Suppose F Belongs To Aut(zn) And A Is Relatively Prime To N. If F(a) 5 B, Determine A Formula For F(x).

Suppose F Belongs To Aut(zn) And A Is Relatively Prime To N. If F(a) = B, Determine A Formula For F(x).

Understanding the structure of automorphisms in the group $\mathbb{Z}_n$ and how they act on elements is a fundamental topic in algebra, especially in the study of cyclic groups. When given that F is an automorphism in $\text{Aut}(\mathbb{Z}_n)$, and that A is an element relatively prime to N, with the condition $F(a) = B$, the question arises: how can we explicitly determine the formula for $F(x)$? This article explores the theoretical background, provides step-by-step derivations, and offers concrete formulas to understand and compute automorphisms of $\mathbb{Z}_n$, especially when specific mappings are given.

Understanding Automorphisms of $\mathbb{Z}_n$

What is $\text{Aut}(\mathbb{Z}_n)$?

- $\text{Aut}(\mathbb{Z}_n)$ is the group of all automorphisms (structure-preserving bijections) from $\mathbb{Z}_n$ to itself.
- Since $\mathbb{Z}_n$ is cyclic, generated by 1, every automorphism is determined entirely by the image of 1.
- The automorphisms correspond to elements k in $\mathbb{Z}_n$ where multiplication by k mod n is a bijection.

Key Properties of $\text{Aut}(\mathbb{Z}_n)$

- The automorphism group $\text{Aut}(\mathbb{Z}_n)$ is isomorphic to the group of units $\mathbb{Z}_n^$, i.e., the set of integers modulo n that are relatively prime to n with multiplication as the operation.
- Therefore, each automorphism F can be associated with an element $k \in \mathbb{Z}_n^$, and acts as:

$$
F(x) = kx \quad (\text{mod } n)
$$

Given Conditions and Their Implications

Given: $F \in \text{Aut}(\mathbb{Z}_n)$ and $A \in \mathbb{Z}_n$ with $\gcd(A, n) = 1$

- Because A is relatively prime to n, A is a unit in $\mathbb{Z}_n$.
- The automorphism F is determined by a unit k such that $F(x) = kx \ (\text{mod } n)$.

Given: $F(a) = B$

- This condition helps identify the specific automorphism F, i.e., find k such that:

$$
F(a) = k a \equiv B \ (\text{mod } n)
$$

- Since a is relatively prime to n, it has a multiplicative inverse modulo n, denoted a^{-1}.

Deriving the Formula for $F(x)$

Step 1: Find the automorphism's defining parameter k

- From the condition:

$$
k a \equiv B \ (\text{mod } n)
$$

- Since $\gcd(a, n) = 1$, a has an inverse a^{-1} in $\mathbb{Z}_n$, satisfying:

$$
a a^{-1} \equiv 1 \ (\text{mod } n)
$$

- Multiply both sides of the previous congruence by a^{-1}:

$$
k a a^{-1} \equiv B a^{-1} \ (\text{mod } n)
\implies k \equiv B a^{-1} \ (\text{mod } n)
$$

- Therefore, the automorphism F is determined by:

$$
F(x) = k x \equiv (B a^{-1}) x \ (\text{mod } n)
$$

Step 2: Express the automorphism explicitly

- The formula for $F(x)$ becomes:

$$
\boxed{
F(x) \equiv (B \cdot a^{-1}) x \ (\text{mod } n)
}
$$

- Here, a^{-1} is the multiplicative inverse of a modulo n, which exists because $\gcd(a, n) = 1$.

Step 3: Computing a^{-1} in practice

- To find a^{-1} modulo n, use the Extended Euclidean Algorithm, which provides integers x, y such that:

$$
a x + n y = 1
$$

- The value of x modulo n is the multiplicative inverse a^{-1}.

Summary of the Formula for $F(x)$

- The automorphism $F: \mathbb{Z}_n \to \mathbb{Z}_n$ satisfying $F(a) = B$ where $\gcd(a, n) = 1$, is given by:

$$
\boxed{
F(x) \equiv (B \cdot a^{-1}) x \ (\text{mod } n)
}
$$

- This formula explicitly describes how F acts on any element $x \in \mathbb{Z}_n$.

Practical Steps to Find $F(x)$ in Specific Cases

Step 1: Verify $\gcd(a, n) = 1$

- Ensure that a and n are coprime; otherwise, the inverse a^{-1} does not exist.

Step 2: Compute a^{-1} modulo n

- Use the Extended Euclidean Algorithm to find integers x, y such that:

$$
a x + n y = 1
$$

- The value of x modulo n is a^{-1}.

Step 3: Calculate $B \cdot a^{-1}$ modulo n

- Multiply B by a^{-1} and reduce modulo n.

