Geoffrey Parker - grp352
HW 1: 1.1 - 1.3, 1.6 - 1.14
M328K
January 19th, 2012

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

Proof. Let a, b, and c be integers where $a|b$ and $a|c$. We will show that, given this, $a|(b+c)$. Since $a|b$ and $a|c$, then by the definition of divides $b = aj$ and $c = ak$ for some integers j and k. Therefore $b + c = aj + ak$ and $b + c = a(j + k)$. Because j and k are both integers, $j + k$ is also an integer. So by the definition of divides, $a|(b+c)$. $\square$

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

Proof. Let a, b, and c be integers where $a|b$ and $a|c$. We will show that, given this, $a|(b-c)$. Since $a|b$ and $a|c$, then by the definition of divides $b = aj$ and $c = ak$ for some integers j and k. Therefore $b - c = aj - ak$ and $b - c = a(j - k)$. Because j and k are both integers, $j - k$ is also an integer. So by the definition of divides, $a|(b-c)$. $\square$

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

Proof. Let a, b, and c be integers where $a|b$ and $a|c$. We will show that, given this, $a|bc$. Since $a|b$ and $a|c$, then by the definition of divides $b = aj$ and $c = ak$ for some integers j and k. Therefore $bc = ajak$ and $b + c = a(ajk)$. Because a, j, and k are all integers, ajk is also an integer. So by the definition of divides, $a|bc$. $\square$

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

Proof. Let a, b, and c be integers where $a|b$. We will show that $a|bc$. Since $a|b$, then by the definition of divides $b = ak$ for some integer k. Therefore $bc = akc$. Because k and c are both integers, kc is also an integer. So by the definition of divides, $a|bc$. $\square$

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

(1) Is $45 \equiv 9 \pmod 4$?
Yes.

Proof. $45 - 9 = 36$. $36 = 4 \times 9$. Therefore $4|36$. So by the definition of congruence, $45 \equiv 9 \pmod 4$. $\square$

(2) Is $37 \equiv 2 \pmod 5$?
Yes.

Proof. $37 - 2 = 35$. $35 = 5 \times 7$. Therefore $5|35$. So by the definition of congruence, $37 \equiv 2 \pmod 5$. $\square$

(3) Is $37 \equiv 3 \pmod 5$?
No.

Proof. $37 - 3 = 34$. $5 \times 6 = 30$ and $5 \times 7 = 35$. Since $30 < 34 < 35$, there is no integer x such that $5 \times x = 34$. Therefore by the definition of divides, $5 \nmid 34$. So by the definition of congruence, $37 \not\equiv 3 \pmod 5$. $\square$

(4) Is $31 \equiv -3 \pmod 5$?
No.

Proof. $31 - (-3) = 34$. $5 \times 6 = 30$ and $5 \times 7 = 35$. Since $30 < 34 < 35$, there is no integer x such that $5 \times x = 34$. Therefore by the definition of divides, $5 \nmid 34$. So by the definition of congruence, $31 \not\equiv -3 \pmod 5$. $\square$

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

(1) $m \equiv 0 \pmod 3$.

Solution. This is satisfied when $m = 3n$ for any integer n. $\square$

(2) $m \equiv 1 \pmod 3$.

Solution. This is satisfied when $m = 3n + 1$ for any integer n. □

(3) $m \equiv 2 \pmod 3$.

Solution. This is satisfied when $m = 3n + 2$ for any integer n. □

(4) $m \equiv 3 \pmod 3$.

Solution. This is satisfied when $m = 3n$ for any integer n. □

(5) $m \equiv 4 \pmod 3$.

Solution. This is satisfied when $m = 3n + 1$ for any integer n. □

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

Proof. Let a and n be integers with $n > 0$. We will show that $a \equiv a \pmod n$. To start with, $a - a = 0$. Since all integers divide 0, $n \mid (a - a)$. Therefore, by definition of congruence, $a \equiv a \pmod n$. □

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. Let a, b, and n be integers with $n > 0$ and $a \equiv b \pmod n$. We will show that $b \equiv a \pmod n$. Since $a \equiv b \pmod n$, then by definition of congruence, $n|(a - b)$. This in turn means, by definition of divides, that $a - b = nk$ for some integer k. From here, we can say that $b - a = -(a - b) = -(nk) = n(-k)$. Since k is an integer, $-k$ is also an integer. Therefore $n|(b - a)$, which means that $b \equiv a \pmod n$. □

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. Let a, b, c, and n be integers with $n > 0$, $a \equiv b \pmod n$, and $b \equiv c \pmod n$. We will show $a \equiv c \pmod n$. By definition of congruence, we have $n|(a - b)$ and $n|(b - c)$. By definition of divides, this gives us $a - b = nj$ and $b - c = nk$ for some integers j and k. So $a - c = (a - b) + (b - c) = nj + nk = n(j + k)$. Since j and k are integers, $j + k$ is also an integer. Therefore $n|(a - c)$, which means that $a \equiv c \pmod n$. □

1.12 Theorem. *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.*

Proof. Let a, b, c, d, and n be integers with $n > 0$, $a \equiv b \pmod{n}$, and $c \equiv d \pmod{n}$. We will show that $a+c \equiv b+d \pmod{n}$. By definition of congruence, we have $n|(a-b)$ and $n|(c-d)$. By definition of divides, this gives us $a - b = nj$ and $c - d = nk$ for some integers j and k. So $(a + c) - (b + d) = (a - b) + (c - d) = nj + nk = n(j + k)$. Since j and k are integers, $j+k$ is also an integer. Therefore $n|(a+c)-(b+d)$, which means that $a + c \equiv b + d \pmod{n}$. $\square$

1.13 Theorem. *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$.*

Proof. Let a, b, c, d, and n be integers with $n > 0$, $a \equiv b \pmod{n}$, and $c \equiv d \pmod{n}$. We will show that $a-c \equiv b-d \pmod{n}$. By definition of congruence, we have $n|(a-b)$ and $n|(c-d)$. By definition of divides, this gives us $a-b = nj$ and $c-d = nk$ for some integers j and k. So $(a - c) - (b - d) = -(a - b) - (c - d) = -nj - nk = n(-j - k)$. Since j and k are integers, $-j - k$ is also an integer. Therefore $n|(a - c) - (b - d)$, which means that $a - c \equiv b - d \pmod{n}$. $\square$

1.14 Theorem. *Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.*

Proof. Let a, b, c, d, and n be integers with $n > 0$, $a \equiv b \pmod{n}$, and $c \equiv d \pmod{n}$. We will show that $ac \equiv bd \pmod{n}$. By definition of congruence, we have $n|(a - b)$ and $n|(c - d)$. By definition of divides, this gives us $a - b = nj$ and $c - d = nk$ for some integers j and k. So, $ac - bd = n(dj + bk + jkn)$ Since b, d, j, k, and n are all integers, $dj + bk + jkn$ is also an integer. Therefore $n|ac - bd$, which means that $ac \equiv bd \pmod{n}$. $\square$