THE BASIC AXIOMS AND SOME SIMPLE THEOREMS OF INTEGER ARITHMETIC

1. THE BASIC VOCABULARY

I. The **logical connectives:**

1. The **propositional connectives:**
   a. the *negation symbol* ("$\neg \dots$", read as "not ...", or "it is not the case that ..."),
   b. the *conjunction symbol* ("$\dots \wedge \dots$", read as "...and..."),
   c. the *disjunction symbol* ("$\dots \vee \dots$", read as "...or..."),
   d. the *implication symbol* ("$\dots \longrightarrow \dots$", read as "...implies...", or "if,...then..."),
   e. the *biconditional symbol* ("$\dots \longleftrightarrow \dots$", read as "...if and only if..."),
2. The **quantifiers:**
   a. the *existential quantifier* ("$\exists \dots$", read as "there exists ... such that");
   b. the *universal quantifier* ("$\forall \dots$", read as "for all ...");
3. The **right and left parentheses and the comma.**

II. The **letter variables:** a, b, ..., i, j, k, ..., m, n, p, q, ..., x, y, z, ... (In principle, any symbol can be used as a variable, provided you declare it as such. This includes Greek letters such as α, β, etc., Hebrew or Arabic letters, weird symbols such as $\diamondsuit$ or $\clubsuit$,

II. **The arithmetical symbols:**

a. the *constants* "0" ("zero") and "1" ("one"),
b. the *symbols for the arithmetical operations*: "+" ("plus") and "$\cdot$" ("times", sometimes written "$\times$"),
c. the *minus* (or *negative*) *symbol*: "$-$" (read "minus", or "negative"),
d. the *predicates:* "$=$" ("is equal to", or "equals") , "$<$" ("is less than", or "is smaller than"), "$>$" ("is larger than"), "$\leq$" ("is less than or equal to", or "is not greater than"), "$\geq$" ("is greater than or equal to", or "is not smaller than").

If you want, you can also include the predicates "$\in \mathbb{N}$" ("belongs to $\mathbb{N}$", or "is a natural number", or "is a nonnegative integer") and "$\in \mathbb{N}$" ("belongs to $\mathbb{Z}$", or "is an integer"). This, however, is not necessary, strictly speaking, because

A. If it is clear that we are just talking about the integers, then *everything is an integer*, so there is not need to say "x is an integer" every time we bring in an object x, because x couldn't possibly be anything other than an integer. So if this is the case then "$\in \mathbb{Z}$" is not needed.

B. The predicate "$\in \mathbb{N}$" is unnecessary, because instead of saying "$x \in \mathbb{N}$" you could just say "$x \geq 0$", or "$0 \leq x$."

On the other hand,

C. If you include the predicate "$\in \mathbb{N}$" then you do not need to include the predicates $<$, $>$, $\leq$, and $\geq$, because you can *define* them in terms of the other symbols together with "$\in \mathbb{N}$". (This is what Problem 4 of page 5 of the book is about.)

D. If you want to talk about integers and also things that are not integers (e.g., sets, lists, integers modulo n), then you need the predicate "$\in \mathbb{Z}$ to specify when the things you are talking about are supposed to be integers.

Here are four versions of the basic vocabulary. Version I is used if the universe of discourse is $\mathbb{Z}$, i.e., if we are talking about integers only. Version II can be substituted for Version I. Version III is used if the universe of discourse contains $\mathbb{Z}$ and other things as well, i.e., if we are talking about integers and also other things. Version IV can be substituted for Version III.

THE BASIC VOCABULARY OF INTEGER ARITHMETIC, VERSION I

$$\neg \quad \wedge \quad \vee \longrightarrow \quad \longleftrightarrow \quad \exists \quad \forall \quad (\quad) \quad ,$$

$$= \quad < \quad > \quad \leq \quad \geq \quad 0 \quad 1 \quad + \quad - \quad \cdot$$

and the variables.

THE BASIC VOCABULARY OF INTEGER ARITHMETIC, VERSION II

$$\neg \quad \wedge \quad \vee \longrightarrow \quad \longleftrightarrow \quad \exists \quad \forall \quad (\quad) \quad ,$$

$$= \quad \in \mathbb{N} \quad 0 \quad 1 \quad + \quad - \quad \cdot$$

and the variables.

