Chapitre 4.4
Solutions

1.

(a)

$$\begin{aligned} 9 &= 2 \cdot 4 + 1 \\ 4 &= 5 \cdot 1 + 0 \end{aligned}$$

Donc

$$\begin{aligned} 1 &= 9 - 2 \cdot 4 \\ 1 &\equiv -2 \cdot 4 \pmod 9. \end{aligned}$$

Donc

$$\overline{4} \pmod 9 \equiv -2 \pmod 9 \equiv 7 \pmod 9$$

(par convention on prend la valeur comprise entre 0 et $m - 1$).

(b)

$$\begin{aligned} 141 &= 7 \cdot 19 + 8 \\ 19 &= 2 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Donc

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (8 - 2 \cdot 3) \\ &= -1 \cdot 8 + 3 \cdot 3 \\ &= -1 \cdot 8 + 3 \cdot (19 - 2 \cdot 8) \\ &= 3 \cdot 19 - 7 \cdot 8 \\ &= 3 \cdot 19 - 7 \cdot (141 - 7 \cdot 19) \\ &= -7 \cdot 141 + 52 \cdot 19. \\ &\equiv 52 \cdot 19 \pmod{141}. \end{aligned}$$

Donc

$$\overline{19} \pmod{141} \equiv 52 \pmod{141}.$$

(c)

$$\begin{aligned}
232 &= 2 \cdot 89 + 54 \\
89 &= 1 \cdot 54 + 35 \\
54 &= 1 \cdot 35 + 19 \\
35 &= 1 \cdot 19 + 16 \\
19 &= 1 \cdot 16 + 3 \\
16 &= 5 \cdot 3 + 1 \\
3 &= 3 \cdot 1 + 0
\end{aligned}$$

Donc

$$\begin{aligned}
1 &= 16 - 5 \cdot 3 \\
&= 16 - 5 \cdot (19 - 1 \cdot 16) \\
&= -5 \cdot 19 + 6 \cdot 16 \\
&= -5 \cdot 19 + 6 \cdot (35 - 1 \cdot 19) \\
&= 6 \cdot 35 - 11 \cdot 19 \\
&= 6 \cdot 35 - 11 \cdot (54 - 1 \cdot 35) \\
&= -11 \cdot 54 + 17 \cdot 35 \\
&= -11 \cdot 54 + 17 \cdot (89 - 1 \cdot 54) \\
&= 17 \cdot 89 - 28 \cdot 54 \\
&= 17 \cdot 89 - 28 \cdot (232 - 2 \cdot 89) \\
&= -28 \cdot 232 + 73 \cdot 89. \\
&\equiv 73 \cdot 89 \pmod{232}.
\end{aligned}$$

Donc

$$\overline{89} \pmod{232} \equiv 73 \pmod{232}.$$

(d)

$$\begin{aligned}
1231 &= 6 \cdot 189 + 97 \\
189 &= 1 \cdot 97 + 92 \\
97 &= 1 \cdot 92 + 5 \\
92 &= 18 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Donc

$$\begin{aligned}
1 &= 5 - 2 \cdot 2 \\
&= 5 - 2 \cdot (92 - 18 \cdot 5) \\
&= -2 \cdot 92 + 37 \cdot 5 \\
&= -2 \cdot 92 + 37 \cdot (97 - 1 \cdot 92) \\
&= 37 \cdot 97 - 39 \cdot 92 \\
&= 37 \cdot 97 - 39 \cdot (189 - 1 \cdot 97) \\
&= -39 \cdot 189 + 76 \cdot 97 \\
&= -39 \cdot 189 + 76 \cdot (1231 - 6 \cdot 189) \\
&= 76 \cdot 1231 - 495 \cdot 189 \\
&\equiv -495 \cdot 189 \pmod{1231}.
\end{aligned}$$

Donc

$$\overline{189} \pmod{1231} \equiv -495 \pmod{1231} \equiv 736 \pmod{1231}.$$

(e)

$$\begin{aligned}
1232 &= 6 \cdot 189 + 98 \\
189 &= 1 \cdot 98 + 91 \\
98 &= 1 \cdot 91 + 7 \\
91 &= 13 \cdot 7 + 0.
\end{aligned}$$

Par l'algorithme d'Euclide, on trouve que $\gcd(1232, 189) = 7 \neq 1$. Le théorème qu'on a vu en classe nous garanti qu'un inverse existe si les deux nombres sont co-premiers. Ici, 1232 et 189 ne sont pas co-premiers. Donc le théorème ne s'applique pas !

Qu'est-ce qu'on fait ?

3.

Cette question est un prétexte pour vous faire pratiquer davantage. Prenons par exemple $a = 1041$ et $b = 244$.

