Basic properties of the Integers

Branko Ćurgus

March 2, 2019

1 Axioms for the Integers

In the axioms below we use the standard notation for logical operators: the conjunction is $\wedge$, the disjunction is $\vee$, the exclusive disjunction is $\oplus$, the implication is $\Rightarrow$, the universal quantifier is $\forall$, the existential quantifier is $\exists$.

We also use the standard set notation: the set membership $\in$, the subset $\subseteq$, the equality $=$, the set difference $\setminus$ and the Cartesian product $\times$. For singleton sets instead of writing $\{a\} = \{b\}$ we write $a = b$.

The notation $f : A \to B$ stands for a function f which is defined on a set A with the values in B.

Axiom 2 below establishes the existence of the addition function defined on $\mathbb{Z}\times\mathbb{Z}$ with the values in $\mathbb{Z}$. It is common to denote the value of $+$ at a pair $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ by $a + b$.

Axiom 7 establishes the existence of the multiplication function defined on $\mathbb{Z}\times\mathbb{Z}$ with the values in $\mathbb{Z}$. It is common to denote the value of this function at a pair $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ by $a \cdot b$ which is almost always abbreviated as ab.

Axiom 12 introduces the set of positive integers.

As a mnemonic aid I have assigned each axiom an abbreviation. Here are explanations of the abbreviations: ZE - integers exist, AE - addition exists, AA - addition is associative, AC - addition is commutative, AZ - addition has zero, AO - addition has opposites, ME - multiplication exists, MA - multiplication is associative, MC - multiplication is commutative, MO - multiplication has one, MZ - multiplication respects zero, DL - distributive law, PE - positive integers exist, PD - dichotomy involving positive integers, PA - positive integers respect addition, PM - positive integers respect multiplication, WO - the well-ordering axiom.

Definition. The set $\mathbb{Z}$ of *integers* satisfies the following 16 axioms.

Axiom 1 (ZE). $\mathbb{Z} \neq \emptyset$

Axiom 2 (AE). $\exists\ + : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

Axiom 3 (AA). $\forall a \in \mathbb{Z}\ \ \forall b \in \mathbb{Z}\ \ \forall c \in \mathbb{Z} \quad a+(b+c) = (a+b)+c$

Axiom 4 (AC). $\forall a \in \mathbb{Z}\ \ \forall b \in \mathbb{Z} \quad a+b = b+a$

Axiom 5 (AZ). $\exists\, 0 \in \mathbb{Z}\ \ \forall a \in \mathbb{Z} \quad 0 + a = a$

Axiom 6 (AO). $\forall a \in \mathbb{Z}\ \ \exists\, (-a) \in \mathbb{Z} \quad a + (-a) = 0$

Axiom 7 (ME). $\exists\ \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

Axiom 8 (MA). $\forall a \in \mathbb{Z}\ \ \forall b \in \mathbb{Z}\ \forall c \in \mathbb{Z} \quad a(bc) = (ab)c$

Axiom 9 (MC). $\forall a \in \mathbb{Z}\ \ \forall b \in \mathbb{Z} \quad ab = ba$

Axiom 10 (MO). $\exists\, 1 \in \mathbb{Z}\backslash\{0\} \quad \forall a \in \mathbb{Z} \quad 1 \cdot a = a$

Axiom 11 (DL). $\forall a \in \mathbb{Z}\ \ \forall b \in \mathbb{Z}\ \ \forall c \in \mathbb{Z} \quad a(b+c) = ab + ac$

Axiom 12 (PE). $\exists\ \mathbb{P} \quad \big(\mathbb{P} \subseteq \mathbb{Z}\backslash\{0\}\big) \wedge \big(\mathbb{P} \neq \emptyset\big)$

Axiom 13 (PD). $\forall a \in \mathbb{Z}\backslash\{0\} \quad (a \in \mathbb{P}) \oplus (-a \in \mathbb{P})$

Axiom 14 (PA). $\forall a \in \mathbb{P}\ \ \forall b \in \mathbb{P} \quad a + b \in \mathbb{P}$

Axiom 15 (PM). $\forall\, a \in \mathbb{P}\ \ \forall b \in \mathbb{P} \quad ab \in \mathbb{P}$

Axiom 16 (WO).
$\big(S \subseteq \mathbb{P}\big) \wedge \big(S \neq \emptyset\big) \Rightarrow \big(\exists\, m \in S\ \ \forall\, x \in S\backslash\{m\} \quad x + (-m) \in \mathbb{P}\big)$

2 Basic algebraic properties of the integers

In this section we list properties of the integers which involve the axioms related to the addition and the multiplication, but not the order.

