1 1.2

Let $x, d \in \mathbb{Z}$, where $d > 0$. Prove that $M \cap N \neq \emptyset$, where $M = \{x - qd | q \in \mathbb{Z}\}$.

Solution 1.1. Let $x, d \in \mathbb{Z}$, where $d > 0$. Let $M = \{x - qd \mid q \in \mathbb{Z}\}$ and $N = \{x + pd \mid p \in \mathbb{Z}\}$.
Consider $x \in \mathbb{Z}$:

$$x = x - 0d \in M \quad \text{(where } q = 0\text{)}$$
$$x = x + 0d \in N \quad \text{(where } p = 0\text{)}$$

Therefore, $x \in M \cap N$, and thus $M \cap N \neq \emptyset$.

2 1.3

Let $a, b, N \in \mathbb{Z}$ where $N > 0$ Prove that $[a][b] = [[a][b]]$ where $[x]$ denotes the remainder of x after divison by N

Solution 2.1. By definition of modular arithmetic:

$$a \equiv [a] \pmod{N}$$
$$b \equiv [b] \pmod{N}$$

This means there exist integers k and m such that:

$$a = [a] + kN$$
$$b = [b] + mN$$

Multiplying these equations:

$$\begin{aligned} ab &= ([a] + kN)([b] + mN) \\ &= [a][b] + [a]mN + [b]kN + kmN^2 \end{aligned}$$

Taking both sides modulo N:

$$\begin{aligned} [ab] &\equiv [[a][b] + [a]mN + [b]kN + kmN^2] \pmod{N} \\ &\equiv [[a][b]] \pmod{N} \end{aligned}$$

and thus $[ab] = [[a][b]]$.
this is because $[a]mN$, $[b]kN$, and kmN^2 are all multiples of N.

3 1.6

Solution 3.1. Let $a = a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n$, where $0 \leq a_i < 10$.
(i) 2 divides a if and only if 2 divides a_0:
$a \equiv a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n \pmod 2 \equiv a_0 + 0 + 0 + \cdots + 0 \pmod 2$ (since $10^k \equiv 0 \pmod 2$ for $k \geq 1$) $\equiv a_0 \pmod 2$
Therefore, $a \equiv 0 \pmod 2$ if and only if $a_0 \equiv 0 \pmod 2$.

(ii) 4 divides a if and only if 4 divides $a_0 + 2a_1$:
$a \equiv a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n \pmod 4 \equiv a_0 + 2a_1 + 0 + \cdots + 0 \pmod 4$ (since $10 \equiv 2 \pmod 4$ and $10^k \equiv 0 \pmod 4$ for $k \geq 2$) $\equiv a_0 + 2a_1 \pmod 4$
Therefore, $a \equiv 0 \pmod 4$ if and only if $a_0 + 2a_1 \equiv 0 \pmod 4$.

(iii) 8 divides a if and only if 8 divides $a_0 + 2a_1 + 4a_2$:
$a \equiv a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n \pmod 8 \equiv a_0 + 2a_1 + 4a_2 + 0 + \cdots + 0 \pmod 8$ (since $10 \equiv 2 \pmod 8$, $10^2 \equiv 4 \pmod 8$, and $10^k \equiv 0 \pmod 8$ for $k \geq 3$) $\equiv a_0 + 2a_1 + 4a_2 \pmod 8$
Therefore, $a \equiv 0 \pmod 8$ if and only if $a_0 + 2a_1 + 4a_2 \equiv 0 \pmod 8$

(iv) 5 divides a if and only if 5 divides a_0:
$a \equiv a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n \pmod 5 \equiv a_0 + 0 + 0 + \cdots + 0 \pmod 5$ (since $10^k \equiv 0 \pmod 5$ for $k \geq 1$) $\equiv a_0 \pmod 5$
Therefore, $a \equiv 0 \pmod 5$ if and only if $a_0 \equiv 0 \pmod 5$.
(v) Let $a = a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n$, where $0 \leq a_i < 10$.
9 divides a if and only if 9 divides the sum $a_0 + a_1 + \cdots + a_n$ of its digits:
$a \equiv a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n \pmod 9 \equiv a_0 + a_1 + a_2 + \cdots + a_n \pmod 9$ (since $10^k \equiv 1 \pmod 9$ for all $k \geq 0$)
Therefore, $a \equiv 0 \pmod 9$ if and only if $(a_0 + a_1 + \cdots + a_n) \equiv 0 \pmod 9$.
Note: $10^k \equiv 1 \pmod 9$ for all $k \geq 0$ because $10^k - 1 = (10-1)(10^{k-1} + 10^{k-2} + \cdots + 1)$ is divisible by 9 for $k \geq 1$, and $10^0 - 1 = 0$ is also divisible by 9.

