HW3

1. Prove $\{Z_{18}, +\}$

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

Addition

Closure: $(a+b)\%18$ will always be less than 18 and will always be an integer

Associativity: $((a+b)+c)\%18 = (a+(b+c))\%18$

Identity: $a+0=a$ $(a+0)\%18 = a\%18$

Inverse: All elements have an additive inverse

This means that $\{Z_{18}, +\}$ is a group

Multiplication

Inverse not all elements have a M.I.,

so $\{Z_{18}, \times\}$ is not a group

2. Prove $\{W, \gcd()\}$

Closure: gcd() of two integers will always be a positive integer

Associativity: The order of the gcd() operator doesn't matte

Identity: gcd(a, 0) will always return a since a|0

Inverse: gcd() can never return zero, so there is no inverse for numbers in W

so, $\{W, \gcd()\}$ is not a group

3. gcd(10946, 19838) → gcd(19838, 10946)

↓

gcd(8892, 2054) ← gcd(10946, 8892)

↓

gcd(2054, 676) → gcd(676, 26) → gcd(26, 0)

↓

gcd(10946, 19838) = 26

4. M. I. of 19 Z_{35}

gcd (19, 35)
gcd (35, 19)
gcd (19, 16)
gcd (16, 3)
gcd (3, 1)
gcd (1, 0)
gcd = 1

residue 16 = $1 \times 35 - 1 \times 19$
residue 3 = $1 \times 19 - (1 \times 35 - 1 \times 19)$
residue 1 = $1 \times 16 - 5(1 \times 19 - (1 \times 35 - 1 \times 19))$
$= 1 \times 35 - 1 \times 19 - 5(1 \times 19 - (1 \times 35 - 1 \times 19))$
$= 1 \times 35 - 1 \times 19 - 5 \times 19 + 5 \times 35 - 5 \times 19$
$= 6 \times 35 - 11 \times 19$
$= 6 \times 35 + 24 \times 19$ since $-11 = 24$ in mod 35
So 24 is the M. I. of 19 in Z_{35}

5. $6x \equiv 3 \bmod 23$ M. I. of 6 is $4 \cdot 3 = 12$
$x = 12$

$7x \equiv 11 \bmod 13$ M. I. of 7 is $2 \cdot 11 = 22 \% 13 = 9$
$x = 9$

$5x \equiv 7 \bmod 11$ M. I. of 5 is $9 \cdot 7 = 63 \% 11 = 8$
$x = 8$