Proposition 2.1. *Let a, b and c be integers. Then $a + c = b + c$ implies $a = b$.*

Proof. Let a, b and c be arbitrary integers. Assume $a + c = b + c$. By Axiom AO there exists $-c \in \mathbb{Z}$ such that $c + (-c) = 0$. Since $+$ is a function $a + c = b + c$ implies that

$(a+c)+(-c) = (b+c)+(-c)$. By Axiom AA $a+(c+(-c)) = b+(c+(-c))$ and, since $c+(-c) = 0$, $a+0 = b+0$. By Axiom AZ this yields. $a = b$. □

Proposition 2.2. *The element* $0 \in \mathbb{Z}$ *introduced in* Axiom AZ *is unique.*

Proof. Assume that there exist $0' \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$ we have $0' + a = a$. Let $c \in \mathbb{Z}$. The universal instantiation yields $0' + c = c$. The universal instantiation in Axiom AZ yields $0 + c = c$. Thus $0' + c = 0 + c$. By Proposition 2.1 we deduce $0' = 0$. □

Proposition 2.3. *For every* $a \in \mathbb{Z}$ *the equation* $a + x = 0$ *has a unique solution.*

Proof. Let $a \in \mathbb{Z}$ be arbitrary. By Axiom AO the equation $a + x = 0$ has a solution $x = -a$, that is $a+(-a) = 0$. Assume that $a+x' = 0$. Consequently, $a+(-a) = a+x$. By Axiom AC the last equality implies $(-a) + a = x + a$. By Proposition 2.1 we deduce $x = -a$. □

Definition 2.4. Let $a \in \mathbb{Z}$. The unique solution $-a$ of the equation $a + x = 0$ is called the *opposite* of a. For $b \in \mathbb{Z}$ we write $b - a$ instead of $b + (-a)$.

Proposition 2.5. *For every* $a \in \mathbb{Z}$ *we have* $-(-a) = a$.

Proof. Let $a \in \mathbb{Z}$ be arbitrary. By definition $-(-a)$ we have $(-a) + \bigl(-(-a)\bigr) = 0$. By definition of $-a$ we have $a + (-a) = 0$. By Axiom AC we have $(-a) + a = 0$. From $(-a) + \bigl(-(-a)\bigr) = 0$ and $(-a) + a = 0$ we conclude that $(-a) + \bigl(-(-a)\bigr) = (-a) + a$. By By Proposition 2.1 we conclude that $a = -(-a)$. □

Proposition 2.6. *For every* $a \in \mathbb{Z}$ *we have* $a = 0$ *if and only if* $-a = a$.

Proof. Assume that $a = 0$. By Definition 2.4 -0 is the unique solution of the equation $0 + x = 0$. Since by Axiom AZ we have $0 + 0 = 0$, we deduce $-0 = 0$. That is $-a = a$ holds. We prove the converse by proving its contrapositive. Assume that $a \neq 0$. Then by Axiom PD we have that

$$\bigl((a \in \mathbb{P}) \wedge -a \notin \mathbb{P}\bigr) \oplus \bigl((-a \in \mathbb{P}) \wedge (a \notin \mathbb{P})\bigr)$$

In both cases $-a \neq a$. □

Proposition 2.7. *For every* $a \in \mathbb{Z}$ *we have* $a0 = 0a = 0$.

Proof. Let $a \in \mathbb{Z}$ be arbitrary. By Axiom AZ and universal instantiation we have $0+0 = 0$. Since the multiplication is a function $a(0 + 0) = a0$. By Axiom DL $a0 + a0 = a0$. By Axiom ME $a0 \in \mathbb{Z}$. Hence $-(a0) \in \mathbb{Z}$ exists by Axiom AO. Now $a0 + a0 = a0$ yields $(a0+a0)-(a0) = a0-(a0)$. By Axiom AA and AO we obtain $a0 = 0$. Axiom AC now yields $a0 = 0a = 0$. □

Proposition 2.8. *For every* $a \in \mathbb{Z}$ *and for every* $b \in \mathbb{Z}$ *we have* $(-a)b = a(-b) = -(ab)$.

Proof. Let a and b be arbitrary integers. Then by Axiom AO we have $a + (-a) = 0$. By Axioms ME, we have $\big(a + (-a)\big)b = 0b$. Now, Axioms MC and DL and Proposition 2.7 yield $ab+(-a)b = 0$. By Axiom AO we have $ab+\big(-(ab)\big) = 0$. Hence, $ab+(-a)b = ab+\big(-(ab)\big)$. By Axiom AC $(-a)b+ab = \big(-(ab)\big)+ab$. By Proposition 2.1 we conclude $(-a)b = \big(-(ab)\big)$. The equality $a(-b) = -(ab)$ is proved similary. □

Proposition 2.9. *For every $a \in \mathbb{Z}$ and for every $b \in \mathbb{Z}$ we have $(-a)(-b) = ab$.*

Proof. Let a and b be arbitrary integers. By Proposition 2.8 we have $(-a)(-b) = -\big(a(-b)\big)$. Applying Proposition 2.8 yields $a(-b) = -(ab)$. Hence $(-a)(-b) = -\big(-(ab)\big)$. Now, Proposition 2.5 implies $-\big(-(ab)\big) = ab$, and consequently $(-a)(-b) = ab$. □

3 Basic properties of the integers involving the order

The following proposition gives in some sense a converse of Axiom PM.

