Definitions

1. Natural Numbers: $\{1, 2, 3, 4, ...\}$

2. Integers: $\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$

3. Suppose a and d are integers. Then d *divides* a, denoted $d|a$, if and only if there is an integer k such that $a = kd$.

4. Suppose that a, b, and n are integers, with $n > 0$. We say that a and b are *congruent modulo* n if and only if $n|(a - b)$. We denote this relationship as $a \equiv b \pmod{n}$ and read these symbols as a *is congruent to* b *modulo* n.

Exercises

1.1 Theorem. *Let a, b, and c be integers. If $a|b$ and $a|c$, then $a|(b+c)$.*

Proof: Suppose a, b, and c to be integers such that $a|b$ and $a|c$. By definition of divides, $b = ka$ for some $k \in \mathbb{Z}$ and $c = la$ for some $l \in \mathbb{Z}$. By substitution, $b + c = ka + la = a(k + l)$. Because integers are closed under addition, then $(k+l) \in \mathbb{Z}$. Therefore, by definition of divides, $a|(b+c)$. □

1.2 Theorem. *Let a, b, and c be integers. If $a|b$ and $a|c$, then $a|(b-c)$.*

Proof: Suppose a, b, and c to be integers such that $a|b$ and $a|c$. By definition of divides, $b = ka$ for some $k \in \mathbb{Z}$ and $c = la$ for some $l \in \mathbb{Z}$. By substitution, $b - c = ka - la = a(k - l)$. Because integers are closed under addition, then $(k-l) \in \mathbb{Z}$. Therefore, by definition of divides, $a|(b-c)$. □

1.3 Theorem. *Let a, b, and c be integers. If $a|b$ and $a|c$, then $a|bc$.*

Proof: Suppose a, b, and c to be integers such that $a|b$ and $a|c$. By definition of divides, $b = ka$ for some $k \in \mathbb{Z}$ and $c = la$ for some $l \in \mathbb{Z}$. By substition, $bc = (ka) \cdot (la) = a \cdot (akl)$. Because integers are closed under multiplication, then $akl \in \mathbb{Z}$. Therefore, by definition of divides, $a|bc$. □

1.4a Question. *Can you weaken the hypothesis of the previous theorem and still prove the conclusion?*

Answer: Yes, a only needs to divide b or c instead of b and c.

1.4b Question. *Can you keep the same hypothesis, but replace the conclusion by the stronger conclusion that $a^2|bc$ and still prove the theorem?*

Answer: Yes, you can.

1.5 Theorem. *Let a, b, and c be integers. If $a|b$ and $a|c$, then $a^2|bc$.*

Proof: Suppose a, b, and c to be integers such that $a|b$ and $a|c$. By definition of divides, $b = ka$ for some $k \in \mathbb{Z}$ and $c = la$ for some $l \in \mathbb{Z}$. By substition, $bc = (ka) \cdot (la) = a^2 \cdot (kl)$. Because integers are closed under multiplication, then $kl \in \mathbb{Z}$. Therefore, by definition of divides, $a^2|bc$. □

1.6 Theorem. *Let a, b, and c be integers. If $a|b$, then $a|bc$.*

Proof: Suppose a, b, and c to be integers such that $a|b$. By definition of divides, $b = ka$ for some $k \in \mathbb{Z}$. By substitution, $bc = (ka) \cdot c = a \cdot (kc)$. Because integers are closed under multiplication, then $kc \in \mathbb{Z}$. Therefore, by definition of divides, $a|bc$. □

1.7 Exercise. *Answer each of the following questions, and prove that your answer is correct.*
1. Is $45 \equiv 9 \pmod 4$*?* Yes, $4|(45-9)$.
2. Is $37 \equiv 2 \pmod 5$*?* Yes, $5|(37-2)$.
3. Is $37 \equiv 3 \pmod 5$*?* No, $5 \not| (37-3)$.
4. Is $37 \equiv$ -3 $\pmod 5$*?* Yes, $5|(37-(-3))$.

1.8 Exercise. *For each of the following congruences, characterize all the integers m that satisfy that congruence.*
1. $m \equiv 0 \pmod 3$. $\quad m = 3k \quad k \in \mathbb{Z}$
2. $m \equiv 1 \pmod 3$. $\quad m = 3k+1 \quad k \in \mathbb{Z}$
3. $m \equiv 2 \pmod 3$. $\quad m = 3k+2 \quad k \in \mathbb{Z}$
4. $m \equiv 3 \pmod 3$. $\quad m = 3k \quad k \in \mathbb{Z}$
5. $m \equiv 4 \pmod 3$. $\quad m = 3k+1 \quad k \in \mathbb{Z}$

1.9 Theorem. *Let a and n be integers with $n > 0$. Then $a \equiv a \pmod n$.*

Proof: Suppose a and n be integers with $n > 0$. By algebra, $a - a = 0 = n \cdot 0$. So, by definition of divides, $n|(a-a)$. Therefore, by definition of congruence, $a \equiv a \pmod n$ $\square$

1.10 Theorem. *Let a, b, and n be integers with $n > 0$. If $a \equiv b \pmod n$, then $b \equiv a \pmod n$.*

Proof: Suppose a and n be integers with $n > 0$ such that $a \equiv b \pmod n$. By definition of congruence, $n|(a-b)$. By definition of divides, $a - b = nk$ where $k \in \mathbb{Z}$. Multiplying both sides by -1, $b - a \equiv n(-k)$. Since integers are closed under multiplication, $(-k) \in \mathbb{Z}$. Hence, $n|(b-a)$ by definition of divides. Therefore, $b \equiv a \pmod n$. $\square$

1.11 Theorem. *Let a, b, c, and n be integers with $n > 0$. If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.*

Proof: Suppose a, b, c, and n to be integers with $n > 0$ such that $a \equiv b \pmod n$ and $b \equiv c \pmod n$. By definition of congruence, $n|(a-b)$ and $n|(b-c)$. By definition of divides, $a - b = kn$ where $k \in \mathbb{Z}$ and $b - c = ln$ where $l \in \mathbb{Z}$. By substitution, $a - c = (a-b)+(b-c) = kn + ln = n(k+l)$. Since integers are closed under addition, $(k+l) \in \mathbb{Z}$. Thus, by definition of divides, $n|(a-c)$. Therefore, by definition of congruence, $a \equiv c \pmod n$. $\square$