a finite group by arranging all the possible products of all the group's elements in a square table. Many properties of a group can be discovered from its Cayley table, such as whether or not the group is abelian, which element is an identity element, and which elements are inverses of which elements. Cayley table of $\mathbb{Z}_5$ is as in Table 1.. It can be seen that its identity elements is 0.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 1. Caley table of $\mathbb{Z}_5$

Cayley table of $\mathbb{U}_5$ is as in Table 2. It can be seen that its identity elements is 1.

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Table 2. Cayley table of $\mathbb{U}_5$

The set $\{1, 2, 3, 4, 5\}$ is not a group under multiplication modulo 6; it has identity element 1, but there is an element that has no invers. The elements 2, 3, and 4, have no invers. In addition, the set is not closed under multilpication. Its Cayley table is as in Table 3.

×	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Table 3. Elements 2, 3, and 4 have no invers

In the multiplicatve group $\mathbb{U}_n = \{a \in \mathbb{Z}_n | (a, n) = 1\}$, the identity element is 1, but it is known that some group under multiplication modulo n have an identity element which is not necessarily 1. For example, $\{3, 6, 9, 12\}$ is a group under multiplication modulo 5 with the identity element is 6. Its Caley table is Table 4.

×	3	6	9	12
3	9	3	12	6
6	3	6	9	12
9	12	9	6	3
12	6	12	3	9

Table 4. Multiplicative group modulo 5

In this paper we review some of the constructions, and show that there still exists a problem to find other constructions.

2. Construction

In this section we review some construction of multiplicative groups in modular arithmetic each of which has an identity element which is not necessarily 1. Some of the construction is an extension of the existing group, and some other is a new construction.

McLeans [2] constructs a new group from the existing multiplicative group by multiplying every element of the group and the modulo number by an element of the group. For example, $\mathbb{U}_5 = \{1, 2, 3, 4\}$ is a group under multiplication modulo 5; multiply every element by 3 we get a multiplicative group modulo 15

$$\{3, 6, 9, 12\}.$$

Such construction is known as McLean's criterion.

McLean's Criterion. *If* $G = \{e, a, b, \dots\}$ *(mod* n*) is a multiplicative group, then* $G = \{ke, ka, kb, \dots\}$ *(mod* kn*) is a multiplicative group if and only if* $ke \in G$. []

Other example, if we multiply every element of multiplicative group modulo 14

$$\mathbb{U}_{15} = \{1, 3, 5, 9, 11, 13\}$$

by 5 , then we we get a multiplicative group modulo 70

$$\{5, 15, 25, 45, 55, 65\}.$$

Its Caley table is as in Table 5.

×	5	15	25	45	55	65
5	25	3	55	15	65	45
15	5	15	25	45	55	65
25	55	25	65	5	45	15
45	15	45	5	65	25	55
55	65	55	45	25	15	5
65	45	65	15	55	5	45

Table 5. Multiplicative group modulo 70

Denniss [2] constructs groups in modular arithmetic under multiplication modulo *m* each of which has an identity element which is not necessarily 1, for some value of *m*. Dennis starts the construction by considering a set $\{1, n, n^2, \dots, n^{q-1}\}$, where n and q are positive integers, $n > 1$, and using the fact that

$$n^q - 1 = (n - 1)(1 + n + n^2 + \cdots + n^{q-1}),$$

$$n^q \equiv 1 \bmod(1 + n + n^2 + \cdots + n^{q-1}),$$

since$(1 + n + n^2 + \cdots + n^{q-1})$ divides $n^q - 1$. Thus,

$$\{1, n, n^2, \dots, n^{q-1}\}$$

is a group under multiplication modulo $(1 + n + n^2 + \cdots + n^{q-1})$. Then, by McLean's criterion, Dennis has the following result.

Theorem 2.1 (Denniss). *Let* n *and* q *be positive integers,* $n > 1$*, and* $k \equiv n^i \bmod(1 + n + n^2 + \cdots + n^{q-1})$ *for some integer* $i \geq 0$*. Then the set* $\{k, kn, kn^2, \dots, kn^{q-1}\}$ *forms a group under multiplication* $\bmod(k + kn + kn^2 + \cdots + kn^{q-1})$. []

For example, in Theorem 2.1, if we let $n = 5$, $q = 4$, and $k = 1$, then we have

$$\{1, 5, 25, 125\}$$

is a group under multiplication modulo 1 + 5 + 25 + 125 = 156. If we take k = 5, then we have

$$\{5, 25, 125, 625\}$$

is a group under multiplication modulo 5 + 25 + 125 + 625 = 780. Its identity element is 625, and its Cayley table is as in the following Table 6.

×	5	25	125	625
5	25	125	625	5
25	125	64	5	25
125	625	5	25	125
625	5	25	125	625

Table 6. Multiplicative group modulo 780

In Theorem 2.1, let $m = k + kn + kn^2 + ... + kn^{q-1}$. Hidayah and Purwanto (2016) find other possible values of m such that $\{k, kn, kn^2, ..., kn^{q-1}\}$ is also a group under multiplication modulo m. This slightly extends Denniss' theorem.