Proposition 3.1. *For every $a \in \mathbb{Z}$ and every $b \in \mathbb{P}$ we have $ab \in \mathbb{P}$ if and only if $a \in \mathbb{P}$.*

Proof. Let $a \in \mathbb{Z}$ and $b \in \mathbb{P}$ be arbitrary. If $a \in \mathbb{P}$, then by Axiom PM $ab \in \mathbb{P}$. We prove the converse by proving its contrapositive. Assume that $a \notin \mathbb{P}$. We distinguish two cases: $a = 0$ and $a \neq 0$. If $a = 0$, then by Proposition 2.7 $ab = 0$. Therefore, $ab \notin \mathbb{P}$. If $a \neq 0$, then the disjunctive syllogism of $a \notin \mathbb{P}$ and Axiom PD yields that $-a \in \mathbb{P}$. Now, by Axiom PM and Proposition 2.8 we conclude $-(ab) \in \mathbb{P}$. Since $ab \neq 0$, Axiom PD yields $ab \notin \mathbb{P}$. In both cases $a \notin \mathbb{P} \Rightarrow ab \notin \mathbb{P}$. □

In Axiom PE we have introduced the nonempty set of nonzero integers $\mathbb{P}$. Now we will prove that this set contains a lot of integers.

Proposition 3.2. *For every nonzero integer a we have $aa \in \mathbb{P}$.*

Proof. Let a be an arbitrary nonzero integer. By Axiom PD we have two possibilities for a: either $a \in \mathbb{P}$ or $-a \in \mathbb{P}$. We proceed with two cases. Case 1. Assume $a \in \mathbb{P}$. By Axiom PM we have $aa \in \mathbb{P}$. Case 2. Assume $-a \in \mathbb{P}$. By Axiom PM we have $(-a)(-a) \in \mathbb{P}$. By Proposition 2.9 we have $(-a)(-a) = aa$. Therefore $aa \in \mathbb{P}$ in this case as well. □

Proposition 3.3. *For all $a \in \mathbb{Z}$ and all $b \in \mathbb{Z}$ we have $ab = 0$ if and only if $a = 0$ or $b = 0$.*

Proof. We first prove the “only if” part by proving its contrapositive. Assume $a \neq 0$ and $b \neq 0$. By Axiom PD we have $(a \in \mathbb{P}) \oplus (-a \in \mathbb{P})$ and $(b \in \mathbb{P}) \oplus (-b \in \mathbb{P})$. Therefore we consider four different cases: Case 1 $a \in \mathbb{P}$ and $b \in \mathbb{P}$, Case 2 $a \in \mathbb{P}$ and $-b \in \mathbb{P}$, Case 3 $-a \in \mathbb{P}$ and $b \in \mathbb{P}$, Case 4 $-a \in \mathbb{P}$ and $-b \in \mathbb{P}$. By Axiom PM, in Case 1 and Case 4 (using Proposition 2.9) we have $ab \in \mathbb{P}$. By Axiom PM and Proposition 2.8, in Case 2 and Case 3 we have $-ab \in \mathbb{P}$. The converse follows from Proposition 2.7. □

Definition 3.4. For $a \in \mathbb{Z}$ the product aa is called the *square of* a and it is denoted by a^2.

Corollary 3.5. $1 \in \mathbb{P}$.

Proof. By Axiom MO we have $1 \neq 0$. By Proposition 3.2 we deduce $1^2 \in \mathbb{P}$. By Axiom MO $1^2 = 1$. Thus, $1 \in \mathbb{P}$. $\square$

Corollary 3.6. *For every $a \in \mathbb{P}$ we have $a + 1 \in \mathbb{P}$.*

Proof. Let $a \in \mathbb{P}$ be arbitrary. Since $1 \in \mathbb{P}$, Axiom PA implies $a + 1 \in \mathbb{P}$. $\square$

Thus, $1 \in \mathbb{P}$, $1+1 \in \mathbb{P}$, $1+1+1 \in \mathbb{P}$, and so on. This is the motivation for the following definition

Definition 3.7. The integers in the set $\mathbb{P}$ are called *positive integers*. An alternative notation for positive integers is $\mathbb{Z}^+$. An integer a is said to be negative if and only if $-a \in \mathbb{P}$. The set of all negative integers is denoted by $\mathbb{Z}^-$.

Notice the following important trichotomy for integers which follows from Axioms PE and PD: For each $a \in \mathbb{Z}$ exactly one of the following three propositions is true:

$$\boxed{a \text{ is negative}} \qquad \boxed{a = 0} \qquad \boxed{a \text{ is positive}}$$

Definition 3.8. For arbitrary integers a and b we say that a is *smaller then* b and write $a < b$ (or equivalently $b > a$) if and only if $b - a \in \mathbb{P}$.