(a)

$$\begin{aligned}
1041 &= 4 \cdot 244 + 65 \\
244 &= 3 \cdot 65 + 49 \\
65 &= 1 \cdot 49 + 16 \\
49 &= 3 \cdot 16 + 1 \\
16 &= 16 \cdot 1 + 0
\end{aligned}$$

(b)

$$\begin{aligned}1 &= 49 - 3 \cdot 16 \\ &= 49 - 3 \cdot (65 - 1 \cdot 49) \\ &= -3 \cdot 65 + 4 \cdot 49 \\ &= -3 \cdot 65 + 4 \cdot (244 - 3 \cdot 65) \\ &= 4 \cdot 244 - 15 \cdot 65 \\ &= 4 \cdot 244 - 15 \cdot (1041 - 4 \cdot 244) \\ &= -15 \cdot 1041 + 64 \cdot 244\end{aligned}$$

(c) On a donc

$$1 \equiv 64 \cdot 244 \pmod{1041},$$

donc

$$\overline{244} \pmod{1041} \equiv 64 \pmod{1041}.$$

(d) On a donc

$$1 \equiv -15 \cdot 1041 \pmod{244},$$

donc

$$\overline{1041} \pmod{244} \equiv -15 \pmod{244} \equiv 229 \pmod{244}.$$

5.

(a) On a $x = 6a + 3$ pour un entier a. Donc

$$\begin{aligned}6a + 3 &\equiv 4 \pmod{7} \\ 6a &\equiv 1 \pmod{7} \\ 6 \cdot 6a &\equiv 6 \cdot 1 \pmod{7} \\ 36a &\equiv 6 \pmod{7} \\ a &\equiv 6 \pmod{7}\end{aligned}$$

Donc $a = 7b + 6$ pour un entier b. On trouve donc

$$x = 6(7b + 6) + 3 = 42b + 39 \equiv 39 \pmod{6 \cdot 7}.$$

(b) On commence par simplifier le système. C'est plus simple si tous les coefficients sont des « 1 ». Le système

$$\begin{aligned}5x &\equiv 3 \pmod{6} \\ 4x &\equiv 4 \pmod{7}\end{aligned}$$

devient

$$\begin{aligned} 5 \cdot 5x &\equiv 5 \cdot 3 \pmod 6 \\ 2 \cdot 4x &\equiv 2 \cdot 4 \pmod 7, \end{aligned}$$

puis

$$\begin{aligned} 25x &\equiv 3 \pmod 6 \\ 8x &\equiv 1 \pmod 7, \end{aligned}$$

puis

$$\begin{aligned} x &\equiv 3 \pmod 6 \\ x &\equiv 1 \pmod 7. \end{aligned}$$

Donc $x = 6a + 3$ pour un entier a. Donc

$$\begin{aligned} 6a + 3 &\equiv 1 \pmod 7 \\ 6a &\equiv 5 \pmod 7 \\ 6 \cdot 6a &\equiv 6 \cdot 5 \pmod 7 \\ 36a &\equiv 2 \pmod 7 \\ a &\equiv 2 \pmod 7. \end{aligned}$$

Donc $a = 7b + 2$ pour un entier b. On trouve donc

$$x = 6a + 3 = 6(7b + 2) + 3 = 42b + 15 \equiv 15 \pmod{6 \cdot 7}.$$

(c) Si on prend $x = 1$, ça fonctionne !

Mais la question demande de procéder par substitution, alors voici comment on y arrive.

On a $x = 5a + 1$ pour un entier a. Donc

$$\begin{aligned} 5a + 1 &\equiv 1 \pmod 4 \\ 5a &\equiv 0 \pmod 4 \\ a &\equiv 0 \pmod 4. \end{aligned}$$

Donc $a = 4b$ pour un entier b. Donc $x = 5a + 1 = 5(4b) + 1 = 20b + 1$. Donc

$$\begin{aligned} 20b + 1 &\equiv 1 \pmod 3 \\ 2b &\equiv 0 \pmod 3 \\ 2 \cdot 2b &\equiv 0 \pmod 3 \\ 4b &\equiv 0 \pmod 3 \\ b &\equiv 0 \pmod 3. \end{aligned}$$

Donc $b = 3c$ pour un entier c. Donc

$$x = 20b + 1 = 20(3c) + 1 = 60c + 1 \equiv 1 \pmod{5 \cdot 4 \cdot 3}.$$

(d) Celui-ci est un petit peu plus difficile.

On pourrait essayer de simplifier le système. C'est plus simple si tous les coefficients sont des « 1 ». Par contre, il y a un problème : 2 n'a pas d'inverse dans $\mathbb{Z}_4$. Donc on ne peut pas simplifier $2x \equiv 2 \pmod 4$.
On peut simplifier la première équation :

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

Procédons maintenant par simplification. On a $x = 5a + 3$ pour un entier a. On a donc

$$\begin{aligned} 2(5a + 3) &\equiv 2 \pmod 4 \\ 10a &\equiv 0 \pmod 4 \\ 2a &\equiv 0 \pmod 4. \end{aligned}$$

Quelle est la solution à cette dernière congruence ? Si $2a \equiv 0 \pmod 4$, alors $2a$ est divisible par 4. Si $2a$ est divisible par 4, alors a est pair. Autrement dit, $a \equiv 0 \pmod 2$. On a donc $a = 2b$ pour un entier b.
On trouve $x = 5a + 3 = 5(2b) + 3 = 10b + 3$. On a donc

$$\begin{aligned} 10b + 3 &\equiv 1 \pmod 3 \\ 10b &\equiv 1 \pmod 3 \\ b &\equiv 1 \pmod 3. \end{aligned}$$

Donc $b = 3c + 1$ pour un entier c. On trouve

$$x = 10b + 3 = 10(3c + 1) + 3 = 30c + 13 \equiv 13 \pmod{5 \cdot 2 \cdot 3}.$$

On utilise $\pmod{5 \cdot 2 \cdot 3}$ et non pas $\pmod{5 \cdot 4 \cdot 3}$ parce que, comme on l'a vu, la deuxième congruence est équivalent à une congruence $\pmod 2$.