Considering the set $\{1, n, n^2, \ldots, n^{q-1}\}$, where n and q are positive integers, n > 1, and let d be a popsitive integer divide $n - 1$. By using the fact that

$$n^q - 1 = (n-1)(1 + n + n^2 + \cdots + n^{q-1}),$$
$$n^q \equiv 1 \bmod d(1 + n + n^2 + \cdots + n^{q-1}),$$

$d(1 + n + n^2 + \cdots + n^{q-1})$divides $n^q - 1$, we have

$$\{1, n, n^2, \ldots, n^{q-1}\}$$

is a group under multiplication modulo $d(1 + n + n^2 + \cdots + n^{q-1})$. Then, by McLean's criterion, we have following result.

Theorem 2.2 (Hidayah and Purwanto). *Let n, d, and q be positive integers,* n > 1, q > 1, *d divide* $n - 1$, *and* $s = d(1 + n + n^2 + \cdots + n^{q-1})$. *If* $k \equiv n^i$ mod s *for some integer* i > 1, *then the set* $\{k, kn, kn^2, \ldots, kn^{q-1}\}$ *forms a group under multiplication* mod ks. *Its identity element is e where* $e \equiv$ 1mod s. []

For example, in Theorem 2.1, if we let n = 5and q = 4, then we can have d = 4, and so s = 4(1 + 5 + 5^2 + 5^3) = 624. If we take k = 1, then we have

$$\{1, 5, 25, 125\}$$

is a group under multiplication modulo s = 4(1 + 5 + 25 + 125) = 624. If we take k = 5, then we have

$$\{5, 25, 125, 625\}$$

is a group under multiplication modulo $ks = 5(624) = 3120$. Its identity element is 625, and its Cayley table is as in Table 2.2.

Let the group in Theorem 2.2 be G. Hidayah and Purwanto [5] extend the set G. They find a set $H \supseteq G$ such that H is also a group under multiplication modulo m. They use the following remark.

Remark 2.3. *If G is a group under multiplication modulo m with the identity element e, then the set $H = \{h|h = g \text{ or } h = m - g, for\ some\ g \in G\}$ is also a group under multiplication modulo m with identity element e.*

For example, since

$$\{1, 5, 25, 125\}$$

is a group under multiplication modulo $m = 624$, then

$$\{1, 5, 25, 125, 624 - 1, 624 - 5, 624 - 25, 624 - 125\}$$
$$= \{1, 5, 25, 125, 499, 599, 619, 623\}$$

is a group under multiplication modulo $m = 624$. Its Cyley table is as in Table 7.

×	1	5	25	125	499	599	619	623
1	1	5	25	125	499	599	619	623
5	5	25	125	1	623	499	599	619
25	25	125	1	5	619	623	499	599
125	125	1	5	25	599	619	623	499
499	499	623	619	599	25	5	1	125
599	599	499	623	619	5	1	125	25
619	619	599	499	623	1	125	25	5
623	623	619	599	499	125	25	5	1

Table 7. Multiplicative group modulo 624

By using Theorem 2.2 and Remark 2.3 we find the following result.

Theorem 2.4 (Hidayah and Purwanto). *Let n, d, and q be positive integers, $n > 1$, $q > 1$, d divide $n - 1$, and $s = d(1 + n + n^2 + \cdots + n^{q-1})$. If $k \equiv n^i \bmod s$ for some integer $i > 1$, then the set $\{h \mid h = kn^j \text{ or } h = k(s - n^j), j = 0, 1, 2, \dots q - 1\}$ forms a group under multiplication $\bmod ks$. Its identity element is ewhere $e \equiv 1 \bmod s$.* []

For example, in Theorem 2.4, if we let $n = 5$ and $q = 4$, then we can have $d = 4$, and so $s = 4(1 + 5 + 5^2 + 5^3) = 624$. If we take $k = 5$, then we have $ks = 3120$ and

$$\{5, 25, 125, 625, 2495, 2995, 3095, 3115\}$$

is a group under multiplication modulo ks = 5(624) = 3120. Its identity element is 625, and its Cayley table is as in Table 8.

×	5	25	125	625	2495	2995	3095	3115
5	25	125	625	5	3115	2495	2995	3095
25	125	625	5	25	3095	3115	2495	2995
125	625	5	25	125	2995	3095	3115	2495
625	5	25	125	625	2495	2995	3095	3115
2495	3115	3095	2995	2495	625	125	25	5
2995	2495	3115	3095	2995	125	25	5	625
3095	2995	2495	3115	3095	25	5	625	125
3115	3095	2995	2495	3115	5	625	125	25

Table 8. Multiplicative group modulo 3120

Hidayah and Purwanto [5] also find other constructions of groups in modular arithmetic by generate the elements of group using $-n$ instead of n, n > 1.