Since $1 - 0 = 1$ and $1 \in \mathbb{P}$ we have $0 < 1$. The following proposition gives the basic properties of order $<$.

Proposition 3.9. (A) *For all $a \in \mathbb{Z}$ and for all $b \in \mathbb{Z}$ exactly one of the following three propositions is true:*

$$\boxed{a < b} \qquad \boxed{a = b} \qquad \boxed{b < a}$$

(B) $\forall a \in \mathbb{Z}\ \forall b \in \mathbb{Z}\ \forall c \in \mathbb{Z} \quad (a < b) \wedge (b < c) \Rightarrow (a < c)$

(C) $\forall a \in \mathbb{Z}\ \forall b \in \mathbb{Z}\ \forall c \in \mathbb{Z} \quad (a < b) \Leftrightarrow (a + c < b + c)$

(D) $\forall a \in \mathbb{Z}\ \forall b \in \mathbb{Z}\ \forall c \in \mathbb{P} \quad (a < b) \Leftrightarrow (ac < bc)$

Proof. We prove (A). Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ be arbitrary. Then by Axioms AE and AO we have $b - a \in \mathbb{Z}$. We have two exclusive cases: Case 1: $b - a = 0$ and Case 2: $b - a \in \mathbb{Z}\backslash\{0\}$. In Case 1 we have $a = b$. In Case 2 we use Axiom PD to conclude

$$(b - a \in \mathbb{P}) \oplus (-(b - a) \in \mathbb{P}),$$

that is

$$(a < b) \oplus (b < a).$$

This proves (A). Statements (B), (C) and (D) are proved similarly. $\square$

Proposition 3.10. *Let a and b be integers. Then $a < b$ if and only if $-b < -a$.*

Proof. Let a and b be arbitrary integers. By Proposition 2.5 we have $b - a = (-a) - (-b)$. Therefore, $a < b$ if and only if $b - a \in \mathbb{P}$ if and only if $(-a) - (-b) \in \mathbb{P}$ if and only if $-b < -a$. $\square$

Proposition 3.11. *Let a, b and c be integers. Then $a < b$ and $c < 0$ imply $bc < ac$.*

Proof. Let a, b and c be arbitrary integers. Assume $a < b$ and $c < 0$. Then by Propositions 3.10 and 2.6 $0 < -c$. Now, $a < b$, $0 < -c$ and Proposition 3.9(D) imply $a(-c) < b(-c)$. By Proposition 2.8, the last inequality can be rewritten as $-(ac) < -(bc)$. By Propositions 3.10 the last inequality implies $bc < ac$. $\square$

Since $0 < 1$, Proposition 3.9(C) yields $1 < 1 + 1$. Therefore, by Proposition 3.9(A), $1 \neq 1 + 1$. Therefore we define

Definition 3.12. $2 = 1 + 1$.

Again by Proposition 3.9(C) $2 < 2 + 1$. Therefore we define

Definition 3.13. $3 = 2+1,\ 4 = 3+1,\ 5 = 4+1,\ 6 = 5+1,\ 7 = 6+1,\ 8 = 7+1, 9 = 8+1$.

By Proposition 3.9(C), $0 < 1 < 2 < 3 < 4 < 5 < 6 < 7 < 8 < 9$.

Exercise 3.14. Prove $2 + 2 = 4$.

Exercise 3.15. Prove $2 \cdot 2 = 4$.

4 The Well Ordering Axiom

We use the common abbreviation $a \leq b$ for the proposition $(a < b) \oplus (a = b)$. With this abbreviation and the notation $\mathbb{P} = \mathbb{Z}^+$ the Well-Ordering Axiom can be rewritten as:

Axiom 16 (WO). $\big(S \subseteq \mathbb{Z}^+\big) \wedge \big(S \neq \emptyset\big) \Rightarrow \big(\exists\, m \in S \ \ \forall x \in S \quad m \leq x\big)$

Definition 4.1. Let S be a nonempty subset of $\mathbb{Z}$. We say that S *has a minimum* if there exists $m \in S$ such that for every $x \in S$ we have $m \leq x$. Formally,

$$S \text{ has a minimum} \quad \Leftrightarrow \quad \exists\, m \in S \ \ \forall\, x \in S \quad m \leq x. \tag{4.1}$$

The integer $m \in S$ satisfying the proposition on the right-hand side of (4.1) is called the *minimum* of S. It is denoted by $\min S$.

