Section 4.4

1. Trouver l'inverse de $a \pmod{m}$ pour chacune de ces paires d'entiers à l'aide de Euclide et Bézout.
   (a) $a = 4$, $m = 9$
   (b) $a = 19$, $m = 141$
   (c) $a = 89$, $m = 232$
   (d) $a = 189$, $m = 1231$
   (e) $a = 189$, $m = 1232$
2. Résoudre les congruences suivantes (l'exercice précédent pourrait être utile).
   (a) $4x \equiv 2 \pmod{9}$
   (b) $19x \equiv 12 \pmod{141}$
   (c) $89x \equiv 22 \pmod{232}$
   (d) $189x \equiv 32 \pmod{1231}$
   (e) $189x \equiv 42 \pmod{1232}$
3. Prendre deux nombres a et b.
   (a) Trouver $\text{pgcd}(a, b)$ à l'aide de l'algorithme d'Euclide.
   (b) Trouver $s, t \in \mathbb{Z}$ tels que $sa + tb = \text{pgcd}(a, b)$.
   (c) Est-ce que a admet un inverse $\pmod{b}$? Si oui, quel est-il ?
   (d) Est-ce que b admet un inverse $\pmod{a}$? Si oui, quel est-il ?
4. Refaire l'exercice précédent avec deux autres nombres a et b.
5. Résoudre les systèmes de congruence suivants en utilisant la méthode par substitution.
   (a)

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

   (b)

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

   (c)

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

(d)

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

(e)

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 1 \pmod 9 \\ x &\equiv 1 \pmod{25} \end{aligned}$$

6. Résoudre les systèmes de congruence suivants en utilisant le théorème du reste chinois.
   (a)

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

   (b)

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

   (c)

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 1 \pmod 9 \\ x &\equiv 1 \pmod{25} \end{aligned}$$

   (d)

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod{11} \end{aligned}$$

7. Résoudre les systèmes de congruence suivants.
   (a)

$$\begin{aligned} x &\equiv 0 \pmod{101} \\ x &\equiv 0 \pmod{103} \\ x &\equiv 0 \pmod{107} \end{aligned}$$

(b)

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

8. Simplifier les expressions suivantes au maximum.
   (a) $7^{121} \pmod{13}$
   (b) $23^{1002} \pmod{41}$
9. Simplifier les expressions suivantes au maximum.
   (a) $28^{1000000} \pmod 7$
   (b) $6^{778} \pmod 7$
10. Répondre à cette question à l'aide d'un ordinateur.
    (a) Trouver deux pseudo-premiers base 2.
    (b) Trouver trois pseudo-premiers base 3.
    (c) Trouver quatre pseudo-premiers base 4.
11. Trouver le chiffre des unités dans les nombres suivants.
    (a) 2020!
    (b) $1^1 + 2^2 + 3^3 + 4^4 + 5^5 + ... + 2019^{2019} + 2020^{2020}$
    (c) $3^{400} + 11^{400}$
12. Soit $a, m \in \mathbb{Z}$ avec $m \geq 2$ et $0 < a < m$. Supposons que $\text{pgcd}(a, m) = d > 1$. Trouver une solution à la congruence linéaire suivante

$$a \cdot x \equiv a \pmod m.$$

    Votre solution doit satisfaire $0 \leq x < m$.
13. Vrai ou faux ? Démontrer. Si $\text{pgcd}(a, m) \neq 1$, alors l'inverse de $a \pmod m$ n'existe pas.
14. Vrai ou faux ? Démontrer. Soit $m_1, m_2, ..., m_r \in \mathbb{Z}$ des entiers positifs. Supposons qu'il existe i et j avec $1 \leq i < j \leq r$ tels que m_i et m_j ne sont pas copremiers. Alors le système

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

    n'admet pas de solution.
15. Vrai ou faux ? Démontrer. Soit $p \in \mathbb{Z}$ un premier et $a \in \mathbb{Z}$ tels que $\text{pgcd}(a, p) \neq 1$. Alors $a^{p-1} \not\equiv 1 \pmod p$.
16. Vrai ou faux ? Démontrer. Soit $a, m \in \mathbb{Z}$ tels que $\text{pgcd}(a, m) = 1$. Si m n'est pas premier, alors $a^{m-1} \not\equiv 1 \pmod m$.