THE BASIC VOCABULARY OF INTEGER ARITHMETIC, VERSION III

$$\neg \quad \wedge \quad \vee \longrightarrow \quad \longleftrightarrow \quad \exists \quad \forall \quad (\quad) \quad ,$$

$$= \quad < \quad > \quad \leq \quad \geq \quad \in \mathbb{Z} \quad 0 \quad 1 \quad + \quad - \quad \cdot$$

and the variables.

THE BASIC VOCABULARY OF INTEGER ARITHMETIC, VERSION IV

$\neg \quad \wedge \quad \vee \longrightarrow \quad \longleftrightarrow \quad \exists \quad \forall \quad (\quad) \quad ,$

$= \quad \in \mathbb{N} \quad \in \mathbb{Z} \quad 0 \quad 1 \quad + \quad - \quad \cdot$

and the variables.

THE AXIOMS

The axioms give us some basic properties of addition, multiplication, the "negative of" predicate, 0, 1, $<$, $\leq$, $>$, and $\geq$.

We divide these axioms into three groups:

1. The **integral domain axioms**, i.e., the axioms that deal with addition, multiplication, the "negative of" predicate, 0, and 1.
2. The **order axioms**, i.e., the axioms that deal with $<$, $\leq$, $>$, and $\geq$.
3. The well-ordering principle.

THE AXIOMS OF INTEGER ARITHMETIC

INTEGRAL DOMAIN AXIOMS

IDA1. $\forall x, \forall y, x + y = y + x.$

IDA2. $\forall x, \forall y, x.y = y.x.$

IDA3. $\forall x, \forall y, \forall z, (x + y) + z = x + (y + z).$

IDA4. $\forall x, \forall y, \forall z, (x.y).z = x.(y.z).$

IDA5. $\forall x, \forall y, \forall z, (x + y).z = x.z + y.z.$

IDA6. $\forall x, x + 0 = x.$

IDA7. $\forall x, x + (-x) = 0.$

IDA8. $\forall x, x.1 = x.$

IDA9. $\forall x, \forall y, \forall z, \Big((y.x = z.x \wedge \neg x = 0) \longrightarrow y = z\Big).$

IDA10. $\neg 1 = 0.$

ORDER AXIOMS

OA1. $\forall x, \forall y, (x > y \longleftrightarrow y < x)$

OA2. $\forall x, \forall y, (x \leq y \longleftrightarrow (x < y \vee x = y))$

OA3. $\forall x, \forall y, (x \geq y \longleftrightarrow (x > y \vee x = y))$

OA4. $\forall x, \forall y, ((0 < x \wedge 0 < y) \longrightarrow 0 < x + y)$

OA5. $\forall x, \forall y, ((0 < x \wedge 0 < y) \longrightarrow 0 < x.y)$

OA6. $\forall x, \forall y, (x < y \longleftrightarrow 0 < y + (-x))$

OA7. $\forall x, (0 \leq x \vee x \leq 0)$

OA8. $\neg\, 0 < 0$

THE WELL-ORDERING PRINCIPLE

WOP. Let u, v be variables, let $p(u)$ be a formula not containing v at all and containing no quantifiers $\exists u$, $\forall u$. Let $p(v)$ be the formula obtained from $p(u)$ by substituting v for u throughout $p(u)$. Then

$$(\exists u, (0 \leq u \wedge p(u))) \longrightarrow (\exists u, (0 \leq u \wedge p(u) \wedge \forall v, ((0 \leq v \wedge p(v)) \longrightarrow u \leq v))) .$$

THEOREM T1. $-0 = 0.$

PROOF.

$$-0 = (-0) + 0 \qquad \boxed{\text{IDA6}}$$

and

$$(-0) + 0 = 0 \qquad \boxed{\text{IDA7}}$$

So $-0 = 0$. **THE END**

DEFINITION D1. $2 = 1 + 1$.

DEFINITION D2. $3 = 2 + 1$.