With this definition the Well-Ordering Axiom can be restated as

$$\big(S \subseteq \mathbb{Z}^+\big) \wedge \big(S \neq \emptyset\big) \;\Rightarrow\; S \text{ has a minimum} \tag{4.2}$$

Recall that the propositions $p \wedge q \Rightarrow r$ and $p \wedge \neg r \Rightarrow \neg q$ are equivalent. Consequently, the well ordering Axiom WO, as stated in (4.2), is equivalent to

$$\big(S \subseteq \mathbb{Z}^+\big) \wedge \big(S \text{ does not have a minimum}\big) \;\Rightarrow\; \big(S = \emptyset\big) \tag{4.3}$$

At this point it is useful to note the formal meaning of the phrase "S does not have a minimum". Negating (4.1) we get:

$$S \text{ does not have a minimum} \quad \Leftrightarrow \quad \forall x \in S \;\; \exists\, y \in S \quad y < x.$$

I will illustrate how to use (4.3) in the following proposition.

Proposition 4.2. *There are no integers between* 0 *and* 1*.*

Proof. Define the set S by

$$S = \{x \in \mathbb{Z} \,|\, (0 < x) \wedge (x < 1)\}.$$

Clearly $S \subset \mathbb{Z}^+$. Next we will prove that S does not have a minimum. Let $x \in S$ be arbitrary. Then $0 < x$ and $x < 1$. The last two inequalities and Proposition 3.9(D) imply $x^2 < x$. Since $x \neq 0$, Proposition 3.2 implies $0 < x^2$. Since $x^2 < x$ and $x < 1$, Proposition 3.9(B) implies $x^2 < 1$. Now we have, $x^2 \in \mathbb{Z}$ and $0 < x^2$ and $x < 1$. Thus, $x^2 \in S$ and also $x^2 < x$. Hence we have proved that for every $x \in S$ there exists $y = x^2 \in S$ such that $y = x^2 < x$. That is, S does not have a minimum. By (4.3), we deduce $S = \emptyset$. □

The next proposition can be deduced from the previous one. However, I will give a direct proof.

Proposition 4.3. *The minimum of* $\mathbb{Z}^+$ *is* 1*.*

Proof. Since $1 \in \mathbb{Z}^+$ the set $\mathbb{Z}^+$ is not empty. Since clearly $\mathbb{Z}^+ \subseteq \mathbb{Z}^+$, Axiom WO implies that $\mathbb{Z}^+$ has a minimum. Denote by m the minimum of $\mathbb{Z}^+$; that is, set $m = \min \mathbb{Z}^+$. Recall that m has the following properties:

$$m \in \mathbb{Z}^+ \quad \text{and} \quad \forall x \in \mathbb{Z}^+ \; m \leq x. \tag{4.4}$$

Since $1 \in \mathbb{Z}^+$ we have $m \leq 1$. Since $m > 0$, Axiom OM yields $m^2 \leq m$. Since $0 < m$ by Proposition 3.9(D) we deduce $0 < m^2$. Thus $m^2 \in \mathbb{Z}^+$. Since $m = \min \mathbb{Z}^+$ we conclude $m \leq m^2$. Since both $m^2 \leq m$ and $m \leq m^2$, we have $m = m^2$, that is $m(m-1) = 0$. Now Proposition 3.3 implies $m = 0$ or $m - 1 = 0$. Since $m > 0$, disjunctive syllogism yields $m - 1 = 0$. That is $m = 1$ is proved. □

Definition 4.4. An integer a is a *square* if there exists an integer b such that $a = b^2$.

Proposition 4.5. *Let s be an integer. If s and $2s$ are both square, then $s = 0$.*

Proof. In this proof we will use the fact that an integer x is even if and only if x^2 is even.

Consider the set

$$S = \bigl\{ s \in \mathbb{Z} \,|\ \ s > 0,\ \ s \ \text{ and } \ 2s \ \text{ are squares } \bigr\}.$$

Clearly $S \subseteq \mathbb{Z}^+$.

Next we shall prove that S does not have a minimum. Let $s \in S$ be arbitrary. Then $s > 0$ and there exist positive integers j and k such that $s = j^2$ and $2s = k^2$. Since k^2 is even, the integer k is even. Therefore there exist a positive integer m such that $k = 2m$. Thus, $2s = 4m^2$, or, equivalently $s = 2m^2$. Clearly, $m^2 < 2m^2 = s$. Since m is positive, $m^2 > 0$. Now we have that $m^2 > 0$ and both integers m^2 and $2m^2 = s$ are square. Therefore $m^2 \in S$ and $m^2 < s$. Consequently s is not a minimum of S. Since $s \in S$ was arbitrary element in S, we have proved that S does not have a minimum. By Axiom WO, see (4.3), $S = \emptyset$. Thus, there are no positive integers s such that both s and $2s$ are squares. Therefore, if s and s^2 are both square, then $s \leq 0$. Since for each square number s by Proposition 3.2 we have $s \geq 0$, we conclude that $s = 0$. □

Proposition 4.6. *If $p \in \mathbb{Z}$ and $q \in \mathbb{Z}^+$, then $p^2 \neq 2q^2$.*

Proof. Let $p \in \mathbb{Z}$ and $q \in \mathbb{Z}^+$. Proposition 4.5 is equivalent to: If s is a square and $s \neq 0$, then $2s$ is not a square. Applying this to q^2 we conclude that $2q^2$ is not a square. Since p^2 is a square, we conclude $p^2 \neq 2q^2$. □

The preceding proposition implies that a square of a rational number cannot equal 2. In other words, $\sqrt{2}$ is irrational.

