Section 4.4

1. Find the inverse of $a \pmod{m}$ for each of the following pairs of integers through Euclid and 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. Solve the following congruences (the previous exercise could be useful).
   (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. Take two numbers a and b.
   (a) Find $\gcd(a, b)$ using Euclid's algorithm.
   (b) Find $s, t \in \mathbb{Z}$ such that $sa + tb = \gcd(a, b)$.
   (c) Does a admit and inverse $\pmod{b}$? If yes, what is it?
   (d) Does b admit and inverse $\pmod{b}$? If yes, what is it?
4. Redo the previous exercise with two different numbers a and b.
5. Solve the following systems of congruences by using the substitution method.
   (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. Solve the following systems of congruences by using the chinese remainder theroem.

(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. Solve the following systems of congruences.

(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. Simplify the following expressions as much as possible.
   (a) $7^{121} \pmod{13}$
   (b) $23^{1002} \pmod{41}$
9. Simplify the following expressions as much as possible.
   (a) $28^{1000000} \pmod 7$
   (b) $6^{778} \pmod 7$
10. Answer these questions with the help of a computer.
    (a) Find two pseudo-primes base 2.
    (b) Find three pseudo-primes base 3.
    (c) Find four pseudo-primes base 4.
11. Find the last digit of the following numbers.
    (a) 2020!
    (b) $1^1 + 2^2 + 3^3 + 4^4 + 5^5 + ... + 2019^{2019} + 2020^{2020}$
    (c) $3^{400} + 11^{400}$
12. Let $a, m \in \mathbb{Z}$ with $m \geq 2$ and $0 < a < m$. Suppose that $\gcd(a, m) = d > 1$. Find a solution to the following linear congruence

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

    Your solution must satisfy $0 \leq x < m$.
13. True or false? Demonstrate. If $\gcd(a, m) \neq 1$, then the inverse of $a \pmod m$ does not exist.
14. True or false? Demonstrate. Let $m_1, m_2, ..., m_r \in \mathbb{Z}$ be positive integers. Suppose there exist i and j with $1 \leq i < j \leq r$ such that m_i and m_j and not co-prime. Then the system

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

    does not have a solution.
15. True or false? Demonstrate. Let $p \in \mathbb{Z}$ a prime and $a \in \mathbb{Z}$ such that $\gcd(a, p) \neq 1$. Then $a^{p-1} \not\equiv 1 \pmod p$.
16. True or false? Demonstrate. Let $a, m \in \mathbb{Z}$ such that $\gcd(a, m) = 1$. If m is not prime, then $a^{m-1} \not\equiv 1 \pmod m$.