Math-42 Worksheet #13

Divisibility and Modular Arithmetic

1. Determine whether the following propositions are true or false. Use the division algorithm to prove your answer.
   (a) $2 \mid 10$
   (b) $-2 \mid 10$
   (c) $2 \mid -10$
   (d) $-2 \mid -10$
   (e) $5 \mid 5$
   (f) $10 \mid 2$
   (g) $2 \mid 11$
   (h) $17 \mid 51$
   (i) $11 \mid 126$
   (j) $5 \mid 0$
   (k) $0 \mid 5$
   (l) $0 \mid 0$

2. You were told repeated in elementary school that you cannot divide by 0. Using the number theory definition of *divides*, is it true that 0 does not divide anything?

3. One of your friends claims that the uniqueness part of the division algorithm is not true. As a supposed counterexample, they provide you with the following two expansions of 11 with divisor 5:

$$11 = 5 * 2 + 1$$
$$11 = 5 * 1 + 6$$

   What is wrong with their argument?

4. Determine the division algorithm expansion of each the following using divisor 13. For each, indicate which value is $(n \operatorname{div} 13)$ and which value is $(n \bmod 13)$.

   (a) 117

   (b) -117

   (c) 100

   (d) -100

   (e) 0

   (f) 13

   (g) -13

   (h) 5

   (i) -5

5. There are two possible definitions for $a \equiv b \pmod{n}$:

   - $n \mid (a - b)$
   - $(a \bmod n) = (b \bmod n)$

   In this exercise we will prove that these definitions are equivalent:

   $$(a \bmod n) = (b \bmod n) \iff n \mid (a - b)$$

   Since this is an equivalence, we need to prove both directions.

   (a) First, prove the forward (easier) direction:

   $$(a \bmod n) = (b \bmod n) \implies n \mid (a - b)$$

   (Hint: write a and b as division algorithm expansions)

   (b) Next, prove the reverse direction:

   $$n \mid (a - b) \implies (a \bmod n) = (b \bmod n)$$

   This direction is a bit trickier. Start by writing a and b as division algorithm expansions:

   $$a = q_1 n + r_1$$
   $$b = q_2 n + r_2$$

   Next, subtract them: $a - b$. You can assume without loss of generality that $r_1 \geq r_2$. So what do we know about r_1 and r_2 and what does this mean for $r_1 - r_2$? Now, using the hypothesis $n \mid (a - b)$ and the uniqueness of the division algorithm, this should lead you to a conclusion about $r_1 - r_2$.

6. Evaluate the following:

   (a) $((1000 \bmod 39) + (500 \bmod 39)) \bmod 39$

   (b) $((-100 \bmod 23) + (100 \bmod 23)) \bmod 23$

   (c) $(10^4 \bmod 21)^3 \bmod 25$

   (d) $(-10^4 \bmod 21)^3 \bmod 25$