Step 4: Write the explicit formula for $F(x)$

- The automorphism is then:

$$
F(x) = (B \cdot a^{-1}) x \ (\text{mod } n)
$$

Examples Illustrating the Formula

Example 1: $n=12$, $a=5$, $A=5$, $B=7$

- Check $\gcd(5, 12) = 1$. Yes.
- Find a^{-1} modulo 12:

- Using Extended Euclidean Algorithm:

$$
12 = 5 \times 2 + 2
$$
$$
5 = 2 \times 2 + 1
$$
$$
2 = 1 \times 2 + 0
$$

- Back-substitute:

$$
1 = 5 - 2 \times 2
$$
$$
2 = 12 - 5 \times 2
$$
$$
1 = 5 - 2 \times (12 - 5 \times 2) = 5 - 2 \times 12 + 5 \times 4 = 5 \times 5 - 2 \times 12
$$

- So:

$$
1 \equiv 5 \times 5 \ (\text{mod } 12)
$$

\]

- Therefore, \(a^{-1} \equiv 5\) mod 12.

- Compute \(B \cdot a^{-1} = 7 \times 5 = 35 \equiv 35 - 2 \times 12 = 35 - 24 = 11 \ (\text{mod } 12)\).

- The automorphism:

\[
F(x) \equiv 11 x \ (\text{mod } 12)
\]

- This automorphism satisfies \(F(5) \equiv 11 \times 5 = 55 \equiv 55 - 4 \times 12 = 55 - 48 = 7 \ (\text{mod } 12)\

Frequently Asked Questions

What does it mean for F to belong to Aut(zn)?

F belongs to Aut(zn) means F is an automorphism of the cyclic group zn, i.e., a bijective group homomorphism from zn to itself.

Why is the condition that A is relatively prime to N important?

Because A being relatively prime to N ensures that the multiplication map x ↦ A·x mod N is a permutation of zn, making it an automorphism of the group.

Given that F(a) = B, how can we express F(x) for an arbitrary x in zn?

Since automorphisms of zn are determined by the image of 1, and F is an automorphism with F(a) = B, we can express F(x) as F(x) = B^{x} where the operation is in the appropriate group context, or more generally, as F(x) ≡ A·x mod N.

What is the general form of automorphisms in Aut(zn)?

Automorphisms in Aut(zn) are functions of the form F(x) = A·x mod N, where A is an integer coprime to N.

How is the value of F(a) = B related to A in the

formula for F(x)?

Since F is determined by multiplication by A, and F(a) = B, then B ≡ A·a mod N, so A ≡ B·a^{-1} mod N, where a^{-1} is the inverse of a modulo N.

How do you find the formula for F(x) given F(a) = B?

First, find the inverse of a modulo N, then compute A ≡ B·a^{-1} mod N. The formula for F(x) becomes F(x) ≡ A·x mod N.

Can F(x) be expressed directly in terms of a and B? If so, what is it?

Yes, F(x) = (B · a^{-1})·x mod N, where a^{-1} is the multiplicative inverse of a modulo N.

What is the significance of the automorphism being determined by A in Aut(zn)?

It signifies that every automorphism corresponds to multiplication by a unique element A in zn^, and knowing F(a) allows us to find this A, thus fully determining the automorphism.

Additional Resources

Suppose F Belongs To Aut(zn) And A Is Relatively Prime To N. If F(a) ≡ B, Determine A Formula For F(x).

This intriguing problem lies at the intersection of group theory, number theory, and algebraic functions. It challenges us to understand how automorphisms of the cyclic group $\mathbb{Z}_n$ behave, especially when they are constrained by specific conditions such as the images of particular elements and the relative primality of certain parameters. In this comprehensive guide, we'll explore the problem in depth, clarify the underlying concepts, and provide a step-by-step approach to derive a formula for the automorphism $F(x)$.

Understanding the Context and Key Concepts

1. The Group $\mathbb{Z}_n$ and Its Automorphisms

- Definition of $\mathbb{Z}_n$: The cyclic group of order n, consisting of elements $\{0, 1, 2, \ldots, n-1\}$ with addition modulo n.
- Automorphisms $\text{Aut}(\mathbb{Z}_n)$: The set of all bijective group homomorphisms from $\mathbb{Z}_n$ to itself. Since $\mathbb{Z}_n$

\) is cyclic, its automorphisms are determined entirely by the image of a generator, typically 1.

2. The Group \(\text{Aut}(\mathbb{Z}_n) \)

- Structure: \(\text{Aut}(\mathbb{Z}_n) \) is isomorphic to the multiplicative group of units modulo \(n \), denoted \((\mathbb{Z}/n\mathbb{Z})^\times \).
- Automorphisms as Multiplication: Each automorphism \(F \) can be expressed as \(F(x) \equiv a x \pmod{n} \) for some \(a \) with \(\gcd(a, n) = 1 \).

3. The Role of the Element \(a \) and the Condition \(\gcd(a, n) = 1 \)

- The element \(a \) in the problem is used to define the automorphism \(F \). Since \(A \) (not to be confused with the element \(a \)) is relatively prime to \(n \), this ensures that \(F \) is invertible and indeed an automorphism.

Restating the Problem

Given:

- \(F \in \text{Aut}(\mathbb{Z}_n) \), i.e., \(F \) is an automorphism of \(\mathbb{Z}_n \).
- \(A \) is an element of \(\mathbb{Z}_n \) with \(\gcd(A, n) = 1 \).
- \(F(a) \equiv B \pmod{n} \), where \(a \) is an element of \(\mathbb{Z}_n \) (often we consider \(a \) as a generator or an element in the group).

