

Assignment 1: Selected Solutions

Section 1.1

15. Prove that for $a, b \in \mathbb{Z}$, $b|a$ if, and only if, $a\mathbb{Z} \subseteq b\mathbb{Z}$.

Proof: First, if $a|b$, then $a = bk$ for some $k \in \mathbb{Z}$. Now, if $c \in a\mathbb{Z}$, then, for some $h \in \mathbb{Z}$, $c = ah = (bk)h = b(kh) \in b\mathbb{Z}$.

In the other direction, suppose $a\mathbb{Z} \subseteq b\mathbb{Z}$. Then, since $a \in a\mathbb{Z}$, $a \in b\mathbb{Z}$, $a = bk$ for some k . It follows that $b|a$. ■

Section 1.2

10. Show that $a\mathbb{Z} \cap b\mathbb{Z} = [a, b]\mathbb{Z}$.

Proof: The *least common multiple* $m = [a, b]$ is characterized by the properties

- (1) $a|m$ and $b|m$; and
- (2) if $c \in \mathbb{Z}$ is such that $a|c$ and $b|c$, then $m|c$.

Now, we begin by showing that $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$ for some $c \in \mathbb{Z}$. This follows since $a\mathbb{Z} \cap b\mathbb{Z}$ is closed under addition and subtraction. Indeed, if $x, y \in a\mathbb{Z} \cap b\mathbb{Z}$, then $x \pm y \in a\mathbb{Z}$ because $x, y \in a\mathbb{Z}$ and $a\mathbb{Z}$ is closed under addition and subtraction. Similarly, $x \pm y \in b\mathbb{Z}$ and the result follows.

Next, we show that $c = m$. Indeed, by property (1), $m \in a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$, so $c|m$. But, since $c \in c\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, $a|c$ and $b|c$. So, by property (2), $m|c$. ■

21. Prove that every positive integer can be written uniquely as a product of a square and a square-free integer.

Proof: First, note that the problem is incorrect as written, since it fails for the integer 1. We therefore prove this for integers $a > 1$.

By the Fundamental Theorem of Arithmetic, a can be written uniquely as a product

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}.$$

Each α_i can be written uniquely in the form $\alpha_i = 2\beta_i + \varepsilon_i$, where $\beta_i \geq 0$ and $\varepsilon_i \in \{0, 1\}$ (depending on whether α_i is even or odd). Now, set $n = p_1^{\beta_1} \cdots p_n^{\beta_n}$ and $m = p_1^{\varepsilon_1} \cdots p_n^{\varepsilon_n}$. Then, $a = n^2m$ is a presentation of a a product of a square and square-free integer. Uniqueness follows from the uniqueness of the prime decomposition and the uniqueness of the presentation of the α_i . ■