Far East Journal of Mathematical Sciences (FJMS)

Published Online: January 2016
http://dx.doi.org/10.17654/MS099040569
Volume 99, Number 4, 2016, Pages 569-576 **ISSN: 0972-0871**

CONSTRUCTING MULTIPLICATIVE GROUPS IN MODULAR ARITHMETIC

Indriati Nurul Hidayah and Purwanto

Department of Mathematics
Universitas Negeri Malang
Jl. Semarang 5, Malang, 65145, Indonesia
e-mail: indriati.nurul.fmipa@um.ac.id
purwanto.fmipa@um.ac.id

Abstract

It is known that multiplicative groups occur in modular arithmetic. Many authors have studied these groups. Denniss constructed groups in modular arithmetic *G* under multiplication modulo *m* each of which has an identity element which is not necessarily 1, for some value of *m*. We find other possible values of *m* and a set $H \supseteq G$ such that *H* and *G* are also groups under multiplication modulo *m*. Further, we also find other multiplicative groups in modular arithmetic.

1. Introduction

For the most part of our notation and terminology, we follow that of Gallian [3]. Thus, the set $\{0, 1, 2, ..., n-1\}$, $n \geq 1$, is denoted by Z_n. The set Z_n is a group under addition modulo *n*. The set of all positive integers less than *n* and relative prime to *n*, $U_n = \{a \in Z_n \mid (a, n) = 1\}$, is a group

Received: July 7, 2015; Revised: September 25, 2015; Accepted: November 23, 2015
2010 Mathematics Subject Classification: 20N99, 20K77.
Keywords and phrases: group, modular arithmetic, multiplicative.
Communicated by K. K. Azad

under multiplication modulo n, the identity element is being 1. In [3, p. 52], we can see that $G = \{5, 15, 25, 35\}$ is a group under multiplication modulo 40. We can show that it is a group by constructing its Cayley table, and we can see that its identity element is 25. In this paper, we find further examples of multiplicative groups modulo n.

Many authors, for example, McLean [4], Denniss [2] and Brakes [1] have studied multiplicative groups in modular arithmetic. Denniss constructed 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. The Denniss' Theorem is as follows.

Theorem (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 $\{k, kn, kn^2, ..., kn^{q-1}\}$ forms a group under multiplication $\bmod(k + kn + kn^2 + \cdots + kn^{q-1})$.*

In this theorem, let $m = k + kn + kn^2 + \cdots + kn^{q-1}$. In this paper, we 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. We also find a set $H \supseteq G$ such that H is a group under multiplication modulo m. Further, we find other multiplicative groups in modular arithmetic. Thus, we can find further examples of groups in modular arithmetic.

2. Constructions

To derive our results, we use McLean's criterion [4], which says that if $G = \{e, a, b, ...\} (\bmod n)$ is a multiplicative group, then $H = \{ke, ka, kb, ...\} (\bmod kn)$ is a multiplicative group if and only if $ke \in G$.

Our first result is as follows.

Theorem 2.1. *Let* n, d *and* q *be positive integers*, $n > 1$, $q > 1$, *where* d *divides* $n - 1$, *and* $s = \frac{n^q - 1}{d}$. *If* $k \equiv n^i \bmod s$ *for some integer* $i \geq 0$, *then the set* $\{k, kn, kn^2, \ldots, kn^{q-1}\}$ *forms a group under multiplication* $\bmod ks$. *Its identity element is* e, *where* $e \equiv 1 \bmod s$.

Proof. Since $n^q - 1 = (n-1)(1 + n + n^2 + \cdots + n^{q-1})$ and d divides $n - 1$,

$$s = \frac{n^q - 1}{d} = \frac{n-1}{d}(1 + n + n^2 + \cdots + n^{q-1})$$

is an integer, and

$$n^q - 1 \equiv d\,\frac{n^q - 1}{d} = ds,$$

$$n^q \equiv 1 \bmod s,$$

and so the set

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

forms a group under multiplication mod s. The identity element is 1, and for any t, $0 \leq t \leq q - 1$, $(n^t)^{-1} = n^{q-t}$. By using McLean's criterion, the set

$$G = \{k, kn, kn^2, \ldots, kn^{q-1}\}$$

forms a group under multiplication $\bmod ks$ when $k \equiv n^i \bmod s$ for some integer $i \geq 0$.