DEFINITION D3. $4 = 3 + 1$.

THEOREM T2. $2 + 2 = 4$.

PROOF.

$$\begin{aligned} 2 + 2 &= 2 + (1 + 1) && \boxed{\text{D1}} \\ &= (2 + 1) + 1) && \boxed{\text{IDA3}} \\ &= 3 + 1) && \boxed{\text{D2}} \\ &= 4 && \boxed{\text{D3}} \end{aligned}$$

THE END

THEOREM T3. $2.2 = 4$.

PROOF.

$$\begin{aligned} 2.2 &= 2.(1 + 1) && \boxed{\text{D1}} \\ &= 2.1 + 2.1 && \boxed{\text{IDA5}} \\ &= 2 + 2) && \boxed{\text{IDA8}} \\ &= 4 && \boxed{\text{T2}} \end{aligned}$$

THE END

THEOREM T4. $\forall x, x.0 = 0$.

PROOF. Let x be arbitrary. Then

$$\begin{aligned} x.0 &= x.0 + 0 \\ &= x.0 + (x.0 + (-(x.0))) \\ &= (x.0 + x.0) + (-(x.0)) \\ &= x.(0 + 0) + (-(x.0)) \\ &= x.0 + (-(x.0)) \\ &= 0 \end{aligned}$$

THE END

THEOREM T5. $\forall x, \forall y, \forall z, x.(y + z) = x.y + x.z$.

PROOF. Let x, y, z be arbitrary. Then

$$\begin{aligned} x.(y + z) &= (y + z).x && \boxed{\text{IDA2}} \\ &= y.x + z.x && \boxed{\text{IDA5}} \\ &= x.y + x.z && \boxed{\text{IDA2}} \end{aligned}$$

THE END

THEOREM T6. $(-1).(-1) = 1$.

PROOF.

$$\begin{aligned}
(-1).(-1) &= (-1).(-1) + 0 \\
&= (-1).(-1) + (1 + (-1)) \\
&= (-1).(-1) + (1 + (-1).1) \\
&= (-1).(-1) + ((-1).1 + 1) \\
&= ((-1).(-1) + (-1).1) + 1 \\
&= (-1).((-1) + 1) + 1 \\
&= (-1).(1 + (-1)) + 1 \\
&= (-1).0 + 1 \\
&= 0 + 1 \\
&= 1 + 0 \\
&= 1
\end{aligned}$$

THE END

THEOREM T7. $\forall x, (-1).x = -x$.

PROOF. Let x be arbitrary. Then

$$\begin{aligned}
(-1).x &= (-1).x + 0 \\
&= (-1).x + (x + (-x)) \\
&= ((-1).x + x) + (-x) \\
&= (x.(-1) + x) + (-x) \\
&= (x.(-1) + x.1) + (-x) \\
&= x.((-1) + 1) + (-x) \\
&= x.(1 + (-1)) + (-x) \\
&= x.0 + (-x) \\
&= 0 + (-x) \\
&= (-x) + 0 \\
&= -x\,.
\end{aligned}$$

THE END

THEOREM T8. $\forall x, x.(-1) = -x$.

PROOF. Let x be arbitrary. Then $x.(-1) = (-1).x = -x$.

THEOREM T9. $\forall x, -(-x) = x$.

PROOF. Let x be arbitrary. Then

$$\begin{aligned}
-(-x) &= (-x).(-1) \\
&= (x.(-1)).(-1) \\
&= x.((-1).(-1)) \\
&= x.1 \\
&= x
\end{aligned}$$

THE END

THEOREM T10. $\forall x, \forall y, -(x+y) = (-x)+(-y)$.

PROOF. Let x, y be arbitrary. Then

$$\begin{aligned} -(x+y) &= (x+y).(-1) \\ &= x.(-1)+y.(-1) \\ &= (-x)+(-y) \end{aligned}$$

THE END

DEFINITION D4. $\forall x, \forall y, x-y = x+(-y)$.

THEOREM T11. $\forall x, \forall y, \forall z, (x-y=z \longleftrightarrow x=y+z)$.

