4.1 Divisibility and Modular Arithmetic

Divides

$a \mid b$ means "a divides b". That is, there exists an integer c such that $b = ac$. If $a \mid b$, then b/a is an integer.
If a does not divide b, we write $a \nmid b$.

Properties of Divisibility

Let a, b, and c be integers where $a \neq 0$.

- $a \mid 0$
- $(a \mid b \wedge a \mid c) \rightarrow a \mid (b + c)$
- $a \mid b \rightarrow a \mid bc$ for all integer c
- $(a \mid b \wedge b \mid c) \rightarrow a \mid c$

Division Algorithm

If $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, then there are unique integers q and r, with $0 \leq r < d$, such that $a = d \cdot q + r$.

- d is called the divisor
- a is called the dividend
- q is called the quotient
- r is called the remainder

Mod and Div

$a \mod d = r$ **Note that the remainder is non-negative, and less than the divisor**
$a \text{ div } d = q$

Modular Congruence

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then a is congruent to b modulo m if and only if $m \mid (a - b)$.
Written as $a \equiv b \pmod{m}$
m is called the modulus

Two integers are congruent mod m if and only if they have the same remainder when divided by m.
If $a \equiv b \pmod{m}$, then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is an integer.
If $a \equiv b \pmod{m}$, then $c + a \equiv c + b \pmod{m}$, where c is an integer.

4.1 pg 244 # 21

Evaluate these quantities.

a) $13 \mod 3$

$13 = 3 \cdot 4 + 1$
$13 \mod 3 = 1$

b) $-97 \mod 11$

$-97 = 11 \cdot (-9) + 2$
$-97 \mod 11 = 2$

c) $155 \mod 19$

$155 = 19 \cdot 8 + 3$
$155 \mod 19 = 3$

d) $-221 \mod 23$

$-221 = 23 \cdot (-10) + 9$
$-221 \mod 23 = 9$

4.1 pg 244 # 13

Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integers c with $0 \leq c \leq 12$ such that

a) $c \equiv 9a \pmod{13}$.

$c \equiv 9(4) \pmod{13}$
$c \equiv 36 \pmod{13}$
$10 \equiv 36 \pmod{13}$ because $36 = 13 \cdot 2 + 10$
$c = 10$

b) $c \equiv 11b \pmod{13}$.

$c \equiv 11(9) \pmod{13}$
$c \equiv 99 \pmod{13}$
$8 \equiv 99 \pmod{13}$ because $99 = 13 \cdot 7 + 8$
$c = 8$

c) $c \equiv a + b \pmod{13}$.

$c \equiv 4 + 9 \pmod{13}$
$c \equiv 13 \pmod{13}$
$0 \equiv 13 \pmod{13}$ because $13 = 13 \cdot 1 + 0$
$c = 0$

4.1 pg 245 # 29

Decide whether each of these integers is congruent to 5 modulo 17.

a) 80

$80 = 17 \cdot 4 + 12$ (Also, we see that 17 does not divide $80 - 5$)
No

b) 103

$103 = 17 \cdot 6 + 1$ (Also, we see that 17 does not divide $103 - 5$)
No

c) -29

$-29 = 17 \cdot (-2) + 5$ (Also, we see that 17 divides $-29 - 5$)
Yes

d) -122

$-122 = 17 \cdot (-8) + 14$ (Also, we see that 17 does not divide $-122 - 5$)
No