1) $Z_{21} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}$

$a * b = \frac{a+b}{21}$

Closed property

if $a, b \in Z_{21}$

Then $a+b \in Z_{21}$

Associative property is also satisfied

Identity element

$a * e = a$

therefore, 0 is identity element.

Inverse :

$a*b = e = b*a$

$\frac{(0+0)}{21} = 0$, $\frac{1+20}{21} = 0$, $\frac{2+19}{21} = 0$, $\frac{3+18}{21} = 0$,

$\frac{4+17}{21} = 0$, $\frac{5+16}{21} = 0$, $\frac{6+15}{21} = 0$, $\frac{7+14}{21} = 0$,

$\frac{8+13}{21} = 0$, $\frac{9+12}{21} = 0$, $\frac{10+11}{21} = 0$

So, the inverse of each element exists.

Hence, Z_{21} forms a group under addition operator.

Multiplication:

$a * b = \frac{ab}{21}$

Closed & associative properties are satisfied.

Identity element

$a * e = a$

1 is identity element

Hence, identity element exists.

$a * b = e = b * a$

$a * b = 1$

But inverse of 0 does not exist.

So, Z_{21} does not form group under multiplication.

2) Check for closure, associativity, identity, inverse

For closure, $a * b$ belongs to N.

This is true because the gcd of 2 numbers belong to the min (a, b) if a, b are unsigned.

Gcd follows the associativity law

$gcd(gcd(a,b),c) = gcd(a, gcd(b,c))$

They are both the same.

Checking for inverse

for sample $S = \{10, 20, 30, 40, 50, 60\}$
for all S belong to W.

$gcd(30, 40) = 10$
$gcd(30, 20) = 10$
The inverse is not unique for few elements.

So, it is not a group.

3) $gcd(21609, 18432)$

$21609 \% 18432 = 3177$

$18432 \% 3177 = 2547$

$3177 \% 2547 = 630$

$2547 \% 630 = 27$

$630 \% 27 = 9$

$27 \% 9 = 0$

so, $gcd(21609, 18432) = 9$.

4) $24^{-1} \mod 35$

GCD using euclidean algorithm

$35 = 24(1) + 11$ ← Remainder

$24 = 11(2) + 2$

$11 = 2(5) + 1 \rightarrow$ GCD

$2 = 1(2) + 0 \rightarrow$ Have to take remainder before reaching 0.

So, $\gcd(35, 24) = 1$

Extended euclidean algorithm

$1 = 11 - 2(5)$

$1 = 11 - (24 - 11(2))(5)$

$1 = 11 - 24(5) + 11(10)$

$1 = 11(11) + 24(-5)$

$1 = 11(35 - 24(1)) + 24(-5)$

$1 = 35(11) - 24(11) + 24(-5)$

$1 = 35(11) + 24(-16$

$35, (35-16) = 19$

$\therefore 24^{-1} \mod 35 = 19$

5) a) $6x \equiv 3 \pmod{23}$

$ax \equiv b \pmod{m}$

$a = 6$, $b = 3$ & $m = 23$

$\gcd(a, m) = \gcd(6, 23) = 1$ and $1/3$

By euclidean algorithm

$23 = 6 \times 3 + 15$ — (1)

$6 = 5 \times 1 + 1$ — (2)

$5 = 1 \times 5 + 0$

$1 = 6 - 5 \times 1$

$1 = 6 - [23 - 6 \times 3] \times 1$

$1 = 6 - 23 \times 1 + 6 \times 3$

$1 = (3+1) \times 6 - 1 \times 23$

$1 = 4 \times 6 + (-1) \times 23$ — (3)

$3 = (3 \times 4) \times 6 + (-3) \times 23 \pmod{23}$

$3 = 12 \times 6 + (-3) \times 23$ — (4)

$\boxed{x_0 = 12}$ is the solution

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

$a = 7$, $b = 11$, $m = 13$

gcd(a, m) = gcd(7, 13) = 1 and $\frac{1}{11}$
By euclidean algorithm

$13 = 7 \times 1 + 6$ —— ①
$7 = 6 \times 1 + 1$ —— ②
$6 = 1 \times 6 +$

$1 = 7 - 6 \times 1$
$1 = 7 - [13 - 7 \times 1] \times 1$ .. from ①
$1 = 7 - 13 \times 1 + 7 \times 1$
$1 = 2 \times 7 - 1 \times 13$
mutiply above by eqn ②
$11 = 22 \times 7 - 11 \times 13 \pmod{13}$
$11 = 9 \times 7 - 11 \times 13 \pmod{13}$
$\therefore \boxed{x = 9}$ is the solution

c) $5x \equiv 7 \pmod{11}$
$a = 5, b = 7, m = 11$
gcd(a, m) = gcd(5, 11) = 1 and $\frac{1}{7}$
By euclidean algorithm
$11 = 5 \times 2 + 1 \rightarrow$ (*)
$5 = 1 \times 5 + 0$

From (*)

$1 = 11 - 5 \times 2$

$1 = 1 \times 11 + (-2) \times 5$

multiply by 7 to both sides

$7 = 7 \times 11 + (-14) \times 5 \pmod{11}$

$7 = 7 \times 11 + 8 \times 5 \pmod{11}$

$\therefore \boxed{x = 8}$ is the solution