PROOF. Let x, y, z be arbitrary. Assume $x-y=z$. Then

$$\begin{aligned} x &= x+0 \\ &= x+(y+(-y)) \\ &= x+((-y)+y) \\ &= (x+(-y))+y \\ &= (x-y)+y \\ &= z+y \\ &= y+z \end{aligned}$$

So $x-y=z \longrightarrow x=y+z$.

Now suppose $x=y+z$. Then

$$\begin{aligned} x-y &= x+(-y) \\ &= (y+z)+(-y) \\ &= (z+y)+(-y) \\ &= z+(y+(-y)) \\ &= z+0 \\ &= z \end{aligned}$$

So $x=y+z \longrightarrow x-y=z$. **THE END**

THEOREM T12. $\forall x, \forall y, -(x-y) = y-x$.

PROOF. Let x, y be arbitrary. Then

$$\begin{aligned} -(x-y) &= (x-y).(-1) \\ &= (x+(-y)).(-1) \\ &= x.(-1)+(-y).(-1) \\ &= x.(-1)+((y.(-1)).(-1)) \\ &= (-x)+y.((-1).(-1)) \\ &= (-x)+y.1 \\ &= (-x)+y \\ &= y+(-x) \\ &= y-x \end{aligned}$$

THE END

DEFINITION D5. $\forall x, (x \text{ is even } \longleftrightarrow \exists y, x = 2.y)$.

DEFINITION D6. $\forall x, (x \text{ is odd } \longleftrightarrow \exists y, x = 2.y + 1)$.

THEOREM T13. $\forall x, \forall y, ((x \text{ is even } \wedge y \text{ is even }) \longrightarrow x + y \text{ is even })$

PROOF. Let x, y be arbitrary. Suppose x and y are even. Since x is even, $\exists u, x = 2.u$. Pick one such u and call it a. Since y is even, $\exists u, y = 2.u$. Pick one such u and call it b. Then $x = 2.a$ and $y = 2.b$. So $x + y = 2.(a + b)$. So $\exists u, x + y = 2.u$. So $x + y$ is even. **THE END**

THEOREM T14. $\forall x, \forall y, ((x \text{ is even } \wedge y \text{ is odd }) \longrightarrow x + y \text{ is odd })$

PROOF. Let x, y be arbitrary. Suppose x is even and y is odd. Since x is even, $\exists u, x = 2.u$. Pick one such u and call it a. Since y is odd, $\exists u, y = 2.u + 1$. Pick one such u and call it b. Then $x = 2a$ and $y = 2.b + 1$. So $x + y = 2.(a + b) + 1$. So $\exists u, x + y = 2.u + 1$. So $x + y$ is odd. **THE END**

THEOREM T15. $\forall x, \forall y, ((x \text{ is odd } \wedge y \text{ is odd }) \longrightarrow x + y \text{ is even })$

PROOF. Let x, y be arbitrary. Suppose x and y are odd. Since x is odd, $\exists u, x = 2.u + 1$. Pick one such u and call it a. Since y is odd, $\exists u, y = 2.u + 1$. Pick one such u and call it b. Then $x = 2a + 1$ and $y = 2.b + 1$. So $x + y = (2.a + 1) + (2.b + 1) = 2.(a + b + 1)$. So $\exists u, x + y = 2.u$. So $x + y$ is even. **THE END**

THEOREM T16. $\forall x, \forall y, (x \text{ is even } \longrightarrow x.y \text{ is even })$

PROOF. Let x, y be arbitrary. Suppose x is even. Then $\exists u, x = 2.u$. Pick one such u and call it a. Then $x = 2.a$. So $x.y = (2.a).y = 2.(x.y)$. So $\exists u, x.y = 2.u$. So $x.y$ is even. **THE END**

THEOREM T17. $\forall x, \forall y, ((x \text{ is odd } \wedge y \text{ is odd }) \longrightarrow x.y \text{ is odd })$

