HW3
Vivek Khanolkar
vkhanolk
2/11/2021

ECE 404 HW 3

1. $\mathbb{Z}_{18}$ is a group with modulo addition since it checks all criteria for a group:
   closure → modulo always returns # between 0 and n-1
   associativity → + operators can be switched around ⇒ a+b = b+a
   identity element → (0+w) mod n = (w+0) mod n
   inverse element → always a # that can be added to get a 0 mod
   $\mathbb{Z}_{18}$ is NOT a group with modulo multiplication. It satisfies the same conditions as above EXCEPT multiplicative inverse. #'s like 2 will not have an MI.

2. gcd(36459, 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)
   ∴ gcd(36459, 27828) = 9

3. NO. Since it is all unsigned integers, IW we automatically get CLOSURE since the gcd(·) operator will always return an integer. ASSOCIATIVITY is also checked off since gcd(a,b) = gcd(b,a). There is also an IDENTITY ELEMENT → gcd(a, x·a) = a, however (x some constant) there is NO UNIQUE IDENTITY ELEMENT.

4. 27 modulo 32:

$\gcd(27, 32)$
$= \gcd(32, 27)$
$= \gcd(27, 5)$
$= \gcd(5, 2)$
$= \gcd(2, 1)$

residue $27 = 1 \times 27 + 0 \times 32$
$5 = 1 \times 32 + -1 \times 27$
$2 = 1 \times 32 - 6 \times 5$
$= 1 \times 32 - 6 \times (1 \times 32 + -1 \times 27)$
$= -5 \times 32 + 6 \times 27$
$1 = 5 - 2 \times 2$
$= (1 \times 32 + -1 \times 27) - 2 \times (-5 \times 32 + 6 \times 27)$
$= 1 \times 32 + -1 \times 27 + 10 \times 32 + -12 \times 27$
$= 11 \times 32 - 13 \times 27 = 11 \times 32 + 19 \times 27$

additive inverse per mod 32

∴ multiplicative inverse of 27 is 19 //

5: (a) $11 + 13 = 24$
$(24 + 13\alpha) = 9\beta$
3 3 3 ← LCF
$9\beta = 39 + 24 = 63$
$\beta = 7 = x$ //

(b) $3 + 23 = 26$
$(26 + 23\alpha) = 6x$
2 2 2 ← LCF
$26 + 46 = 72 = 6x$
$x = 12$ //

(c) $11 + 9 = 20$
$(20 + 11\alpha) = 5x$
5 5 5
$20 + 55 = 5x = 75$
$x = 15$
//