We show that there exists an identity element $e \in G$, where $e \equiv n^q \equiv 1 \bmod s$. Let $kn^t \in G$. Since $k \equiv n^i \bmod s$, $G = \{n^i, n^{i+1}, \ldots, n^{i+q-1}\} (\bmod s)$, and there exists $n^{uq} \equiv e \bmod s$, $e \in G$, for some nonnegative integer u. Since $n^q \equiv 1 \bmod s$, $n^{uq} \equiv 1 \bmod s$, $n^{uq} - 1 = ls$, for some positive integer l. Hence we have

$$n^{uq}kn^t - kn^t = (n^{uq} - 1)kn^t = lskn^t,$$

$$n^{uq} kn^t \equiv kn^t \bmod ks,$$

and so the identity element is e, where $e \equiv n^{uq} \equiv n^q \equiv 1 \bmod s$. □

Note that, in Theorem 2.1, when $d = n - 1$, then $s = 1 + n + n^2 + \cdots + n^{q-1}$ and we have Denniss' Theorem.

For example, in Theorem 2.1, let $n = 3$ and $q = 4$. Then we can have $d = 1$ or 2, and $s = 80$ or 40, respectively. When we take $d = 2$, $s = 40$, and $k = 1 \equiv 1 \bmod 40$ (or by Dennis' Theorem), then the set $\{1, 3, 9, 27\}$ is a group under multiplication $\bmod 40$ with the identity element 1. When we take $d = 1$, $s = 80$, and $k = 1 \equiv 1 \bmod 80$, then the set $\{1, 3, 9, 27\}$ is a group under multiplication $\bmod 80$ with the identity element 1. When we take $d = 1$, $s = 80$, and $k = 30003 \equiv 3 \bmod 80$, then the set $\{30003, 90009, 270027, 810081\}$ is a group under multiplication $\bmod 2400240$ with the identity element 810081, since $810081 \equiv 1 \bmod 80$.

From Theorem 2.1, if we take $q = j + 1$ and $k = n^i$, then we have the following corollary.

Corollary 2.2. *Let n and d be positive integers where d divides $n - 1$. Then, for any nonnegative integers i and j, the set $\{n^i, n^{i+1}, ..., n^{i+j}\}$ is a group under multiplication $\bmod \frac{n^{j+1} - 1}{d} n^i$. Its identity element is e, where*

$$e \equiv n^{j+1} \equiv 1 \bmod \frac{n^{j+1} - 1}{d}.$$

Now we give a set $H \supseteq \{k, kn, kn^2, ..., kn^{q-1}\}$ such that H is also a group under multiplication modulo $m = k + kn + kn^2 + \cdots + kn^{q-1}$.

Theorem 2.3. *Let n, d and q be positive integers, $n > 1$, $q > 1$, where d divides $n - 1$, and $s = \frac{n^q - 1}{d}$. If $k \equiv n^i \bmod s$ or $k \equiv s - n^i \bmod s$ for some integer $i \geq 0$, then the set $\{h \mid h = kn^j$ or $h = k(s - n^j)$, $j = 0, 1,$*

..., $q-1\}$ *forms a group under multiplication* mod ks. *Its identity element is* e, *where* $e \equiv 1 \bmod s$.