PROOF. Let x, y be arbitrary. Suppose x and y are odd. Since x is odd, $\exists u, x = 2.u + 1$. Pick one such u and call it a. Since y is odd, $\exists u, y = 2.u + 1$. Pick one such u and call it b. Then $x = 2a + 1$ and $y = 2.b + 1$. So $x.y = (2.a+1).(2.b+1) = 4.a.b+2.a+2.b+1 = 2(2.a.b+a+b)+1$. So $\exists u, x.y = 2.u+1$. So $x.y$ is odd. **THE END**

THEOREM T18. $\forall x, (x \text{ is odd } \longleftrightarrow x + 1 \text{ is even })$

PROOF. Let x be arbitrary. Suppose x is odd. Then $\exists u, x = 2.u+1$. Pick one such u and call it a. Then $x + 1 = (2.a + 1) + 1 = 2.(a + 1)$. So $\exists u, x + 1 = 2.u$. So $x + 1$ is even.

Now suppose $x+1$ is even. Then $\exists u, x+1 = 2.u$. Pick one such u and call it a. Then $x + 1 = 2.a$. Therefore $x = 2.a - 1 = 2.(a - 1) + 1$. So $\exists u, x = 2.u + 1$. So x is odd. **THE END**

THEOREM T19. $\forall x, x \leq x$.

PROOF. Let x be arbitrary. Then $x \leq x \longleftrightarrow (x < x \vee x = x)$ by OA2. But $x = x$, so "$x < x \vee x = x$" is true, and then $x \leq x$. **THE END**

THEOREM T20. $\forall x, \forall y, (x < y \longleftrightarrow 0 < y - x)$.

PROOF. This follows trivially from OA6 and D4. **THE END**

THEOREM T21. $\forall x, \forall y, (x \leq y \longleftrightarrow 0 \leq y - x)$.

PROOF. Let x, y be arbitrary. Suppose $x \leq y$. Then $x < y \vee x = y$ by OA2. If $x < y$ then $0 < y + (-x)$ by OA6, and $y + (-x) = y - x$ by D4, so $0 < y - x$, and then $0 \leq y - x$ by OA2. If $x = y$ then $y - x = x - x = x + (-x) = 0$, so $\leq y - x$, because $0 \leq 0$ by T19. So in both cases ($x < y$ and $x = y$) the conclusion $0 \leq y - x$ follows. Therefore $x \leq y \longrightarrow 0 \leq y - x$.

Now suppose $0 \leq y - x$. Then $0 < y - x \vee 0 = y - x$ by OA2. If $0 = y - x$ then

$$y = y + 0 = y + (x + (-x)) = y + ((-x) + x) = (y + (-x)) + x$$

$$= (y - x) + x = 0 + x = x + 0 = x\,,$$

so $y = x$. Then $x \leq y$ by OA2. If $0 < y - x$, then $0 < y + (-x)$, so $x < y$ by OA6, and then $x \leq y$ by OA2. So in both cases ($0 < y - x$ and $0 = y - x$) the conclusion $x \leq y$ follows. Therefore $0 \leq y - x \longrightarrow x \leq y$.

Since $x \leq y \longrightarrow 0 \leq y - x$ and $0 \leq y - x \longrightarrow x \leq y$, the conclusion $x \leq y \longrightarrow 0 \leq y - x$ follows. **THE END**

THEOREM T22. $\forall x, \forall y, ((0 \leq x \wedge 0 < y) \longrightarrow 0 < x + y)$.

PROOF. Let x, y be arbitrary. Assume that $0 \leq x \wedge 0 < y$. Then $0 = x$ or $0 < x$ by OA2. If $0 = x$ then $x + y = 0 + y = y + 0 = y$, so the fact that $0 < y$ implies that $0 < x + y$. If $0 < x$ then OA5 implies $0 < x + y$. **THE END**

THEOREM T23. $\forall x, \forall y, ((0 \leq x \wedge 0 \leq y) \longrightarrow 0 \leq x + y)$.

PROOF. Let x, y be arbitrary. Assume that $0 \leq x \wedge 0 \leq y$. If $0 < x$ or $0 < y$ we can use T22 and conclude that $0 < x + y$, so $0 \leq x + y$. If $x = 0$ and $y = 0$ then $x + y = 0 + 0 = 0$, so $0 \leq x + y$. **THE END**

THEOREM T24. $\forall x, \forall y, \forall z, \forall u, ((x \leq y \wedge z < u) \longrightarrow x + z < y + u)$.

