Chapter 10

Divisibility

Recall that we denote the natural numbers and the integers by $\mathbb{N}$ and $\mathbb{Z}$ respectively:

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\},$$
$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Definition 10.1. Suppose that $a, b \in \mathbb{Z}$. If $\exists c \in \mathbb{Z}$ such that $a = bc$ then we say that b *divides* a, and we write $b \mid a$.(This includes the case $b = a$.)

Remark 10.2. If $a, b \in \mathbb{N}$ satisfy $b \mid a$, then $b \leq a$.

Lemma 10.3. *Suppose that $a, b, d, x, y \in \mathbb{Z}$. If $d \mid a$ and $d \mid b$, then $d \mid ax + by$.*

Proof Since $d \mid a$ and $d \mid b$, $\exists l, m \in \mathbb{Z}$ such that $a = dl$ and $b = dm$. Hence

$$ax + by = (dl)\,x + (dm)\,y = d\,(lx + my),$$

giving that $d \mid ax + by$. □

Definition 10.4. Let $a, b \in \mathbb{N}$. A *greatest common divisor* of a, b is an element $d \in \mathbb{N}$ such that

(D1) $d \mid a$ and $d \mid b$;

(D2) if $e \in \mathbb{N}$ satisfies $e \mid a$ and $e \mid b$, then $e \mid d$.

In this case we write $d = \gcd(a, b)$, which we abbreviate to $d = (a, b)$ if there is no ambiguity caused by doing so.

Lemma 10.5. *Given $a, b \in \mathbb{N}$ with $a > b$, $\exists$ unique $q \in \mathbb{N}$ and $r \in \overline{\mathbb{N}}$ with $0 \leq r < b$ such that $a = qb + r$.*