5 Proof of the principle of mathematical induction

In the next theorem the universe of discourse is the set $\mathbb{Z}^+$ of positive integers.

Theorem 5.1. *Let $P(n)$ be a propositional function involving a positive integer n. Then*

$$\boxed{P(1) \wedge \Bigl(\forall\, k \ \bigl(P(k) \Rightarrow P(k+1)\bigr)\Bigr)} \ \Rightarrow \ \boxed{\forall n \ P(n)}$$

Proof. Recall that the implications $p \wedge q \Rightarrow r$ and $p \wedge (\neg r) \Rightarrow (\neg q)$ are equivalent. Therefore we will prove:

$$\boxed{P(1) \wedge \bigl(\exists\, j \ \neg P(j)\bigr)} \Rightarrow \boxed{\exists\, k \ \bigl(P(k) \wedge \neg P(k+1)\bigr)}. \tag{5.1}$$

Assume $\boxed{P(1)}$ and $\boxed{\exists\, j\ \neg P(j)}$. That is, assume that there exists $j_0 \in \mathbb{Z}^+$ such that $\boxed{\neg P(j_0)}$. Now consider the set

$$S = \bigl\{n \in \mathbb{Z}^+ \,|\, \neg P(n)\bigr\} = \bigl\{n \,|\, \bigl(n \in \mathbb{Z}^+\bigr) \wedge \bigl(\neg P(n)\bigr)\bigr\}.$$

Clearly $S \subseteq \mathbb{Z}^+$ and $j_0 \in S$. Hence

$$\boxed{\bigl(S \subseteq \mathbb{Z}^+\bigr) \wedge \bigl(S \neq \emptyset\bigr)}$$

is true. This and Axiom WO, via modus ponens, yield that the set S has a minimum, that is,

$$\boxed{\exists\, m \in S\ \ \forall x \in S \quad m \leq x}. \tag{5.2}$$

Since $m \in S$ we have $\boxed{m \in \mathbb{Z}^+}$ and $\boxed{\neg P(m)}$. As $\boxed{P(1)}$ is true, $\boxed{\bigl(\neg P(m)\bigr) \wedge P(1)}$ imply $1 \neq m$. Since $\boxed{1 = \min \mathbb{Z}^+}$ we have $\boxed{1 < m}$. By the definition of the order $<$ we have $\boxed{m - 1 \in \mathbb{Z}^+}$.

Next we rewrite the proposition (5.2). First, we notice that the proposition

$$\forall x \in S \quad m \leq x$$

is equivalent to

$$\forall x \quad x \in S \Rightarrow m \leq x,$$

which is further equivalent to

$$\forall x \quad x < m \Rightarrow x \notin S.$$

Thus (5.2) is equivalent to

$$\boxed{\exists\, m \in S\ \ \forall x\ \ \bigl(x < m \Rightarrow x \notin S\bigr)}. \tag{5.3}$$

Define $k = m - 1$. Then $\boxed{k \in \mathbb{Z}^+}$. Further, since $\boxed{k < m}$, (5.3) implies $\boxed{k \notin S}$. Since $n \in S$ is equivalent to $(n \in \mathbb{Z}^+) \wedge (\neg P(n))$ we conclude that $\boxed{k \notin S}$ is equivalent to $\boxed{\bigl(k \notin \mathbb{Z}^+\bigr) \vee P(k)}$. Since we know that $\boxed{k \in \mathbb{Z}^+}$ and $\boxed{k \notin S}$, by disjunctive syllogism we deduce $\boxed{P(k)}$ is true. Recall that $\boxed{k + 1 = m \in S}$. Hence $\boxed{\neg P(k+1)}$ is true. Thus, by setting $k = m - 1$, we just proved that

$$\boxed{\exists\, k\ \bigl(P(k) \wedge \neg P(k+1)\bigr)}$$

is true. This completes the proof. $\square$

6 Even and Odd Integers

First recall the definitions of even and odd integers. The set of all even integers we denote by $\mathbb{E}$ and the set of all odd integers we denote by $\mathbb{O}$. For $n \in \mathbb{Z}$ we define

$$n \in \mathbb{E} \quad \Leftrightarrow \quad \exists k \in \mathbb{Z} \;\; n = 2k, \tag{6.1}$$

$$n \in \mathbb{O} \quad \Leftrightarrow \quad \exists k \in \mathbb{Z} \;\; n = 2k+1. \tag{6.2}$$

Proposition 6.1. $\mathbb{E} \cap \mathbb{O} = \emptyset$.

