HW03 ECE 40400

Matteo Miglio

February 11th, 2021

Problem 1. Show whether or not the set of remainders Z_{18} forms a group with the modulo addition operator. Then show whether or not Z_{18} forms a group with the modulo multiplication operator.

a Addition: In order to prove that the set of remainders form a group under the modulo addition operator, we must show that the set satisfies closure, associativity, satisfies the identity element, and has an inverse element.

The set Z_{18} will satisfy closure because, for all a, b in the set Z_{18}, the element a + b = c is also in the set.

The set Z_{18} will satisfy associativity because of all w,x,y in the set Z_{18}, $[(w + x) + y]\ mod\ 18 = [w + (x + y)]\ mod\ 18$.

The set Z_{18} satisfies the identity element as a + 0 = a. Therefore the identity element is zero where there exists some w in set Z_{18} such that $(0 + w)\ mod\ 18 = w\ mod\ 18$.

The set Z_{18}, for each w ϵ Z_{18} there exists a $z\epsilon$ Z_{18} such that $w + z = 0\ mod\ 18$.

b In order to prove whether the set Z_{18} does not form a group under the modulo multiplication operator, all we have to do is disprove that it does not satisfy the inverse element property.

The set Z_{18} does not satisfy the inverse element property as some elements do not satisfy $b\epsilon$ Z_{18} such that $(a * b) \equiv 1\ mod\ 18$ where a,b are members of the set.

Problem 2. Compute $gcd(36459, 27828)$ using Euclid's algorithm.

$$\begin{aligned} & gcd(36549, 27828) \\ &= gcd(27828, 8631) \\ &= gcd(8631, 1935) \\ &= gcd(1935, 891) \\ &= gcd(891, 153) \\ &= gcd(153, 126) \\ &= gcd(126, 27) \\ &= gcd(27, 18) \\ &= gcd(18, 9) \\ &= gcd(9, 0) \end{aligned}$$

Therefore $gcd(36549, 27828) = 9$

Problem 3 Is the set of all unsigned integers $\mathbb{N}$ group under the gcd(.) operation?

Let us say that $gcd(a, i) = a$ where i = idetity element, such that i = 0. Then we ca directly infer that there cannot exist an inverse element with respect to the gcd operation because, for gcd(a,b) = i. = 0, a must be equal to 0. in every single model.

Problem 4 Use the extended Euclid's Algorithm to compute by hand the multiplicative inverse of 27 in Z_{32}. List all the steps.

Euclid's Extended Algorithm	
gcd(27, 32)	-
=gcd(32, 27)	$27 = (27 * 1) + (32 * 0)$
=gcd(27, 5)	$5 = (32 * 1) + (27 * 10)$
=gcd(5,2)	$2 = (27 * 1) - (5 * 5)$
=gcd(5,2)	$= (27 * 1) - 5 * (32 * 1 - 27 * 1)$
=gcd(5,2)	$= (-32 * 5) + (27 * 6)$
=gcd(2,1)	$1 = (32 * 11) - (27 * 13)$

Therefore the multiplicative inverse of 27 in Z_{32} is -13 which equivalent to 19.

Problem 5. The approach to solving this problem is by dividing x's coefficient to the other side and finding the multiplicative inverse of that coefficient with respect to the modulus. After finding that multiplicative inverse, we must plug it back in to find the smallest possible x such that it satisfies the modulus condition given.

a $9x = 11 \ (mod\ 13)$
x = 7

b $6x = 3 \ (mod\ 23)$
x = 12

c $5x = 9 \ (mod\ 11)$
x = 4