PROOF. Let x, y, z, u be arbitrary. Assume that $x \leq y \wedge z < u$. Then $0 \leq y - x$ by T20, and $0 < u - z$ by T21. So $0 < (y - x) + (u - z)$ by T22. But $(y - x) + (u - z) = (y + u) - (x + z)$. So $0 < (y + u) - (x + z)$, and then $x + z < y + u$ by T14. **THE END**

THEOREM T25. $\forall x, \forall y, \forall z, \forall u, ((x \leq y \wedge z \leq u) \longrightarrow x + z \leq y + u)$.

PROOF. Let x, y, z, u be arbitrary. If $x < y$ or $z < u$ then we can apply T24 and conclude that $x + z < y + u$, so $x + z \leq y + u$. If $x = y$ and $z = u$ then $x + z = y + u$, so $x + z \leq y + u$. **THE END**

THEOREM T26. $\forall x, \forall y, ((0 \leq x \wedge 0 \leq y) \longrightarrow 0 \leq x.y)$.

PROOF. Let x, y be arbitrary. Assume that $0 \leq x \wedge 0 \leq y$. If both $\neg x = 0$ and $\neg y = 0$, then OA2 implies that $0 < x$ and $0 < y$, so $0 < x.y$ by OA5, and then $0 \leq x.y$ by OA2. If $x = 0 \vee y = 0$ then $x.y = 0$ by T4, so $0 \leq x.y$, because $0 \leq 0$. **THE END**

THEOREM T27. $\forall x, \forall y, \forall z, ((x \leq y \wedge 0 \leq z) \longrightarrow x.z \leq y.z)$.

PROOF. Let x, y, z be arbitrary. Assume that $x \leq y \wedge 0 \leq z$. Then $0 \leq y - x$ by T21. So $0 \leq (y - x).z$ by T26. But

$$(y - x).z = (y + (-x)).z = y.z + (-x).z = y.z + ((-1).x).y$$

$$= y.z + (-1).(x.y) = y.z + (-(x.y)) = y.z - x.y\,.$$

So $0 \leq y.z - x.z$, and then T21 tells us that $x.z \leq y.z$. **THE END**

THEOREM T28. $\forall x, \forall y, (((\neg\, x = 0) \wedge \neg\, y = 0) \longrightarrow (\neg\, x.y = 0))$.

PROOF. Let x, y be arbitrary. Assume that $(\neg x = 0) \wedge \neg y = 0$. By OA7, $0 \leq x \vee x \leq 0$. If $0 \leq x$, then $0 < x$, because $0 < x \vee 0 = x$ by OA2, and $\neg 0 = x$. If $x \leq 0$, then $x < 0$, because $x < 0 \vee x = 0$ by OA2, and $\neg x = 0$, and this implies that $0 < -x$, because OA6 says that $x < 0 \longleftrightarrow 0 < 0 + (-x)$, and $0 + (-x) = -x$. So "$0 < x \vee 0 < -x$" is true if $0 \leq x$ and also if $x \leq 0$. Since $0 \leq x \vee x \leq 0$, we have established that $0 < x \vee 0 < -x$. Similarly, $0 < y \vee 0 < -y$.

So one of the following four possibilities hold:

(1) $0 < x \wedge 0 < y$,

(2) $0 < x \wedge 0 < -y$,

(3) $0 < -x \wedge 0 < y$,

(4) $0 < -x \wedge 0 < -y$.

If (1) holds, then $0 < x.y$ by OA5. Therefore $\neg x.y = 0$, because if $x.y = 0$ it would follow that $0 < 0$, contradicting OA8.

If (2) holds, then $0 < x.(-y)$ by OA5. Therefore $\neg x.(-y) = 0$, because if $x.(-y) = 0$ it would follow that $0 < 0$, contradicting OA8. Then $\neg x.y = 0$, because if $x.y = 0$ we would have $x.(-y) = x.((-1).y) = (x.(-1)).y = ((-1).x).y) = (-1).(x.y) = -(x.y) = -0 = 0$, contradicting the fact that $\neg x.(-y) = 0$.