Theorem 2.5 (Hidayah and Purwanto). *Let n, d, and q be positive integers,* $n > 1$*,* $q > 1$*, d divide* $n + 1$*, and* $s = d(n^{q-1} - n^{q-2} + n^{q-3} - \cdots + (-1)^{q-1})$*. Ifk* $\equiv (-n)^i$ mod s*for some integer* $i > 1$*, then the set* $\{k,\ k(-n), k(-n)^2, \ldots, k(-n)^{q-1}\}$ *forms a group under multiplication* mod ks*. Its identity element is ewhere* $e \equiv 1$ mod s*.* []

For example, in Theorem 2.5, let n = 2and q = 4. Then we can have d = 1 or 3, and $s = 1(2^3 - 2^2 + 2 - 1) = 5$or $s = 3(2^3 - 2^2 + 2 - 1) = 15$, respectively. When we take s = 15 and $k = 4 \equiv (-2)^2$ mod 15, then ks = 60 and we find a set $\{4, -8, 16, -32\} \equiv \{4, 52, 16, 28\} \equiv \{4, 16, 28, 52\}$ is a group under multiplication mod 60 the identity element 16, since 15 ≡ 1 mod 16. Its Cayley table is as in Table 9.

×	4	16	28	52
4	16	4	52	28
16	4	16	28	52
28	52	28	4	16
52	28	52	16	4

Table 9. Multilpicative group modulo 60

By using Theorem 2.5 and Remark 2.4, we have the following theorem.

Theorem 2.6 (Hidayah and Purwanto). *Let n, d, and q be positive integers,* $n > 1$, $q > 1$, *d divide* $n + 1$, *and* $s = d(n^{q-1} - n^{q-2} + n^{q-3} - \cdots + (-1)^{q-1})$. *If* $k \equiv (-n)^i \bmod s$ *for some integer* $i > 1$, *then the set* $\{h |\, h = k(-n)^j \text{ or } h = ks - k(-n)^j,\ j = 0, 1, 2, \dots, q - 1\}$ *forms a group under multiplication* mod ks. *Its identity element is e where* $e \equiv 1 \bmod s$.

For example, in Theorem 2.6, let $n = 2$and $q = 4$. Then we can have $d = 1$ or 3, and $s = 1(2^3 - 2^2 + 2 - 1) = 5$or $s = 3(2^3 - 2^2 + 2 - 1) = 15$, respectively. When we take $s = 15$, and $k = 4 \equiv (-2)^2 \bmod 15$, then $ks = 60$ and we find a set

$$\{4, -8, 16, -32, 56, 68, 44, 92\} \equiv \{4, 52, 16, 28, 56, 8, 44, 32\} \equiv \{4, 8, 16, 28, 32, 44, 52, 56\}$$

is a group under multiplication mod 60 the identity element 16, since $15 \equiv 1 \bmod 16$. Its Cayley table is as in Table 10.

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

Table 10. Multiplicative group modulo 60

3. Problems

The constructions of the groups we just discussed are very useful when we begin to study about group; the constructions provide examples of multiplicative group in modular arithmetic in which the identity element is not necessarily 1. The constructions start with geometric series.

Are there any other different construction, from the above construction, of such groups? I think so; for example, the following two groups should be constructed by a new way. First,

$\{1, 17, 31, 47\}$ is a group under multiplication modulo 48, and its Cayley table is as in Table 11

×	1	17	31	47
1	1	17	31	47
17	17	1	47	31
31	31	47	1	17
47	47	31	17	1

Table 11. Multiplicative group modulo 48

Second, $\{7, 49, 41\}$ is a group under multiplication modulo 126, and its Cayley table is as in Table 12.

×	7	49	91
7	49	91	7
49	91	7	49
91	7	49	91

Table 12. Multiplicative group modulo 126

We still have the following problem.

Problem 3.1. Find new constructions of multiplication groups in modular arithmetic in which the identity element is not necessarily 1.

Conclusion

Groups occur in modular arithmetic, and many authors have studied multiplicative these groups. Many multiplicative groups in modular arithmetic each of which has an identity element which is not necessarily 1 have been constructed. Problem to find new constructions of multiplication groups in modular arithmetic is still open.

References

[1] Gallian JA, Contemporary Abstract Algebra 8th Ed, Bellmont: Brooks/Cole, 2013

[2] McLean KR, Groups in Modular Arithmetic. Math.Gaz. 62 No.420, 1978, 94-104

[3] Denniss J, Modular Group Revisited Math. Gaz. 63 No.424, 1979, 121-123

[4] Brakes W R, Unexpected Groups Math. Gaz. 79 No.486, 1995, 513-520

[5] Hidayah I N and Purwanto. Constructing Multiplicative Groups In Modular Arithmetic. Far East Journal of Mathematical SciencesVol 99 No.4, 2016, 569-576

[6] Hidayah I N and Purwanto. Minimum Number of Vertices of Graphs without Perfect Matching with Given Edge Connectivity and Minimum and Maximum Degrees. *J. Combin. Math. Combin. Comput*. 88 (2014), 191-198