WORKSHEET 7

Date: 10/25/2022

Name:

Definitions and statements

DEFINITION 1. Let $a, b \in \mathbb{Z}$ where a is non-zero. We say a **divides** b if

$$b = a \cdot c \text{ for some integer } c.$$

When a divides b, we write $a|b$.

THEOREM 1 (The Division Algorithm)**.** *For positive integers a and b, there exists unique integers q and r such that*

$$b = aq + r \ \textit{ where } 0 \leq r < a.$$

DEFINITION 2. Let n be a positive integer. For $a, b \in \mathbb{Z}$, if n divides $a - b$, we say that a is **congruent to** b **modulo** n. written as

$$a \equiv b \pmod{n}$$

PROPOSITION 2. *Let n, k be positive integers, and $a, b \in \mathbb{Z}$. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.*

Practice Problems

1. Label each of the following *true* or *false*, and justify your answer.

   (a) $8|0$.

   (b) $a|b$ and $b|c \Rightarrow a|c$.

   (c) $a|b$ and $a|c \Rightarrow a|bc$.

   (d) $a|b \Rightarrow -a|b$.

   (e) $a|bc \Rightarrow b|c$ or $c|a$.

2. Let a and b be non zero integers. Prove the following statements.

   (a) If $a|b$ and $b|a$, then $a = \pm b$.

   (b) If $a|b$, then $|a| \leq |b|$.

3. Assume n is a non negative integer. Prove $4|(n-2)(n-1)n(n+1)$.

   Hint: Don't use induction here.

4. Find each congruence. Remember we are asking what is $r \equiv a \pmod{n}$ where $0 \leq r < n$.

   (a) What is 16 mod 12?

   (b) What is 51 mod 2?

   (c) What is 2^5 mod 41?

   (d) What is -9 mod 41?

   (e) Show $41 | (2^{20} - 1)$

5. Suppose a, b, c, d are integers with a and c different from zero. Prove that if $a|b$ and $c|d$, then $ac|(ad+bc)$.

   (a) First, what does it mean for a to divide b, and c to divide d?

   (b) Next, what do you want to show? i.e. what does it mean for $ac|(ad+bc)$?

   (c) Lastly, give your proof of the statement.