Question: Determine a formula for \(F(x) \) in terms of known parameters.

Step-by-Step Approach to Derive the Formula

1. Recognize the Structure of \(F \)

Since \(F \in \text{Aut}(\mathbb{Z}_n) \), and \(\mathbb{Z}_n \) is cyclic, every automorphism is determined by its action on a generator, say \(1 \). Therefore, for some \(a \) with \(\gcd(a, n) = 1 \):

\[
F(x) \equiv a x \pmod{n}
\]

Our goal is to find \(a \) such that \(F(a) \equiv B \pmod{n} \).

---

2. Expressing the Automorphism

Given the form:

$$
F(x) \equiv a x \pmod{n}
$$

and the condition:

$$
F(a) \equiv B \pmod{n}
$$

we substitute:

$$
F(a) \equiv a \cdot a \equiv a^2 \equiv B \pmod{n}
$$

Thus, the key relation simplifies to:

$$
a^2 \equiv B \pmod{n}
$$

---

3. Solving for a

Given that:

$$
a^2 \equiv B \pmod{n}
$$

and $\gcd(a, n) = 1$, the problem reduces to solving a quadratic congruence:

$$
a^2 \equiv B \pmod{n}
$$

Important note: For solutions to exist, B must be a quadratic residue modulo n. The existence of solutions depends on the properties of n and B.

---

4. Conditions for Existence of a

- When n is prime:
The congruence $a^2 \equiv B \pmod{p}$ has solutions if and only if B is a quadratic residue modulo p.
- When n is composite:
Use the Chinese Remainder Theorem (CRT) to solve the quadratic congruence modulo each prime power dividing n.

---

5. Finding a in Practice

- Prime modulus case:
Use quadratic residue tests (Legendre symbol) and techniques like Tonelli-Shanks to find solutions.

- Composite modulus case:
Decompose n into prime powers: $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$.
Solve $a^2 \equiv B \pmod{p_i^{k_i}}$ for each $p_i^{k_i}$.
Use CRT to combine solutions.

Final Formula for $F(x)$

Once a is determined (possibly with multiple solutions), the automorphism F is:

$$
\boxed{
F(x) \equiv a x \pmod{n}
}
$$

where a satisfies:

- $a^2 \equiv B \pmod{n}$,
- $\gcd(a, n) = 1$.

If multiple solutions for a exist, each corresponds to a different automorphism satisfying the given conditions.

Additional Considerations and Special Cases

1. When $B \equiv 1 \pmod{n}$

- The automorphism reduces to $F(x) \equiv a x \pmod{n}$ with $a^2 \equiv 1 \pmod{n}$.
- Solutions for a are elements with order dividing 2 in $($

(\mathbb{Z}/n\mathbb{Z})^\times \), i.e., \(a \equiv \pm 1 \pmod{n} \).

2. When \(\gcd(a, n) \neq 1 \)

- Such \(a \) do not define automorphisms; they correspond to endomorphisms or non-invertible functions.

Summary and Practical Algorithm

Given:

- \(n \)
- \(B \in \mathbb{Z}_n \)
- The condition \(F(a) \equiv B \), with \(\gcd(a, n) = 1 \)

Goal:

- Find \(a \) such that \(a^2 \equiv B \pmod{n} \) and \(\gcd(a, n) = 1 \).
- Define \(F(x) \equiv a x \pmod{n} \).

Algorithm Steps:

1. Verify \(B \)'s Quadratic Residue Status:

- Check if \(B \) is a quadratic residue modulo each prime power dividing \(n \).
- If not, no solution exists.

2. Solve \(a^2 \equiv B \pmod{n} \):

- For prime \(p \), use quadratic residue algorithms to find solutions.
- For composite \(n \), decompose via CRT.

3. Check \(\gcd(a, n) = 1 \):

- Ensure solutions for \(a \) are invertible modulo \(n \).

4. Construct \(F \):

- For each valid \(a \), define \(F(x) \equiv a x \pmod{n} \).

Conclusion

In this problem, the key insight is recognizing that automorphisms of \(

\mathbb{Z}_n \) are characterized by multiplication by units modulo \(n \). The condition \(F(a) \equiv B \pmod{n} \) translates into solving a quadratic congruence \(a^2 \equiv B \pmod{n} \). By solving this congruence and ensuring \(a \) is invertible (i.e., \(\gcd(a, n) = 1 \)), we obtain explicit formulas for

Suppose F Belongs To Aut Zn And A Is Relatively Prime To N If F A 5 B Determine A Formula For F X

Suppose F Belongs To Aut Zn And A Is Relatively Prime To N If F A 5 B Determine A Formula For F X

Related Articles

- The Company Was Organized Into The Detergent Area, The Dishwashing Soap Area, And The Health And Beauty
- Show All Your Work. Indicate Clearly The Methods You Use, Because You Will Be Scored On The Correctness
- What Is The Internal Resistance (in) Of An Automobile Battery That Has An Emf Of 12.0 V And A Terminal

Back to Home