Section 4.1

1. Suppose a and b are integers, $a \equiv 4 \pmod{13}$ and $b \equiv 9 \pmod{13}$. Find the integer c where $0 \leq c \leq 12$ such that
   (a) $c = 9a \pmod{13}$
   (b) $c = 2a + 3b \pmod{13}$
   (c) $c = a^3 - b^3 \pmod{13}$
2. Find a **div** m and a **mod** m when
   (a) $a = 228$ and $m = 119$.
   (b) $a = 9009$ and $m = 223$.
   (c) $a = -10101$ and $m = 333$.
3. Find the integer a such that
   (a) $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$.
   (b) $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$.
4. Find the set of all values from $\mathbb{Z}_m$ that satisfy the following equations.
   (a) $x \equiv -1 \pmod{6}$
   (b) $3x \equiv 4 \pmod{17}$
   (c) $2x + 7 \equiv 4x \pmod{27}$
   (d) $3x^2 + 5x \equiv 8 \pmod{4}$
5. Find a multiplicative inverse to 4 in $\mathbb{Z}_m$ for $5 \leq m \leq 12$. If such an inverse does not exist, show that it does not exist.
6. (a) State a criterion of divisibility by 2 and demonstrate that it works.
   (b) State a criterion of divisibility by 3 and demonstrate that it works.
   (c) State a criterion of divisibility by 4 and demonstrate that it works.
   (d) State a criterion of divisibility by 5 and demonstrate that it works.
   (e) State a criterion of divisibility by 7 and demonstrate that it works.
   (f) State a criterion of divisibility by 9 and demonstrate that it works.
   (g) State a criterion of divisibility by 10 and demonstrate that it works.
   (h) State a criterion of divisibility by 11 and demonstrate that it works.

For each of the following statements,

— Write the statement using quantifiers and logical operators.

— Determine if the statement is true or false.

— Prove that your reponse is correct.

— Indicate the method of proof used.

7. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a|b$ and $a|c$, then $a|(b+c)$.
8. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a|(b+c)$, then $a|b$ and $a|c$.
9. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If for any integer c, $a|bc$, then $a|b$.
10. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a|b$, then $a|bc$ for any integer c.
11. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a|bc$, then $a|b$.
12. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If there exists an integer c such that $a|bc$, then $a|b$.
13. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a|c$, then $a|b$ and $b|c$.
14. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a|c$, then there exists an integer b such that $a|b$ and $b|c$.
15. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a|c$, then for any integer b, $a|b$ and $b|c$.
16. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a|b$ and $b|c$, then $a|c$.
17. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a|(m \cdot b + n \cdot c)$ for all integers m and n, then $a|b$ and $a|c$.
18. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If there exist integers m and n such that $a|(m \cdot b + n \cdot c)$, then $a|b$ and $a|c$.
19. Let $a, b \in \mathbb{Z}$. If $a^2 \equiv b^2 \pmod{m}$, then $a \equiv b \pmod{m}$.
20. Let $a, b \in \mathbb{Z}$. If $a \equiv b \pmod{m}$, then $a^2 \equiv b^2 \pmod{m}$.
21. Let $a, b, c \in \mathbb{Z}_m$ such that $ab \equiv 1 \pmod{m}$ and $ac \equiv 1 \pmod{m}$. Then $b \equiv c \pmod{m}$.
22. Demonstrate the properties of closure, associativity, commutativity, identity, additive inverses and distributivity of $+_m$ and $\cdot_m$ in $\mathbb{Z}_m$.