Proof. First, we show that

$$G = \{g \mid g = n^j \text{ or } h = s - n^j,\ j = 0, 1, ..., q-1\}$$

forms a group under multiplication $\bmod s$. As in the proof of Theorem 2.1, since $n^q - 1 = (n-1)(1 + n + n^2 + \cdots + n^{q-1})$ and d divides $n-1$,

$$s = \frac{n^q - 1}{d} = \frac{n-1}{d}(1 + n + n^2 + \cdots + n^{q-1})$$

is an integer, and

$$n^q - 1 = d\,\frac{n^q - 1}{d} = ds,$$

$$n^q \equiv 1 \bmod s.$$

Let $g_1, g_2 \in G$. We apply multiplication $\bmod s$. If $g_1, g_2 \in \{1, n, n^2, ..., n^{q-1}\}$, then $g_1g_2 \in \{1, n, n^2, ..., n^{q-1}\} \subseteq G$. If $g_1, g_2 \in \{s-1, s-n, s-n^2, ..., s-n^{q-1}\}$, then $g_1 = s - n^t$ and $g_2 = s - n^u$ for some integers t and u, $0 \le t, u \le q-1$. We have $g_1g_2 = (s-n^t)(s-n^u) \equiv n^{t+u} \bmod s$, and, when it is reduced to $\bmod s$, $g_1g_2 \in \{1, n, n^2, ..., n^{q-1}\} \subseteq G$. Without loss of generality, let $g_1 \in \{1, n, n^2, ..., n^{q-1}\}$ and $g_2 \in \{s-1, s-n, s-n^2, ..., s-n^{q-1}\}$. Then $g_1 = n^t$ and $g_2 = s - n^u$ for some positive integers t and u, $0 \le t, u \le q-1$. We have $g_1g_2 = n^t(s-n^u) \equiv -n^{t+u} \equiv s - n^{t+u} \bmod s$, and, when it is reduced to $\bmod s$, $g_1g_2 \in \{s-1, s-n, s-n^2, ..., s-n^{q-1}\} \subseteq G$. These prove that, if $g_1, g_2 \in G$, then $g_1g_2 \in G$. The identity element is 1. For any integer t, $0 \le t \le q-1$, $(n^t)^{-1} = n^{q-t}$, and $(s-n^t)^{-1} = s - n^{q-t}$. This completes the proof that G forms a group under multiplication mod s.

By using McLean's criterion, the set

$$\{h \mid h = kn^j \text{ or } h = k(s - n^j),\ j = 0, 1, ..., q - 1\}$$

forms a group under multiplication $\bmod ks$, when $k \equiv n^i \bmod s$ or $k \equiv s - n^i \bmod s$ for some integer $i \geq 0$. As in the proof of Theorem 2.1, the identity element is e, where $e \equiv 1 \bmod s$. □

Remark. The following fact can also be proved, as in the proof of Theorem 2.3. If G is a group under multiplication $\bmod m$ with the identity element e, then the set $H = \{h \mid h = g \text{ or } h = m - g \text{ for some } g \in G\}$ is also a group under multiplication $\bmod m$ with identity element e.

For example, in Theorem 2.3, let $n = 3$ and $q = 3$. Then we can have $d = 1$ or 2, and $s = 26$ or 13, respectively. If we take $d = 1$, $s = 26$, and $k = 1 \equiv 1 \bmod 26$, then the set $\{1, 3, 9, 17, 23, 25\}$ is a group under multiplication $\bmod 26$ with the identity element 1. If we take $d = 2$, $s = 13$, and $k = 25 \equiv 13 - 3^0 \bmod 13$, then the set $\{25, 75, 100, 225, 250, 300\}$ is a group under multiplication $\bmod 325$ with the identity element 300, since $300 \equiv 1 \bmod 13$.

From Theorem 2.3, if we take $q = j + 1$ and $k = n^i$, then we have the following corollary.