(e) Ici aussi, si on prend $x = 1$, ça fonctionne !

Mais la question demande de procéder par substitution, alors voici comment on y arrive.

On a $x = 4a + 1$ pour un entier a. Donc

$$\begin{aligned} 4a + 1 &\equiv 1 \pmod 9 \\ 4a &\equiv 0 \pmod 9 \\ 7 \cdot 4a &\equiv 7 \cdot 0 \pmod 9 \\ a &\equiv 0 \pmod 9 \end{aligned}$$

Donc $a = 9b$ pour un entier b. Donc $x = 4a + 1 = 4(9b) + 1 = 36b + 1$.
Donc

$$\begin{aligned} 36b + 1 &\equiv 1 \pmod{25} \\ 36b &\equiv 0 \pmod{25} \\ 16 \cdot 36b &\equiv 16 \cdot 0 \pmod{25} \\ b &\equiv 0 \pmod{25} \end{aligned}$$

Donc $b = 25c$ pour un entier c. On a donc

$$x = 36b + 1 = 36(25c) + 1 = 900c + 1 \equiv 1 \pmod{4 \cdot 9 \cdot 25}.$$

7.

(a) Il suffit de prendre $x \equiv 0 \pmod{101 \cdot 103 \cdot 107}$.

(b) Aucune méthode n'est imposée. Commençons par simplifier le système de congruences.

$$\begin{aligned} 2x &\equiv 1 \pmod 3 \\ 3x &\equiv 2 \pmod 4 \\ 4x &\equiv 3 \pmod 5 \end{aligned}$$

devient

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

qui devient

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 2 \pmod 5 \end{aligned}$$

Il s'agit de prendre $x \equiv 2 \pmod{3 \cdot 4 \cdot 5}$.

9.

(a) On note que $28 = 4 \cdot 7 \equiv 0 \pmod 7$.

$$\begin{aligned} & 28^{1000000} \pmod 7 \\ & \equiv 0^{1000000} \pmod 7 \\ & \equiv 0 \pmod 7 \end{aligned}$$

(b)

$$\begin{aligned} & 6^{778} \pmod 7 \\ & \equiv (-1)^{778} \pmod 7 \\ & \equiv 1 \pmod 7 \end{aligned}$$

car 778 est pair.

11.

(a)

$$2020! = 1 \cdot 2 \ldots 2019 \cdot 2020 \equiv 0 \pmod{10}$$

car 10 est un facteur alors le chiffre des unités est 0.

(b)

$$1^1 + 2^2 + 3^3 + 4^4 + \ldots 2019^{2019} + 2020^{2020}$$

(c) On voit que $3^4 = 81$ et $11^2 = 121$.

$$\begin{aligned} 3^{400} &= 3^{4 \cdot 100} \\ &\equiv 1^{100} \pmod{10} \\ 11^{400} &= 11^{2 \cdot 200} \\ &\equiv 1^{200} \pmod{10} \end{aligned}$$

Donc le chiffre des unités est $1 + 1 = 2$.

13. L'énoncé est vrai. Voici une preuve par contradiction.
Soit $d = \text{pgcd}(a, m)$. Par hypothèse, on a $d > 1$. On a donc $a = d\,k$ pour un entier k et $m = d\,\ell$ pour un entier ℓ. Supposons que a admet un inverse multiplicatif $\overline{a} \pmod m$. Donc

$$\begin{aligned} m &\equiv 0 \pmod m \\ d\,\ell &\equiv 0 \pmod m \\ k\,d\,\ell &\equiv 0 \pmod m \\ a\,\ell &\equiv 0 \pmod m \\ \overline{a}\,a\,\ell &\equiv 0 \pmod m \\ 1\,\ell &\equiv 0 \pmod m \\ \ell &\equiv 0 \pmod m. \end{aligned}$$

Donc ℓ est divisible par m. Mais m est divisible par ℓ. Donc $m = \ell$. Donc $m = dm$, c'est-à-dire que $d = 1$. C'est une contradiction.

15. L'énoncé est vrai. Voici une preuve directe :
    Si $\gcd(a, p) \neq 1$, alors $p|a$.

$$\begin{aligned} & a^{p-1} \pmod{p} \\ & \equiv 0^{p-1} \pmod{p} \\ & \equiv 0 \pmod{p} \\ & \not\equiv 1 \pmod{p} \end{aligned}$$