Journal of Physical Mathematics
ISSN: 2090-0902
Adeniji and Mogbonju, J Phys Math 2019, 10:1
DOI: 10.4172/2090-0902.1000300
Short Communication
Open Access

Generating Tuples of Integers Modulo n

Adeniji AO* and Mogbonju MM
Department of Mathematics, Faculty of Science, University of Abuja, Abuja, Nigeria

Abstract

In this paper, $Z_p^+ \cong Z_p^{p-2}$ for n ≥ 3, where p=2n-1 and Z^{p-1}_p=e (e is the multiplicative identity). The diagonal elements of Z^+_{2n+1} can generate Z^{2k-2}_{2n-1}; k=2, 3,… n-1 by simple algorithm.

Keywords: Integers modulo n; Generator; Isomorphism; Co-prime

Introduction

Given a positive integer n, the set of integers between 1 and n have been studied over the years, yielding interesting viable results. For instance, integers that are co-prime with n forming a group with multiplication modulo n as the operation, denoted by Z^*_n is called the multiplicative group of integers modulo n [1-5].

It is shown in a study [4] that, if Z^*_n is the multiplicative group of integers modulo n that does not possess any primitive roots, then Z*n has a semi-primitive root if and only if n is equal to 2^k(k>2); $4P^{k1}_1$; $P^{k1}_1 P^{k2}_2$ or $2P^{k1}_1 P^{k2}_2$, where P_1 and P_2 are odd prime numbers satisfying ($\phi(P^{k1}_1)$ ϕ (P^{k2}_2))=2: Semi-primitive roots are used in a study [5] to solve certain congruence's.

In this paper, we study the characteristics of multiplicity of multiplicative groups of integers modulo n.

For any positive integer n, the Euler Phi-function represents the number of positive integers not exceeding n that are coprime to n, where by convention $\phi(1)$=1: For example, ϕ (16)=8; since 1,3, 5, 7, 9, 11, 13 and 15 are the only integers that are positive, less than 16 and coprime to 16 [3].

Euler's theorem states that $a^{\phi(n)} \equiv 1 mod(n)$, for any integer a coprime to n, where $\phi(n)$ is the Euler phi-function [1], that is, the number of elements in Z^*_n and a is said to be a primitive root modulo n if the order of a modulo n is equal to $\phi(n)$ [4].

Monogenic Subset of Integers Modulo n

Monogenic subset of a set of integers modulo n follows the notion of monogenic semi group [2]. Let Z_n be a set of integers modulo n and consider monogenic subset of $Z_n, \langle Z_n \rangle = \{Z_n, Z_n^2, Z_n^3, ...\}$ generated by Zn.

If there are no repetitions in the list Z_n, Z^2_n, Z^3_n… that is, $Z_n^t = Z_n^s \Rightarrow t = s$, then evidently $(\langle Z_n \rangle, .)$ is isomorphic to the set (N,+) of natural numbers with respect to addition. Then Z_n is an infinite monogenic set and it has infinite order. Suppose that there are repetitions among the powers of Z_n. Then the set, $\{a \in N : (\exists b \in N) Z_n^b a \neq b\}$ is non-empty and so has a least element. If we denote this least element by m and call it the index of the set Z_n: Then the set {a∊N: $Z^{m+a}_n = Z^m_n$} is non-empty and so it too has a least element r, which we call the period of Z_n. So, m and r are referred to as the index and period respectively. Let Z_n be a set with index m and period r. Thus

$$Z^m_n = Z^{m+r}_n.$$

It follows that

$$Z^m_n = Z^{m+r}_n = Z^m_n Z_n^r = Z^{m+r}_n Z^r_n = Zm+2rn$$

and more generally, that

$$(\forall q \in N) Z_n^m = Z_n^{m+qr}.$$

Diagonal Generators of Z_p^{2n-2}

Theorem 1

Let the diagonals of Z_p be defined say, D={a_1, a_2,… a_k, …} where P=2n-1, n>1. Then Z_p^{2n-2} is obtained from D,D-a_1,D-(a_1+a_2),…D-(a_1+a_2 +…. A_{k-1}).

