

Chapitre 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) $a \equiv 24 \pmod{31} \equiv -7 \pmod{31}$

Donc $a = -7$

(on note que $24 - 31 = -7$)

(b) $a \equiv 99 \pmod{41} \equiv 140 \pmod{41}$

Donc $a = 140$

(on note que $99 + 41 = 140$)

5.

Dans \mathbb{Z}_5 , l'inverse multiplicatif de 4 est 4. En effet, $4 \cdot 4 \pmod{5} = 16 \pmod{5} = 1 \pmod{5}$.

Dans \mathbb{Z}_6 , 4 n'a pas d'inverse multiplicatif. En effet,

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

Dans \mathbb{Z}_7 , l'inverse multiplicatif de 4 est 2. En effet, $4 \cdot 2 \pmod{7} = 8 \pmod{7} = 1 \pmod{7}$.

Dans \mathbb{Z}_8 , 4 n'a pas d'inverse multiplicatif. En effet,

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

Dans \mathbb{Z}_9 , l'inverse multiplicatif de 4 est 7. En effet, $4 \cdot 7 \pmod{9} = 28 \pmod{9} = 1 \pmod{9}$.

Dans \mathbb{Z}_{10} , 4 n'a pas d'inverse multiplicatif. En effet,

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

Dans \mathbb{Z}_{11} , l'inverse multiplicatif de 4 est 3. En effet, $4 \cdot 3 \pmod{11} = 12 \pmod{11} = 1 \pmod{11}$.

Dans \mathbb{Z}_{12} , 4 n'a pas d'inverse multiplicatif. En effet,

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

7. L'énoncé est de la forme

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

Domaine de $a : \mathbb{Z}^*$. Domaine de $b, c : \mathbb{Z}$.

L'énoncé est vrai. Voici une preuve directe : théorème vu en classe !

9.

L'énoncé est de la forme

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

Domaine de $a : \mathbb{Z}^*$. Domaine de $b, c : \mathbb{Z}$.

L'énoncé est vrai. Voici une preuve directe.

Soit $a, b \in \mathbb{Z}$ où $a \neq 0$.

Par hypothèse, on sait que pour tout entier c , $a|bc$. Donc on peut prendre $c = 1$. On obtient $a|(b \cdot 1)$, c'est-à-dire $a|b$.

11.

L'énoncé est de la forme

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

Domaine de $a : \mathbb{Z}^*$. Domaine de $b, c : \mathbb{Z}$.

L'énoncé est faux. Voici un contre-exemple.

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

13.

L'énoncé est de la forme

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

Domaine de $a : \mathbb{Z}^*$. Domaine de $b, c : \mathbb{Z}$.

L'énoncé est faux. Voici un contre-exemple.

$$a = 2, b = 3, c = 2 \\ 2 | 2, \quad 2 \nmid 3 \wedge 3 \nmid 2 \quad \blacksquare$$

15.

L'énoncé est de la forme

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

Domaine de $a : \mathbb{Z}^*$. Domaine de $b, c : \mathbb{Z}$.

L'énoncé est faux. Voici un contre-exemple.

$$a = 2, b = 3, c = 2 \\ 2 | 2, \quad 2 \nmid 3 \wedge 3 \nmid 2 \quad \blacksquare$$

17.

L'énoncé est de la forme

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

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

L'énoncé est vrai. Voici une preuve directe.

Soit $a, b, c \in \mathbb{Z}$ avec $a \neq 0$.

Par hypothèse, on sait que pour tout entier m et n , $a|(m \cdot b + n \cdot c)$. On peut donc prendre $m = 1$ et $n = 0$. On obtient $a|(1 \cdot b + 0 \cdot c)$, c'est-à-dire $a|b$.

On peut aussi prendre $m = 0$ et $n = 1$. On obtient $a|(0 \cdot b + 1 \cdot c)$, c'est-à-dire $a|c$.

19.

L'énoncé est de la forme

$$\forall a \forall b \forall m (a^2 \equiv b^2 \pmod{m} \rightarrow a \equiv b \pmod{m})$$

Domaine de $a, b : \mathbb{Z}$. Domaine de $m : \text{les entiers } \geq 2$.

L'énoncé est faux. Voici un contre-exemple.

Prenons $m = 4$, $a = 5$ et $b = 3$. On a

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

Par contre,

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

21.

L'énoncé est de la forme

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

Domaine de a, b, c : \mathbb{Z} . Domaine de m : les entiers ≥ 2 .

L'énoncé est vrai. Voici une preuve directe.

Soit $a, b, c \in \mathbb{Z}$ et un entier $m \geq 2$. Supposons que $ab \equiv 1 \pmod{m}$ $ac \equiv 1 \pmod{m}$.

On a donc

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