The inverse of primitive root in $\mathbb{Z}^*_{kp}$

Abstract

In 2023, V.P. Ramesh and R. Gowtham published a research proving that *let p be an odd prime, if $a \in \mathbb{Z}_p^2$ is a bad primitive root, i.e., $ord_p(a) = ord_{kp}(a) = \phi(p) = p-1$, then $a^{-1} \in \mathbb{Z}_p^*$ dose not need to be a bad primitive root.* In this independent study, we use the same argrument to study the behavior of the inverse of a in $\mathbb{Z}_{kp}^*$. We prove that *let p be an odd prime, and a be a primitive root of p in $\mathbb{Z}_p^*$. Suppose $ord_p(a) = ord_{kp}(a) = \phi(p) = p-1$, if a^{-1} be the inverse of a in $\mathbb{Z}_p^*$, where $ord_p(a^{-1}) = p-1$ then $ord_{kp}(a^{-1})$ dose not to be $p-1$, $k = 2, 3$.*

Preliminaries

Congruent modulo n

Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. We say that a and b are *congruence modulo n* if $n \mid (a-b)$, denote by $a \equiv b \pmod{n}$.

Group

Let $G \neq \varnothing$ with a binary operation $*$ that G has three requirements satisfied:

1. Associativity: $a * (b * c) = (a * b) * c$ for all elements $a, b, c \in G$.
2. Identity: there is an element $e \in G$ in which $a * e = e * a = a$ for all element of G. We usually denote the identity for groups under multiplications by 1, under addition by 0.
3. Inverse: For every element $a \in G$, there is the inverse of a (let's say b) that satisfies $a * b = b * a = e$.
   We call the pair $(G, *)$ a group.

Order of integer

let n in $\mathbb{Z}^+$, $a \in \mathbb{N}$ where $\gcd(a, n) = 1$, if x be the least positive integer such that $a^x \equiv 1 \pmod{n}$, we call x is order of a modulo n, denote by $x = \text{ord}_n(a)$.

Euler's phi function

let $n \in \mathbb{N}$, $\phi(n)$ is number of positive integer $k \leq n$ and $\gcd(k, n) = 1$, we call $\phi(n)$ is *euler's phi function*.

Important properties of $\phi(n)$

1. If p is prime, then $\phi(p) = p - 1$.
2. For $n \in \mathbb{N}$, if $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, then $\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$

Primitive root of n

Let n be a positive integer, $a \in \mathbb{N}$, if $\text{ord}_n(a) = \phi(n)$, we call a is primitive root of n

Conclusion

From the study of the research paper *The Inverse of Bad Primitive Root is Not Bad* which investigates the inverse elements of primitive roots in p^2 this independent study extends the exploration to the inverse elements of primitive roots in kp . Specifically, we examine the cases where $k = 2, 3$ and obtain the following main theorem:

Let p be an odd prime and a be a primitive root of p in $\mathbb{Z}_p^*$, if a^{-1} be the inverse of a in $\mathbb{Z}_p^*$ where $ord_p(a^{-1}) = p-1$ then $ord_{kp}(a^{-1})$ does not equal to $p-1$, $k = 2, 3$

In proving the main theorem, we find that if b is the inverse element of a in $\mathbb{Z}_{kp}^*$, then $b \neq a^{-1}$. Specifically, for $k = 2$, we obtain $b = a^{-1} + p$, and for $k = 3$, we find $b = a^{-1} + mp$, $0 < m < p-1$. The condition $b \neq a^{-1}$ is necessary for the validity of the main theorem, as demonstrated in Example 3.5. In the case where $p = 7$, no primitive root satisfies the conditions of our main theorem.

Scope

This study examines relevant research on the inverse of of primitive root in p^2 to apply the knowledge and theories from the selected topics to formulate hypotheses and theorems of interest. The formulated hypotheses and theorems will then be proved.

Objective

1. To study the inverse of primitive root of kp
2. To prove our main theorem stating that *if a^{-1} be the inverse of a in $\mathbb{Z}_p^*$ where $ord_p(a^{-1}) = ord_{kp}(a) = ord_p(a^{-1})$ then $ord_{kp}(a^{-1})$ dose not equal to $p-1$ when $k = 2, 3$.*

Result

Lemma 3.2

Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}_n^*$, if a^{-1} be the inverse of a in $\mathbb{Z}_n^*$ then $\text{ord}_n(a^{-1}) = \text{ord}_n(a)$

Theorem 3.3

Let p be an odd prime and a be a primitive root of p in $\mathbb{Z}_p^*$, if a^{-1} be the inverse of a in $\mathbb{Z}_p^*$ where $\text{ord}_p(a^{-1}) = p-1$ then $\text{ord}_{kp}(a^{-1})$ does not equal to $p-1$, $k = 2, 3$

Table 1 : Order of a and a^{-1} in $\mathbb{Z}_p^*$ anf $\mathbb{Z}_{2p}^*$

p	a	a^{-1}	b	$ord_p(a)$	$ord_{2p}(a)$	$ord_p(a^{-1})$	$ord_{2p}(a^{-1})$
5	2	3	-	4	≠4	4	4
	3	2	7	4	4	4	≠4
7	3	5	5	6	6	6	6
	5	3	3	6	6	6	6
11	2	6	-	10	≠10	10	≠10
	6	2	-	10	≠10	10	≠10
	7	8	19	10	10	10	≠10
	8	7	-	10	≠10	10	10

Note that : In case p = 5 , a = 3 and p = 11, a = 7 are satisfy the conthetions for our theorem

Table 1 : Order of a and a^{-1} in $\mathbb{Z}_p^*$ anf $\mathbb{Z}_{3p}^*$

p	a	a^{-1}	b	$ord_p(a)$	$ord_{3p}(a)$	$ord_p(a^{-1})$	$ord_{3p}(a^{-1})$
5	2	3	8	4	4	4	≠4
	3	2	-	4	≠4	4	4
7	3	5	-	6	≠6	6	≠6
	5	3	17	6	≠6	6	≠6
11	2	6	17	10	10	10	≠10
	6	2	-	10	≠10	10	10
	7	8	19	10	10	10	≠10
	8	7	-	10	≠10	10	10

Note that : In case p = 5 , a = 2 and p = 11, a = 2,7 are satisfy the conthetions for our theorem

Chaichana Pasawat Student ID : 640510520

Assistant Professor Dr. Supaluk Phothi

Department of Mathematics, Faculty of Science, Chiang Mai University