# Chapter 4.1
# Solutions

1.

(a)

$$\begin{aligned} c &\equiv 9a \pmod{13} \\ &\equiv 9 \cdot 4 \pmod{13} \\ &\equiv 36 \pmod{13} \\ &\equiv 10 \pmod{13} \end{aligned}$$

(b)

$$\begin{aligned} c &\equiv 2a + 3b \pmod{13} \\ &\equiv 2 \cdot 4 + 3 \cdot 9 \pmod{13} \\ &\equiv 8 + 27 \pmod{13} \\ &\equiv 35 \pmod{13} \\ &\equiv 9 \pmod{13} \end{aligned}$$

(c)

$$\begin{aligned} c &\equiv a^3 - b^3 \pmod{13} \\ &\equiv 4^3 - 9^3 \pmod{13} \\ &\equiv 64 - 729 \pmod{13} \\ &\equiv -665 \pmod{13} \\ &\equiv 11 \pmod{13} \end{aligned}$$

3.

(a) $a \equiv 24 \pmod{31} \equiv -7 \pmod{31}$
Therefore $a = -7$
(We note that $24 - 31 = -7$)
(b) $a \equiv 99 \pmod{41} \equiv 140 \pmod{41}$
Therefore $a = 140$
(we note that $99 + 41 = 140$)

5.

In $\mathbb{Z}_5$, the multiplicative inverse of 4 is 4. Essentially, $4 \cdot 4 \pmod{5} = 16 \pmod{5} = 1 \pmod{5}$.

In $\mathbb{Z}_6$, 4 has no multiplicative inverse Essentially,

$$\begin{aligned}
4 \cdot 0 &\equiv 0 \pmod 6 \neq 1 \pmod 6 \\
4 \cdot 1 &\equiv 4 \pmod 6 \neq 1 \pmod 6 \\
4 \cdot 2 &\equiv 2 \pmod 6 \neq 1 \pmod 6 \\
4 \cdot 3 &\equiv 0 \pmod 6 \neq 1 \pmod 6 \\
4 \cdot 4 &\equiv 4 \pmod 6 \neq 1 \pmod 6 \\
4 \cdot 5 &\equiv 2 \pmod 6 \neq 1 \pmod 6
\end{aligned}$$

In $\mathbb{Z}_7$, the multiplicative inverse of 4 is 2. Essentially, $4 \cdot 2 \pmod 7 = 8 \pmod 7 = 1 \pmod 7$.
In $\mathbb{Z}_8$, 4 has no multiplicative inverse. Essentially,

$$\begin{aligned}
4 \cdot 0 &\equiv 0 \pmod 6 \neq 1 \pmod 8 \\
4 \cdot 1 &\equiv 4 \pmod 6 \neq 1 \pmod 8 \\
4 \cdot 2 &\equiv 0 \pmod 6 \neq 1 \pmod 8 \\
4 \cdot 3 &\equiv 4 \pmod 6 \neq 1 \pmod 8 \\
4 \cdot 4 &\equiv 0 \pmod 6 \neq 1 \pmod 8 \\
4 \cdot 5 &\equiv 4 \pmod 6 \neq 1 \pmod 8 \\
4 \cdot 6 &\equiv 0 \pmod 6 \neq 1 \pmod 8 \\
4 \cdot 7 &\equiv 4 \pmod 6 \neq 1 \pmod 8
\end{aligned}$$

In $\mathbb{Z}_9$, the multiplicative inverse of 4 is 7. Essentially, $4 \cdot 7 \pmod 9 = 28 \pmod 9 = 1 \pmod 9$.
In $\mathbb{Z}_{10}$, 4 has no multiplicative inverse. Essentially,

$$\begin{aligned}
4 \cdot 0 &\equiv 0 \pmod 6 \neq 1 \pmod{10} \\
4 \cdot 1 &\equiv 4 \pmod 6 \neq 1 \pmod{10} \\
4 \cdot 2 &\equiv 8 \pmod 6 \neq 1 \pmod{10} \\
4 \cdot 3 &\equiv 2 \pmod 6 \neq 1 \pmod{10} \\
4 \cdot 4 &\equiv 6 \pmod 6 \neq 1 \pmod{10} \\
4 \cdot 5 &\equiv 0 \pmod 6 \neq 1 \pmod{10} \\
4 \cdot 6 &\equiv 4 \pmod 6 \neq 1 \pmod{10} \\
4 \cdot 7 &\equiv 8 \pmod 6 \neq 1 \pmod{10} \\
4 \cdot 8 &\equiv 2 \pmod 6 \neq 1 \pmod{10} \\
4 \cdot 9 &\equiv 6 \pmod 6 \neq 1 \pmod{10}
\end{aligned}$$

In $\mathbb{Z}_{11}$, the multiplicative inverse of 4 is 3. Essentially, $4 \cdot 3 \pmod{11} = 12 \pmod{11} = 1 \pmod{11}$.