Proof: Algorithm for computing Z_p^{2n-2} is in steps as follows:

Task: Compute each row of Z_p^{2n-2}, n>1;

Declare variables of diagonal elements of Z_p;

List D

Then skip a variable in D

Do until a_k back to a_1 skip no variable

Do until row is filled

Repeat process till nth row is filled with equivalent skips of (n-1) variables from D.

Stop.

Theorem 2

$Z_p = Z_p^p$

Proof: The index of Z_p is 1 while the period is p-1:

Theorem 3

The order of Z_p is p-1, n>1.

Proof: Let $a_1, a_2, a_3, ... \in Z_p, \exists k \in P$ such that $a_1^k = a_2^k = a_3^k = \ldots = 1$. Suppose that k=p, then $Z_p^p = Z_p$ from theorem 2. If k=p+1, then $Z_p^{p+1} = Z_p^2$, if k=p+2, then Zp+2p=Z_p^3. Iteratively, if k=p-1 then $Z_p^{p-1} = Z_p^0 = 1$(equivalently the identity). Hence, p-1 is the order of Z_p:

***Corresponding author:** Adeniji AO, Department of Mathematics, Faculty of Science, University of Abuja, Abuja, Nigeria, Tel: +234 818 6889912; E-mail: adeniji4love@yahoo.com

Received March 19, 2018; **Accepted** April 26, 2019; **Published** May 03, 2019

Citation: Adeniji AO, Mogbonju MM (2019) Generating Tuples of Integers Modulo n. J Phys Math 10: 300. doi: 10.4172/2090-0902.1000300

Citation: Adeniji AO, Mogbonju MM (2019) Generating Tuples of Integers Modulo n. J Phys Math 10: 300. doi: 10.4172/2090-0902.1000300

Theorem 4

The inverse of Z_p is Z_p^{p-2}.

Proof: The order of an element x in a group implies the existence of n∊ Z+ such that a^n=e, the identity element. Following the iteration process in theorem 3, $Z_p^{p-2}=Z_p^{-1}$ implying that the inverse of Z_p is Zp-2p.

Theorem 5

$Z_p \cong Z_p^{p-2}$.

Proof: Since Z_p is invertible for p=2n-1, n>1, then using Euler-phi function, $\phi(Z_p)=\phi(Z_p^k)$.

Let $k \equiv p, Z_p \neq Z_p^k$. If k=±1, $Z_p \neq Z_p^k$.

$Z_p \cong Z_p^{k_1}$ only at k_1=p-2.

For each a ∊ Z_p, b∊ Z_p^{k1} then $a \leftrightarrow b$. Hence $\phi(Z_p)=\phi(Z_p k1)$ if and only if $Z_p=Z^{k1}_p$.

Theorem 6

$\left\langle Z_{2n-1}^{+}, . \right\rangle$ is a group.

Proof: Let $p = 2n-1, \forall n \in N$. Existence of identity is visible in Z_p^{p-1}. For any q<p-1, q+p-1(modp)=p-1, which is the index of Z_p giving the identity of $\left\langle Z_p, . \right\rangle$. Thus, Z_p^q is the inverse of Z_p^n, where q+n=p-1. Also, the order of $\left\langle Z_p^r, . \right\rangle$ is p-1.

Let a, b, c 2 Z+ p, then

[(a.b).c](modp)=[(a(modp).b(modp)).c(modp)]

=[(a(modp)).(b(modp).c(modp))]=[a(modp).(b.c)(modp)]

=[a.(b.c)](modp).

References

1. Abramowitz M, Stegunl IA (1994) Handbook of Mathematical Functions. Dover Publication, New York, USA.
2. Howie JM (1995) Fundamentals of Semi group Theory. Clarendon Press Oxford.
3. James JT (2005) Elementary Number Theory in Nine Chapters. Cambridge University Press New York.
4. Lee K, Kwon M, Kang MK, Shin G (2011) Semi-primitive Root Modulo n. Honam Math J 33: 181-186.
5. Lee K, Kwon M, Shin G (2013) Multiplicative Groups of Integers with Semi-Primitive Roots Modulo n. Commun Korean Math Soc 28: 71-77.