WORKSHEET 8

Date: 10/27/2022

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 $a^k \equiv b^k \pmod{n}$.*

DEFINITION 3. The **greatest common divisor** of integers a and b, denoted $\gcd(a, b)$, is the largest integer that divides both a and b.

Practice Problems

1. Suppose the division algorithm is applied to a and b yields $a = bq + r$. prove $\gcd(a,b) = \gcd(r,b)$.

2. If integers a and b are not both zero, then $\gcd(a,b) = \gcd(a-b,b)$.

3. If $n \in \mathbb{Z}$, then $\gcd(n,n+2) \in \{1,2\}$

4. Show that for any integer k, $\gcd(9k+4, 2k+1) = 1$.

5. Suppose a and b are integers. Then $a \equiv b \pmod 6$ if and only if $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$

6. Find the reminder obtained up diving the sum

$$\sum_{n=1}^{100} n!$$

by 12.

7. Suppose a, b and c are integers. If $a^2 | b$ and $b^3 | c$, then $a^6 | c$.

8. If $n \in \mathbb{N}$, then $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$.

9. If $n \in \mathbb{Z}$, then $4 | n^2$ or $4 | (n^2 - 1)$.

10. Suppose a, b and c are integers. If $a | b$ and $a | (b^2 - c)$, then $a | c$.