Proof. We prove this by contradiction. Assume that $\mathbb{E} \cap \mathbb{O}$ is a nonempty set. Let $n \in \mathbb{E} \cap \mathbb{O}$. Then there exist $k, j \in \mathbb{Z}$ such that $n = 2k = 2j+1$. Hence, there exists $m = k - j \in \mathbb{Z}$ such that $1 = 2m$. Recall that we proved $0 < 1 < 2$. Substituting $1 = 2m$, we get $0 < 2m < 2$. Since $0 < 2$, Proposition 3.9(D) applied to $2 \cdot 0 < 2m$, yields $0 < m$. Proposition 3.9(D) applied to $2m < 2 \cdot 1$, yields $m < 1$. Thus, we have $0 < m$ and $m < 1$ and $m \in \mathbb{Z}$. By Proposition 4.2 the statement "$0 < m$ and $m < 1$ and $m \in \mathbb{Z}$" is false. Since the assumption that $\mathbb{E} \cap \mathbb{O} \neq \emptyset$ leads to a false statement, we proved $\mathbb{E} \cap \mathbb{O} = \emptyset$. □

Proposition 6.2. $\mathbb{E} \cup \mathbb{O} = \mathbb{Z}$.

Proof. First we prove that $\mathbb{Z}^+ \subseteq \mathbb{E} \cup \mathbb{O}$. In other words we prove

$$\forall n \in \mathbb{Z}^+ \quad (n \in \mathbb{E}) \vee (n \in \mathbb{O})$$

The last displayed statement can be proved by Mathematical Induction. Set $P(n)$ to be $(n \in \mathbb{E}) \vee (n \in \mathbb{O})$.

Since $1 = 2 \cdot 0 + 1$ we have $1 \in \mathbb{O}$. Therefore, $(1 \in \mathbb{E}) \vee (1 \in \mathbb{O})$ is true. So, the base step $P(1)$ is true.

Next we prove the inductive step. Let $n \in \mathbb{Z}^+$ be arbitrary and prove the implication $P(n) \Rightarrow P(n+1)$. Assume that $P(n)$ is true. That is, assume that $(n \in \mathbb{E}) \vee (n \in \mathbb{O})$. Consider two cases. For Case 1, assume $n \in \mathbb{E}$. Clearly $n \in \mathbb{E}$ implies $n+1 \in \mathbb{O}$. Therefore, $(n+1 \in \mathbb{E}) \vee (n+1 \in \mathbb{O})$ is true. Thus $P(n+1)$ holds in this case. For Case 2, assume $n \in \mathbb{O}$. Clearly $n \in \mathbb{O}$ implies $n+1 \in \mathbb{E}$. Therefore, $(n+1 \in \mathbb{E}) \vee (n+1 \in \mathbb{O})$ is true. Thus $P(n+1)$ holds in this case as well. Thus, for every $n \in \mathbb{Z}^+$ we proved that $P(n) \Rightarrow P(n+1)$.

By Mathematical induction, this proves that $\forall n \in \mathbb{Z}^+$ we have $(n \in \mathbb{E}) \vee (n \in \mathbb{O})$. In other words, $\mathbb{Z}^+ \subseteq \mathbb{E} \cup \mathbb{O}$.

Since $0 = 2 \cdot 0$, we have $0 \in \mathbb{E}$. Hence, $0 \in \mathbb{E} \cup \mathbb{O}$.

Finally we prove that $\mathbb{Z}^- \subseteq \mathbb{E} \cup \mathbb{O}$. Let $n \in \mathbb{Z}$ be such that $n < 0$. Then $-n > 0$ and thus, $-n \in \mathbb{E} \cup \mathbb{O}$. Now consider two cases. Case 1: if $-n \in \mathbb{E}$, then $-n = 2k$ for some $k \in \mathbb{Z}$. Hence, $n = 2(-k)$ with $-k \in \mathbb{Z}$. Consequently, $n \in \mathbb{E}$. Case 2: if $-n \in \mathbb{O}$, then $-n = 2j+1$ for some $j \in \mathbb{Z}$. Hence, $n = 2(-j) - 1 = 2(-j-1) + 1$ with $-j-1 \in \mathbb{Z}$. Consequently, $n \in \mathbb{O}$. In either case, $n \in \mathbb{E} \cup \mathbb{O}$.

In conclusion, we have proved that for every $n \in \mathbb{Z}$ we have $n \in \mathbb{E} \cup \mathbb{O}$. That is $\mathbb{E} \cup \mathbb{O} = \mathbb{Z}$. □

7 The division algorithm

The following theorem is called the *division algorithm*.

