Daniel Furry ECE 40400 Homework 3

1.

Z_{18}:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
AI:	0	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
MI:	-	1	-	-	-	11	-	13	-	-	-	5	-	7	-	-	-	17

Z_{18} ... forms a group with the modulo addition operator, but does not with the modulo multiplication operator.

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)

Therefore, gcd(36459, 27828) = 9

3. The set of all unsigned integers $\mathbb{W}$ is not a group under the gcd(·) operation. The identity element for $\{\mathbb{W}, gcd(\cdot)\}$ is zero because the gcd of any number and zero is that number. The issue with this being a [redacted] group ... is there is no inverse element if $i = 0$.

4. $\gcd(27, 32) = 27 = 1(27) + 0(32)$

$= \gcd(32, 27) = 5 = -1(27) + 1(32)$

$= \gcd(27, 5) = 2 = 1(27) - 5(5) = 1(27) - 5[-1(27) + 1(32)] = 6(27) - 5(32)$

$= \gcd(5, 2) = 1 = 1(5) - 2(2) = \underbrace{1[-1(27) + 1(32)] - 2[6(27) - 5(32)]}_{-13(27) + 11(32)}$

$= \gcd(2, 1)$

$32 - 13 = 19$

$\boxed{\text{The multiplicative inverse of } 27 \text{ in } Z_{32} \text{ is } 19.}$

5.

a.) $9x \equiv 11 \pmod{13}$

11	1
24	2
32	3
50	4
→ 63	5

$9 \times 7 = 63$

$\boxed{x = 7}$

b.) $6x \equiv 3 \pmod{23}$

3	1
26	2
49	3
→ 72	4

$6 \times 12 = 72$

$\boxed{x = 12}$

c.) $5x \equiv 9 \pmod{11}$

9	1
→ 20	2

$5 \times 4 = 20$

$\boxed{x = 4}$