

Here's another approach to Theorem 2.3.

Notation: Let a, b be integers. Let $\mathbf{Z}a = \{ra \mid r \in \mathbf{Z}\}$.

Let $b + \mathbf{Z}a = \{b + ra \mid r \in \mathbf{Z}\}$.

Let $\mathbf{Z}a + \mathbf{Z}b = \{ra + sb \mid r, s \in \mathbf{Z}\}$.

Examples: $\mathbf{Z}2 = \{\dots, -2, 0, 2, 4, 6\}$ = set of even integers.

$1 + \mathbf{Z}2 = \{\dots, -1, 1, 3, 5, 7\}$ = set of odd integers.

$\mathbf{Z}2 + \mathbf{Z}3 = \mathbf{Z}$

$\mathbf{Z}2 + \mathbf{Z}4 = \mathbf{Z}2$

Remark: Another notation for $\mathbf{Z}a$ (which the text will use later) is $\langle a \rangle$.

Theorem 0.1 *Let a, b be integers. Then there exists an integer d such that $\mathbf{Z}a + \mathbf{Z}b = \mathbf{Z}d$. This integer d is the GCD of a, b .*

Proof: Let $S = (\mathbf{Z}a + \mathbf{Z}b) \cap \mathbf{N}$. By the well-ordering principle, S contains a smallest element, which we will call d . Since d is in $\mathbf{Z}a + \mathbf{Z}b$, there are integers m and n such that

$$d = ma + nb$$

If $\alpha \in \mathbf{Z}$ then $\alpha d = \alpha ma + \alpha nb$, so $\mathbf{Z}d \subseteq \mathbf{Z}a + \mathbf{Z}b$.

Now let $c \in \mathbf{Z}a + \mathbf{Z}b$. By the division algorithm, we can write $c = dq + r$, with $0 \leq r < d$. But since d is the smallest element of S , r must be 0, and $d \mid c$. Thus $c \in \mathbf{Z}d$ and so $\mathbf{Z}a + \mathbf{Z}b \subseteq \mathbf{Z}d$. Thus $\mathbf{Z}a + \mathbf{Z}b = \mathbf{Z}d$.

Now since both a and b are in $\mathbf{Z}a + \mathbf{Z}b$ ($a = 1 \cdot a + 0 \cdot b, b = 0 \cdot a + 1 \cdot b$), and d divides everything in $\mathbf{Z}a + \mathbf{Z}b$, we have $d \mid a$ and $d \mid b$. On the other hand, if $e \in \mathbf{Z}$ and $e \mid a$ and $e \mid b$ then $e \mid ma + nb = d$. Thus d is the GCD of a, b . □