Cases (3) and (4) are handled similarly. **THE END**

THEOREM T29. $\forall x, \forall y, ((x \leq y \wedge y \leq x) \longrightarrow x = y)$.

PROOF. Let x, y be arbitrary. Suppose $x \leq y \wedge y \leq x$. We prove that $x = y$ by contradiction. Suppose $\neg x = y$. Then OA2 tells us that $x < y \vee x = y$. Since $\neg x = y$, we have $x < y$. Then OA6 and D4 imply that $0 < y - x$. Similarly, $0 < x - y$. Then OA4 implies that $0 < (y - x) + (x - y)$, and a simple calculation shows that $(y - x) + (x - y) = 0$. So $0 < 0$, contradicting OA8. **THE END**

THEOREM T30. $\forall x, \forall y, \forall z, ((x \leq y \wedge y \leq z) \longrightarrow x \leq z)$.

PROOF. Let x, y, z be arbitrary. Suppose $x \leq y \wedge y \leq z$. Then $0 \leq y - x$ and $0 \leq z - y$ by T21. So $0 \leq (y - x) + (z - y)$ by T23. But $(y - x) + (z - y) = z - x$. So $0 \leq z - x$, and then T21 implies $x \leq z$. **THE END**

THEOREM T31. $0 < 1$.

PROOF. OA7 tells us that $0 \leq 1 \vee 1 \leq 0$. We consider separately the two cases $0 \leq 1$ and $1 \leq 0$, and show that $0 < 1$ in each case.

First suppose that $0 \leq 1$. Then $0 < 1 \vee 0 = 1$ by OA2. But $\neg 0 = 1$ by IDA10. So $0 < 1$, as desired.

Now suppose that $1 \leq 0$. Then $1 < 0 \vee 1 = 0$ by OA2. But $\neg 1 = 0$ by IDA10. So $1 < 0$. But OA6 tells us that $1 < 0 \longleftrightarrow 0 < 0 + (-1)$. So $0 < 0 + (-1)$, and then $0 < -1$. It then follows from OA4 that $0 < (-1).(-1)$. But $(-1).(-1) = 1$ by T6. So $0 < 1$, as desired. **THE END**

THEOREM T32. $-1 < 0$.

PROOF. OA6 implies that $-1 < 0 \longleftrightarrow 0 < 0 + (-(-1))$. But $-(-1) = 1$ by T9. So $-1 < 0 \longleftrightarrow 0 < 1$. Since $0 < 1$ by T31, we have $-1 < 0$. **THE END**

THEOREM T33. $0 < 2$.

PROOF. Since $0 < 1$ by T31, OA5 implies that $0 < 1 + 1$, i.e., that $0 < 2$. **THE END**

THEOREM T34. $2 \neq 0$.

PROOF. Since $0 < 2$ by T33, OA8 implies that $2 \neq 0$, because if $2 = 0$ then "$0 = 0$" would be true, contradicting OA8. **THE END**

THEOREM T35. $\forall x, (x \leq 0 \vee 1 \leq x)$.

PROOF. Let x be arbitrary. Suppose $\neg x \leq 0$. We will prove that $1 \leq x$.

By OA7, $x \leq 0 \vee 0 \leq x$. Since $\neg x \leq 0$, we have $0 \leq x$. Therefore $0 = x \vee 0 < x$ by OA2. But "$0 = x$" isn't true, because if $0 = x$ it would follow that $x \leq 0$, and we are assuming that $\neg x \leq 0$. So $0 < x$.

We want to prove that $1 \leq x$. We do it by contradiction, Suppose $\neg 1 \leq x$. By OA7, $1 \leq x \vee x \leq 1$. Since $\neg 1 \leq x$, we have $x \leq 1$. Therefore $x = 1 \vee x < 1$ by OA2. But "$x = 1$" isn't true, because if $x = 1$ it would follow that $x \leq 1$, and we are assuming that $\neg 1 \leq x$. So $x < 1$.