Proposition 7.1. *Let n be an integer and let d be a positive integer. Then there exist unique integers q and r such that*

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

Proof. Let $n \in \mathbb{Z}$ and let $d \in \mathbb{Z}^+$. Define the set

$$S = \Big\{ k \in \mathbb{Z} \,\Big|\, \big(k \geq 0\big) \wedge \big(\exists\, j \in \mathbb{Z} \quad k = n - dj\big) \Big\}.$$

By the definition of S we have $S \subset \mathbb{Z}$ and S is bounded below by 0.

Next we prove that S is a nonempty set. We distinguish two cases for n: $n \geq 0$ and $n < 0$. If $n \geq 0$, then $n \in S$ since $n = n - d \cdot 0 \geq 0$. Now assume that $n < 0$. Then $-n > 0$. Now $-n > 0$ and $d \geq 1$, imply $-nd \geq -n$. Adding n to both sides of $-nd \geq -n$ we get $n - dn \geq n - n = 0$. Since with $j = n$ $k = n - dj = n - dn \in S$ we have proved that $S \neq \emptyset$ in this case. Thus, in each case we identified an integer in S, so S is a nonempty set.

Since S is both bounded below and nonempty, Proposition **??** implies that S has a minimum. Denote that minimum by r. The integer r has the following two properties: $r \in S$ and $r \leq k$ for all $k \in S$. Since $r \in S$, we have $r \geq 0$ and there exists $q \in \mathbb{Z}$ such that $r = n - dq$. Hence we proved that there exist integers r and q such that $n = dq + r$ and $r \geq 0$.

It remains to prove that $r < d$. Consider the integer $r - d$. As $d > 0$ we have $r - d < r$. Since $x \in S$ implies $r \leq x$, the contrapositive of the last implication yields $r - d \notin S$. Since

$$x \in S \qquad \Leftrightarrow \qquad (x \geq 0) \wedge \big(\exists\, j \in \mathbb{Z} \quad x = n - dj\big)$$

$r - d \notin S$ means

$$\big(r - d < 0\big) \;\vee\; \big(\forall\, j \in \mathbb{Z} \;\; r - d \neq n - dj\big). \tag{7.1}$$

However, we know that the following is true

$$r - d = n - dq - d = n - d(q + 1).$$

Thus

$$\exists\, j \in \mathbb{Z} \;\; r - d = n - dj. \tag{7.2}$$

By disjunctive syllogism, (7.1) and (7.2) yield $r - d < 0$. That is $r < d$.

It remains to prove the uniqueness of r and q. Assume that q, r, q', r' are integers such that

$$(n = dq + r) \wedge (0 \leq r < d) \qquad \text{and} \qquad (n = dq' + r') \wedge (0 \leq r' < d).$$

Then

$$dq + r = dq' + r' \quad \text{and} \quad 0 \leq r < d \quad \text{and} \quad -d < r' \leq 0.$$

Simplifying the first equality and adding the last two inequalities we get

$$r - r' = d(q' - q) \qquad \text{and} \qquad -d < r - r' < d.$$

Hence

$$-d < d(q' - q) < d.$$

Since $0 < d$, Proposition 3.9(D) implies

$$-1 < q' - q < 1.$$

In Proposition 4.2 we proved that there are no integers between 0 and 1. Since $q' - q$ is an integer we must have $-1 < q' - q \leq 0$. Multiplying by $-1 < 0$ and using Proposition 3.11 we conclude $0 \leq -q' + q < 1$. Now Proposition 4.2 yields $-q' + q = 0$. That is $q = q'$. Since $r - r' = d(q' - q)$ we also conclude that $r' = r$. □

Definition 7.2. The integer r in Proposition 7.1 is called the *remainder* left by n when divided by m.

Example 7.3. When divided by 5, the integer 17 leaves a remainders of 2: $17 = 5 \cdot 3 + 2$. When divided by 5, the integer -17 leaves a remainder of 3: $-17 = 5(-4) + 3$.

Definition 7.4. Let n be an integer. Let r be the remainder left by n when divided by 2. Then $r = 0$ or $r = 1$. We say that n is *even* if $r = 0$ and that n is *odd* if $r = 1$.

Remark 7.5. In Proposition 7.1 we proved that for every $n \in \mathbb{Z}$ and every $d \in \mathbb{Z}^+$ there exist unique $q \in \mathbb{Z}$ and unique $r \in \mathbb{Z}$ such that

$$n = dq + r \qquad \text{and} \qquad 0 \leq r < d. \tag{7.3}$$

Dividing both relations in (7.3) by $d > 0$ we get

$$\frac{n}{d} = q + \frac{r}{d} \qquad \text{and} \qquad 0 \leq \frac{r}{d} < 1.$$

Therefore we have

$$q \in \mathbb{Z} \qquad \text{and} \qquad q \leq \frac{n}{d} < q + 1.$$

The last displayed line is exactly the definition of the floor of $\frac{n}{d}$. Thus, in the division algorithm

$$q = \left\lfloor \frac{n}{d} \right\rfloor \qquad \text{and} \qquad r = n - d \left\lfloor \frac{n}{d} \right\rfloor$$