4 1.8

$3 | 4^n - 1$ for all $n \in \mathbb{N}$

Solution 4.1. e will prove that $3 \mid 4^n - 1$ for all $n \in \mathbb{N}$ using mathematical induction.
Base case: For $n = 1$, $4^1 - 1 = 3$, which is clearly divisible by 3.
Inductive step: Assume the statement holds for some $k \in \mathbb{N}$, i.e., $3 \mid 4^k - 1$. This means there exists an integer m such that $4^k - 1 = 3m$.
Now, let's prove it holds for $k + 1$:

$$\begin{aligned}
4^{k+1} - 1 &= 4 \cdot 4^k - 1 \\
&= 4(4^k - 1) + 4 - 1 \\
&= 4(3m) + 3 \quad \text{(substituting } 4^k - 1 = 3m\text{)} \\
&= 12m + 3 \\
&= 3(4m + 1)
\end{aligned}$$

Since $4m + 1$ is an integer, we have shown that $4^{k+1} - 1$ is divisible by 3.
we can also use the fact that $4 \equiv 1 \pmod 3$ and any power to the 4 bigger than 1 would be divisible by 3.

5 1.11

Solution 5.1. et x, y, z, $d \in \mathbb{Z}$ where $d \neq 0$.
(i) Reflexivity: $x \equiv x \pmod d$
By definition, $x \equiv x \pmod d$ if $d \mid (x - x)$. $x - x = 0 = d \cdot 0$ Therefore, $d \mid (x - x)$, so $x \equiv x \pmod d$.
(ii) Symmetry: If $x \equiv y \pmod d$, then $y \equiv x \pmod d$
Given: $x \equiv y \pmod d$ This means $d \mid (x - y)$, so there exists an integer k such that $x - y = dk$ Rearranging: $y - x = -dk = d(-k)$ Since $-k$ is an integer, $d \mid (y - x)$ Therefore, $y \equiv x \pmod d$
(iii) Transitivity: If $x \equiv y \pmod d$ and $y \equiv z \pmod d$, then $x \equiv z \pmod d$
Given: $x \equiv y \pmod d$ and $y \equiv z \pmod d$ This means there exist integers k and m such that: $x - y = dk$ and $y - z = dm$ Adding these equations: $(x - y) + (y - z) = dk + dm$ $x - z = d(k + m)$ Since $k + m$ is an integer, $d \mid (x - z)$ Therefore, $x \equiv z \pmod d$
(iv)

6 2.1

Solution 6.1.

1. Injectivity:

   Let $x_1, x_2 \in G$ such that $\xi(x_1) = \xi(x_2)$. Then $x_1 g = x_2 g$. Multiplying both sides by g^{-1} on the right (which exists because G is a group): $x_1 g g^{-1} = x_2 g g^{-1}$ $x_1 = x_2$ (by the properties of inverse elements in a group)

   Thus, if $\xi(x_1) = \xi(x_2)$, then $x_1 = x_2$, proving that ξ is injective.

2. Surjectivity:

   Let $y \in G$ be arbitrary. We need to find an $x \in G$ such that $\xi(x) = y$. Consider $x = yg^{-1}$. Then $\xi(x) = \xi(yg^{-1}) = yg^{-1}g = y$ (by the properties of inverse elements)

   Thus, for any $y \in G$, we can find an $x \in G$ (namely, yg^{-1}) such that $\xi(x) = y$, proving that ξ is surjective.

   Since ξ is both injective and surjective, we conclude that ξ is bijective.