We have shown that $0 < x \wedge x < 1$. Let $p(u)$ be the statement $u < 1$. Then we have shown that $0 < x \wedge p(x)$ is true, so $\exists u, (0 < u \wedge p(u))$ is true. By the WOP, there exists a smallest y such that $0 < y \wedge p(y)$. That is,

$$\exists y, (0 < y \wedge y < 1 \wedge \forall u, ((0 < u \wedge u < 1) \longrightarrow y \leq u)) .$$

Pick such a y and call it a. Then

$$0 < a \wedge a < 1 \wedge \forall u, ((0 < u \wedge u < 1) \longrightarrow a \leq u) . \qquad (0.0.1)$$

Since $0 < a$, OA5 implies that $0 < a.a$. On the other hand, $a < 1$ implies that $0 < 1 - a$ by T20. Since $0 < a$, we have $0 < a.(1 - a)$ by OA5. That is, $0 < a - a.a$. Therefore T20 tells us that $a.a < a$. In particular, $a.a < 1$, because $a < 1$.

On the other hand, (0.0.1) implies

$$\forall u, ((0 < u \wedge u < 1) \longrightarrow a \leq u) ,$$

and then we can specialize to $u = a.a$, and get

$$(0 < a.a \wedge a.a < 1) \longrightarrow a \leq a.a\,.$$

Since "$0 < a.a \wedge a.a < 1$" is true, we can conclude that $a \leq a.a$. But this contradicts the fact that $a.a < a$. (If $a \leq a.a$ and $a.a < a$, then $0 \leq a.a - a$ by T21, and $0 < a - a.a$ by OA6, so $0 < (a.a - a) + (a - a.a)$ by T18, and then $0 < 0$, contradicting OA8.)

So the assumption that $\neg 1 \leq x$ has led us to a contradiction. Hence $1 \leq x$. **THE END**

THEOREM T36. $\forall x, \forall y, (x \leq y \vee y + 1 \leq x)$.

PROOF. Let x, y be arbitrary. Suppose $\neg x \leq y$. Using T35, we find that $x - y \leq 0 \vee 1 \leq x - y$. If $x - y \leq 0$, then T25 would imply $x \leq y$, contradicting the assumption that $\neg x \leq y$. So $\neg x - y \leq 0$. Therefore $1 \leq x - y$. Then T25 implies $y + 1 \leq x$. **THE END**

THEOREM T37. $\forall x, (x \leq 0 \vee x = 1 \vee 2 \leq x)$.

PROOF. Let x be arbitrary. Suppose $\neg x \leq 0$. Then T35 implies $1 \leq x$, and T36 implies $x \leq 1 \vee 1 + 1 \leq x$. If $x \leq 1$, then T29 implies $x = 1$, since $1 \leq x$ and $x \leq 1$. If $1 + 1 \leq x$, then $2 \leq x$. **THE END**

THEOREM T38. $\forall x, (x \text{ is even } \vee\ x \text{ is odd})$.

PROOF. Let $q(u)$ be the statement "$0 \leq u \wedge (u \text{ is even } \vee\ u \text{ is odd})$". Let $p(u)$ be the statement $\neg q(u)$. We will prove that $q(u)$ is true for all u such that $0 \leq u$. We do this by contradiction Suppose $\forall u, (0 \leq u \longrightarrow q(u))$ was not true. Then $\exists u, (0 \leq u \wedge p(u))$. By the WOP, there exists a smallest u such that $p(u)$. That is,

$$\exists u, \Big(0 \leq u \wedge p(u) \wedge \forall v, ((0 \leq v \wedge p(v)) \longrightarrow u \leq v)\Big)\,.$$

Pick one such u and call it s. Then

$$0 \leq s \wedge \neg \Big(s \text{ is even } \vee\ s \text{ is odd}\Big)\,,$$

and $s \leq v$ for every v such that $0 \leq v$ and v is neither even nor odd.

It follows that $\neg\, s = 0$, because 0 is even, so if $s = 0$ then "s is even $\vee$ s is odd"would be true. Since $0 \leq s$, OA2 implies that $0 < s$.