

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

Proof: By definition of divides

□

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

Proof:

□

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

Proof:

□

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:

□

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

Proof:

□

1.7 Exercise. *Answer each of the following questions, and prove that your answer is correct.*

1. *Is $45 \equiv 9 \pmod{4}$?*
2. *Is $37 \equiv 2 \pmod{5}$?*
3. *Is $37 \equiv 3 \pmod{5}$?*
4. *Is $37 \equiv -3 \pmod{5}$?*

1.8 Exercise. *For each of the following congruences, characterize all the integers m that satisfy that congruence.*

1. $m \equiv 0 \pmod{3}$. $m = 3k \quad k \in \mathbb{Z}$
2. $m \equiv 1 \pmod{3}$. $m = 3k + 1 \quad k \in \mathbb{Z}$
3. $m \equiv 2 \pmod{3}$. $m = 3k + 2 \quad k \in \mathbb{Z}$
4. $m \equiv 3 \pmod{3}$. $m = 3k \quad k \in \mathbb{Z}$
5. $m \equiv 4 \pmod{3}$. $m = 3k + 1 \quad k \in \mathbb{Z}$

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

Proof:

□

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:

□

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:

□