Discrete Math for Computing II

Diego R.R.

January 18, 2024

Chapter 1

Number Theory and Cryptography

1.1 Divisibility and Modular Arithmetic

Definition 1. Let a and b be integers with $a \neq 0$. We say that a **divides** b if there exists an integer c such that $b = ac$. We write $a \mid b$ to denote that a divides b.

Theorem 1. Let a, b, and c be integers.

1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
2. If $a \mid b$, then $a \mid (bc)$ for all integers c.
3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Corollary 1. Let a, b, and c be integers, where $a \neq 0$. If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for all integers x and y.

Definition 2. The Division Algorithm. Let a and d a positive integers. Then there exist unique integers q and r such that $a = dq + r$ and $0 \leq r < d$.

Definition 3. In the equality given in the division algorithm, d is called the **divisor**, a is called the **dividend**, q is called the **quotient**, and r is called the **remainder**. This notation is used to express the quotient and remainder:

$$q = \frac{a}{d} \quad \text{and} \quad r = a \bmod d$$

1.1.1 exercises

Exercise 1 (22)**.** Let m be a positive integer. Show that $a \pmod{m} = b \pmod{m}$ if and only if $a \equiv b \pmod{m}$.