

1.

Z_{21} forms a group with the modulo addition operation

- Closure: Clearly, adding one element in the set to another element in the set, the output would still be the element in the set.

- Associativity:

We know: $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$, in this case, $n=21$, w , x and y are the element in the set.

- Identity element: 0 is the identity element

- Inverse element

Every element in the set has additive inverse, the additive inverse of 0 is 0.

For element that is not 0 in the set, its additive inverse is $21-n$.

Since all four properties are satisfied with addition operation, Z_{21} forms a group with the modulo addition operation.

Z_{21} does not form a group with the modulo multiplication operation, because not every element in the set has a multiplicative inverse, for example, the element 0 in the set does not have a multiplicative inverse, which makes it not a group with multiplication operation.

2.

The identity element is 0, because 0 is the divisor for all integers, so for any integer a , $\gcd(a,0)=a$.

However, we are not able to find any pairs (a,b) in the set such that $\gcd(a,b)=0$, because we know 0 cannot be divided by any integer, meaning that for any integer a , $\frac{a}{0}$ is invalid, hence the greatest common divisor cannot be 0, which leads to the non-existence of inverse element of each element in the set. Therefore, this set is not a group.

3.

$$\begin{aligned}
 &\gcd(21609, 18432) \\
 &= \gcd(18432, 3177) \\
 &= \gcd(3177, 2547) \\
 &= \gcd(2547, 630) \\
 &= \gcd(630, 27) \\
 &= \gcd(27, 9) \\
 &= \gcd(9, 0)
 \end{aligned}$$

Therefore, $\gcd(21609, 18432) = 9$

4.

$$\begin{array}{ll}
 \gcd(24, 35) & \\
 = \gcd(35, 24) & | \text{ residue } 24 = 1 \times 24 + 0 \times 35 \\
 = \gcd(24, 11) & | \text{ residue } 11 = -1 \times 24 + 1 \times 35 \\
 = \gcd(11, 2) & | \text{ residue } 2 = 1 \times 24 - 2 \times 11 \\
 & | \quad \quad \quad = 1 \times 24 - 2 \times (-1 \times 24 + 1 \times 35) \\
 & | \quad \quad \quad = 1 \times 24 + 2 \times 24 - 2 \times 35 \\
 & | \quad \quad \quad = 3 \times 24 - 2 \times 35 \\
 = \gcd(2, 1) & | \text{ residue } 1 = 1 \times 11 - 5 \times 2 \\
 & | \quad \quad \quad = (35 - 24) - 5 \times (3 \times 24 - 2 \times 35) \\
 & | \quad \quad \quad = 1 \times 35 - 1 \times 24 - 15 \times 24 + 10 \times 35 \\
 & | \quad \quad \quad = -16 \times 24 + 11 \times 35 \\
 & | \quad \quad \quad = 19 \times 24 + 11 \times 35
 \end{array}$$

Therefore, the multiplicative inverse of 24 in Z_{35} is 19.

5.

(a)

$$6x \equiv 3 \pmod{23}$$

6 is relatively prime to 23, so there is multiplicative inverse for 6 in Z_{23} , finding it using Extended Euclid's algorithm:

$$\begin{array}{ll}
 \gcd(23, 6) & \\
 = \gcd(6, 5) & | \text{ residue } 5 = 1 \times 23 - 3 \times 6 \\
 = \gcd(5, 1) & | \text{ residue } 1 = 1 \times 6 - 1 \times 5 \\
 & | \quad \quad \quad = 1 \times 6 - 1 \times (1 \times 23 - 3 \times 6) \\
 & | \quad \quad \quad = 1 \times 6 - 1 \times 23 + 3 \times 6 \\
 & | \quad \quad \quad = 4 \times 6 - 1 \times 23
 \end{array}$$

Which means 6^{-1} in Z_{23} is 4, so

$$x = (3 \times 6^{-1}) \pmod{23} = 12$$

(b)

$$7x \equiv 11 \pmod{13}$$

7 is relatively prime to 13, so there is multiplicative inverse for 7 in Z_{13} , finding it using Extended Euclid's algorithm:

$$\gcd(13, 7)$$

$$= \gcd(7, 6) \quad | \text{ residue} \quad 6 = 1 \times 13 - 1 \times 7$$

$$\begin{array}{l|l} = \gcd(6, 1) & \text{residue} \quad 1 = 1 \times 7 - 1 \times 6 \\ & = 1 \times 7 - 1 \times (1 \times 13 - 1 \times 7) \\ & = 1 \times 7 - 1 \times 13 + 1 \times 7 \\ & = 2 \times 7 - 1 \times 13 \end{array}$$

Which means 7^{-1} in Z_{13} is 2, so

$$x = (11 \times 7^{-1}) \pmod{13} = 9$$

(c)

$$5x \equiv 7 \pmod{11}$$

5 is relatively prime to 11, so there is multiplicative inverse for 5 in Z_{11} , finding it using Extended Euclid's algorithm:

$$\gcd(11, 5)$$

$$\begin{array}{l|l} = \gcd(5, 1) & \text{residue} \quad 1 = 1 \times 11 - 2 \times 5 \\ & = 1 \times 11 + 9 \times 5 \end{array}$$

Which means 5^{-1} in Z_{11} is 9, so

$$x = (7 \times 5^{-1}) \pmod{11} = 8$$