In $\mathbb{Z}_{12}$, 4 has no multiplicative inverse. Essentially,

$$\begin{aligned}
4 \cdot 0 &\equiv 0 \pmod 6 \neq 1 \pmod{12} \\
4 \cdot 1 &\equiv 4 \pmod 6 \neq 1 \pmod{12} \\
4 \cdot 2 &\equiv 8 \pmod 6 \neq 1 \pmod{12} \\
4 \cdot 3 &\equiv 0 \pmod 6 \neq 1 \pmod{12} \\
4 \cdot 4 &\equiv 4 \pmod 6 \neq 1 \pmod{12} \\
4 \cdot 5 &\equiv 8 \pmod 6 \neq 1 \pmod{12} \\
4 \cdot 6 &\equiv 0 \pmod 6 \neq 1 \pmod{12} \\
4 \cdot 7 &\equiv 4 \pmod 6 \neq 1 \pmod{12} \\
4 \cdot 8 &\equiv 8 \pmod 6 \neq 1 \pmod{12} \\
4 \cdot 9 &\equiv 0 \pmod 6 \neq 1 \pmod{12} \\
4 \cdot 10 &\equiv 4 \pmod 6 \neq 1 \pmod{12} \\
4 \cdot 11 &\equiv 8 \pmod 6 \neq 1 \pmod{12}
\end{aligned}$$

7. The statement is of the form

$$\forall a \forall b \forall c \ (a|b \wedge a|c \rightarrow a|(b+c))$$

Domain of $a : \mathbb{Z}^*$. Domain of $b, c : \mathbb{Z}$.
The statement is true. Here is a direct proof : theorem seen in class !

9.

The statement is of the form

$$\forall a \forall b \ (\forall c \, (a|bc) \rightarrow a|b)$$

Domain of $a : \mathbb{Z}^*$. Domain of $b, c : \mathbb{Z}$.
The statement is true. Here is a direct proof.

Let $a, b \in \mathbb{Z}$ where $a \neq 0$.

By hypothesis, we know that for all integers $c$, $a|bc$. Therefore we can take $c = 1$. We obtain $a|(b \cdot 1)$, that is to say $a|b$.

11.

The statement is of the form

$$\forall a \forall b \forall c \ (a|bc \rightarrow a|b)$$

Domain of $a : \mathbb{Z}^*$. Domain of $b, c : \mathbb{Z}$.
The statement is false. Here is a counter example.

$$\begin{aligned}
a = 2, b = 3, c = 2 \\
2 \mid 6, \quad 2 \nmid 3
\end{aligned}$$

13.

The statement is of the form

$$\forall a \forall b \forall c \ (a|c \to a|b \wedge b|c)$$

Domain of $a : \mathbb{Z}^*$. Domain of $b, c : \mathbb{Z}$.

The statement is false. Here is a counter example.

$$a = 2, b = 3, c = 2$$
$$2 \ |2, \quad 2 \not| \ 3 \wedge 3 \not| \ 2 \ \blacksquare$$

15.

The statement is of the form

$$\forall a \forall c \ (a|c \to \forall b \, (a|b \wedge b|c))$$

Domain of $a : \mathbb{Z}^*$. Domain of $b, c : \mathbb{Z}$.

The statement is false. Here is a counter example.

$$a = 2, b = 3, c = 2$$
$$2 \ |2, \quad 2 \not| \ 3 \wedge 3 \not| \ 2 \ \blacksquare$$

17.

The statement is of the form

$$\forall a \forall b \forall c \ (\forall m \forall n \, (a|(m \cdot b + n \cdot c)) \to a|b \wedge a|c)$$

Domain of $a : \mathbb{Z}^*$. Domain of $b, c, m, n : \mathbb{Z}$.

The statement is true. Here is a direct proof.

Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$.

By hypothesis, we know that for all integers $m$ and $n$, $a|(m \cdot b + n \cdot c)$. We can therefore take $m = 1$ and $n = 0$. We get $a|(1 \cdot b + 0 \cdot c)$, that is to say $a|b$.

We could also take $m = 0$ and $n = 1$. We get $a|(0 \cdot b + 1 \cdot c)$, that is to say $a|c$.

19.

The statement is of the form

$$\forall a \forall b \forall m \ \left(a^2 \equiv b^2 (\text{mod } m) \to a \equiv b (\text{mod } m)\right)$$

Domain of $a, b : \mathbb{Z}$. Domain of $m$ : integers $\geq 2$.

The statement is false. Here is a counter example.

Let's take $m = 4$, $a = 5$ and $b = 3$. We have

$$5^2 \equiv 25 \equiv 1 \equiv 9 \equiv 3^2 \pmod 4.$$

On the other hand,

$$5 \equiv 1 \not\equiv 3 \pmod 4.$$

21.

The statement is of the form

$$\forall a \forall b \forall c \forall m \ (ab \equiv 1 \pmod{m} \wedge ac \equiv 1 \pmod{m} \rightarrow b \equiv c \pmod{m})$$

Domain of $a, b, c : \mathbb{Z}$. Domain of $m$ : integers $\geq 2$.

The statement is true. Here is a direct proof.

Let $a, b, c \in \mathbb{Z}$ and the integer $m \geq 2$. Suppose that $ab \equiv 1 \pmod{m}$ $ac \equiv 1 \pmod{m}$. Therefore we have

$$b \equiv b \cdot 1 \equiv b \cdot (ac) \equiv c \cdot (ab) \equiv c \cdot 1 \equiv c \pmod{m}.$$