Basic facts about integers

What can we deduce from the axioms?

Lemma 1: Let $a, b, c \in \mathbb{Z}$. If $a+b = a+c$, then $b = c$. [Additive Cancellation Property]

Proof: Let $a, b, c \in \mathbb{Z}$ and suppose $a+b = a+c$. Then

$$-a + (a+b) = -a + (a+c).$$

By Axiom 3 (Associativity),

$$(-a + a) + b = (-a + a) + c.$$

By Axiom 6 (Additive Inverses), we get

$$0 + b = 0 + c,$$

and by Axiom 5 (Additive Identity), this becomes

$$b = c,$$

as desired. ∎

Lemma 2 (Uniqueness of Additive Inverses).

Let $a, b \in \mathbb{Z}$. If $a + b = 0$, then $b = -a$.

Proof: Let $a, b \in \mathbb{Z}$ and suppose $a + b = 0$. Since $a + (-a) = 0$ also (Axiom 6), we have

$$a + b = a + (-a).$$

By the previous Lemma, we may cancel the a from both sides to get $b = -a$, as desired. ∎

Lemma 3: For any $a \in \mathbb{Z}$, $a \cdot 0 = 0$.

Proof: Let $a \in \mathbb{Z}$. Then

$$\begin{aligned} a \cdot 0 &= a(0 + 0) && \text{(Axiom 5)} \\ &= a \cdot 0 + a \cdot 0. && \text{(Axiom 4)} \end{aligned}$$

Also, $a \cdot 0 = a \cdot 0 + 0$ by Axiom 5. Thus,

$$a \cdot 0 + a \cdot 0 = a \cdot 0 + 0.$$

By cancellation, $a \cdot 0 = 0$. ∎

Lemma 4: For any $a \in \mathbb{Z}$, $-(-a) = a$.

Proof: Homework 9.

Note: You may not prove this using $(-1)\cdot(-1) = 1$. Why? We will use Lemma 4 to prove $(-1)^2 = 1$.

Let's actually do this now.

Lemma 5: For any $a \in \mathbb{Z}$, $-a = (-1)\cdot a$.

Proof: Let $a \in \mathbb{Z}$. Since additive inverses are unique, we can prove $(-1)\cdot a = -a$ by showing that

$$a + (-1)\cdot a = 0.$$

We have

$$\begin{aligned}
a + (-1)\cdot a &= (1)\cdot a + (-1)\cdot a && \text{(Axiom 5)} \\
&= (1 + (-1))\cdot a && \text{(Axiom 4)} \\
&= 0 \cdot a && \text{(Axiom 6)} \\
&= 0, && \text{(Lemma 3)}
\end{aligned}$$

so $(-1)\cdot a = -a$, as desired. ∎

Now, Lemmas 4 and 5 together show that $(-1)\cdot(-1) = 1$.

Indeed,

$$(-1)\cdot(-1) = -(-1) \quad \text{(Lemma 5)}$$
$$= 1. \quad \text{(Lemma 4)}$$

So far, we've only used Axioms 1-6. Axioms 7-10 concern the positive integers $\mathbb{N}$.

<u>Note</u>: We understand that $\mathbb{N}$ <u>should</u> be $\{1, 2, 3, \ldots\}$. But this isn't in the axioms, so we should refrain from assuming it to be true.