Corollary 2.4. *Let n and d be positive integers, $n > 1$, and d divides $n - 1$. Then, for any nonnegative integers i and j, and $s = \frac{n^{j+1} - 1}{d}$, the set $\{h \mid h = n^{i+l} \text{ or } h = n^i(s - n^l), l = 0, 1, ..., j\}$ is a group under multiplication $\bmod n^i s$. Its identity element is e, where $e \equiv n^{j+1} \equiv 1 \bmod s$.*

Now we give other multiplicative groups in modular arithmetic. Let n, d and q be positive integers, $n > 1$, $q > 1$, where d divides $n + 1$. When q is odd, we have

$$n^q + 1 = (n+1)(n^{q-1} - n^{q-2} + n^{q-3} - \cdots + 1).$$

Let

$$s = \frac{n^q + 1}{d} = \frac{n+1}{d}(n^{q-1} - n^{q-2} + n^{q-3} - \cdots + 1).$$

Then s is an integer, and

$$n^q + 1 \equiv d\,\frac{n^q + 1}{d} = ds,$$

$$-n^q \equiv 1 \bmod s.$$

Similarly, when q is even, and

$$s = \frac{n^q - 1}{d} = \frac{n+1}{d}(n^{q-1} - n^{q-2} + n^{q-3} - \cdots - 1),$$

we have

$$n^q \equiv 1 \bmod s.$$

By the same argument as in the proof of Theorem 2.1, we have

$$\{h \,|\, h = (-n)^i,\ i = 0, 1, \ldots, q-1\}$$

is a group under multiplication modulo s. By using McLean's criterion, we find the following theorem.

Theorem 2.5. *Let* n, d *and* q *be positive integers*, $n > 1$, $q > 1$, *where* d *divides* $n+1$, *and* $s = \frac{n^q - (-1)^q}{d}$. *If* k *is a positive integer and* $k \equiv (-n)^i \bmod s$, *for some integer* $i \geq 0$, *then the set* $\{h \,|\, h = k(-n)^j,\ j = 0, 1, \ldots, q-1\}$ *forms a group under multiplication* mod ks. *Its identity element is* e, *where* $e \equiv 1 \bmod s$.

For example, in Theorem 2.5, let $n = 2$ and $q = 3$. Then we can have $d = 1$ or 3, and $s = 9$ or 3, respectively. When we take $d = 1$, $s = 9$, and

$k = 4 \equiv (-2)^2 \bmod 9,$ then we find the set $\{1, -2, 4\} = \{1, 7, 4\} \bmod 9.$ Hence, the set $\{4, 16, 28\}$ is a group under multiplication $\bmod 36$ with the identity element 28, since $28 \equiv 1 \bmod 9.$

By using Theorem 2.5 and the fact in the remark, we have the following theorem.

Theorem 2.6. *Let n, d and q be positive integers,* $n > 1,$ $q > 1,$ *where d divides* $n + 1,$ *and* $s = \dfrac{n^q - (-1)^q}{d}.$ *If k is a positive integer and* $k \equiv (-n)^i \bmod s$ *or* $k \equiv s - (-n)^i \bmod s$ *for some integer* $i \geq 0,$ *then the set* $\{h \mid h = k(-n)^j \text{ or } h = k(s - (-n)^j),\ j = 0, 1, \ldots, q-1\}$ *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 $n = 3$ and $q = 3.$ Then we can have $d = 1,$ 2 or 4, and $s = 28,$ 14 or 7, respectively. When we take $d = 1,$ $s = 28,$ and $k = 1 \equiv 1 \bmod 28,$ then we find the set $\{1, -3, 9, 27, 31, 19\} = \{1, 25, 9, 27, 3, 19\} \bmod 28,$ and so the set $\{1, 3, 9, 19, 25, 27\}$ is a group under multiplication mod 28 with the identity 1.

Acknowledgments

The authors would like to thank the referees for their suggestions and the Directorate General of Higher Education of Republic of Indonesia for the support.

References

[1] W. R. Brakes, Unexpected groups, Math. Gaz. 79(486) (1995), 513-520.

[2] John Denniss, Modular group revisited, Math. Gaz. 63(424) (1979), 121-123.

[3] Joseph A. Gallian, Contemporary Abstract Algebra, 7th ed., Brooks/Cole, Bellmont, 2010.

[4] K. Robin McLean, Groups in Modular Arithmetic, Math. Gaz. 62(420) (1978), 94-104.