EE5609 Challenge Problem

Vimal K B
Roll No - AI20MTECH14002

Abstract—**The problem is about proving that the given set is a field only when the cardinality of the set is a prime number.**

1 Problem Statement

For a positive integer p, consider the set $\mathbb{Z}_p = \{0, 1, 2 \ldots, p-1\}$, along with the operations

$$a \oplus b = [a+b] \bmod p \tag{1.0.1}$$

$$a \odot b = [a.b] \bmod p \tag{1.0.2}$$

for any $a, b \in \mathbb{Z}_p$, where + and . are standard integer addition and multiplication. For what values of p is $(\mathbb{Z}_p, \oplus, \odot)$ a field?

2 Solution

The set $\mathbb{Z}_p$ will be a field when the value of p is a prime number.

3 Proof

As we already know that the operations of addition and multiplication are commutative and associative in nature, they are closed under the $\mathbb{Z}_p$.

For the above set the additive identity is 0, and the multiplicative identity is 1.

In regards with the additive inverse, if we take a set $\mathbb{Z}_p = \{0, 1, 2 \ldots, p-1\}$ where p is any arbiturary value, when performing the additive identity operation we need to get the resultant as 0. Which can be seen as:-

$$\mathbb{Z}_p = \{0, 1, 2 \ldots, p-1\}, p > 2 \tag{3.0.1}$$

Additive inverse of 0 is 0. Additive inverse of 1 is $(p-1)$

$$1 \oplus (p-1) = [1 + p - 1] \bmod p \tag{3.0.2}$$

$$\implies 1 \oplus (p-1) = p \bmod p \implies 0 \tag{3.0.3}$$

For any arbitrary value $x \in \mathbb{Z}_p$, the additive inverse of x is $(p-x)$, since x is present in the set, $(p-x)$ will also be present in the set

$$x \oplus (p-x) = [x + p - x] \bmod p \tag{3.0.4}$$

$$\implies x \oplus (p-x) = p \bmod p \implies 0 \tag{3.0.5}$$

By definition, an integer a is a multiplicative inverse of integer x, if the product ax is congruent to 1 with respect to the modulus p. That is,

$$ax \equiv 1 (\bmod p) \tag{3.0.6}$$

Which means, after dividing ax with p we will get the remainder as 1.

In case of the non prime integer value for p such as 4,6,8,9,... etc. there will be an integer present in the set $\mathbb{Z}_p$ which can perfectly divide the value p. This causes, for some elements in the set $\mathbb{Z}_p$ to not get a multiplicative inverse, whose product when divided by p will result in 1.

To prove this, take an arbitrary value x present in the set $\mathbb{Z}_p$, where p be the multiple of x, represented as $p = nx$, n is any non-zero value. Lets assume that y is the multiplicative inverse of x. Then

$$[x.y] \bmod p = 1 \tag{3.0.7}$$

$$p \times q = xy - 1 \tag{3.0.8}$$

where q is a quotient.

But we know that p is a multiple of x, repsented as nx. So,

$$nx \times q \neq xy - 1 \tag{3.0.9}$$

because $nx \times q$ will again be a multiple of x.

Therefore, our initial assumption was incorrect.

But in the case of the prime numbers as 2,3,5,7,11,... etc, there is no integer (except 1) that can perfectly divide the prime number. This creates a way for finding a multiplicative inverse for the integers in the same set whose product when divided by p will result in 1.

From the above, we can see that for the set $\mathbb{Z}_p$ to be a field, the value of p must always be a prime number.