CHALLENGE PROBLEM 1

LEANDRO RIBEIRO

Axiom (†). There exists a subset $\mathbb{N} \subseteq \mathbb{Z}$ with the following properties:

(1) If $m, n \in \mathbb{N}$, then $m + n \in \mathbb{N}$.
(2) If $m, n \in \mathbb{N}$, then $mn \in \mathbb{N}$.
(3) $0 \notin \mathbb{N}$.
(4) For every $m \in \mathbb{Z}$, we have $m \in \mathbb{N}$, $m = 0$, or $-m \in \mathbb{N}$.

Definition. The **successor function** on the integers is defined by $s(x) := x + 1$. For $m \geq 1$, we define $s^{m+1}(x)$ recursively by $s^{m+1}(x) := s(s^m(x))$.

Axiom(∗). For all $m \geq 1$, $s^m(0) \neq 0$.

Axiom(∗∗). For all x $\in \mathbb{Z}$, there is $m \geq 0$ such that $s^m(x) = 0$ or $s^m(0) = x$.

Definition. The set of **successors of zero** is defined to be

$$N := \{x \in \mathbb{Z} | \exists m \geq 1 s^m(0) = x\}$$

Prove the following proposition.

Proposition. *Assume that the integers satisfy* (∗) *and* (∗∗). *Then, the set* N *satisfies axiom* (†). *That is to say,* N *satisfies the four conditions of the axiom.*

Proof. (1) Let P(n) be the statement "if $m \in N$, then $m + n \in N$". Because $m \in N$, there exists some $y \geq 1$ such that $s^y(0) = m$. Let's first observe P(1)

Base. n = 1. $m + 1 = s^y(0) + 1 = s(s^y(0))$, because $m \in N$ and the definition of the successor function. Also by definition of the successor function, $s(s^y(0)) = s^{y+1}(0)$. Clearly, $y + 1 > y \geq 1$. Thus, for $m + 1$ there exists $y + 1 > 1$ such that $s^{y+1}(0) = m + 1$, $m + 1 \in N$, and the proposition holds.

Successor. Assume P(n) holds. That is, $m + n \in N$. By definition, this means there exists some $y \geq 1$ such that $s^y(0) = m + n$. Consider $m + n + 1$. $m + n + 1 = s(m + n) = s(s^y(0))$ by definition of the successor function. By induction, we know $m + n = s^y(0) \in N$. Thus,

Date: March 24, 2017.

$s(s^y(0)) = s^{y+1}(0) \in N$ since for $m + n + 1$ there exists $y + 1 > y \geq 1$ such that $s^{y+1}(0) = m + n + 1$. By the principal of mathematical induction, the proposition holds.

(2) Let P(n) be the statement " If $m \in N$, then $mn \in N$." Observe P(1):

Base. n = 1. $m \cdot 1 = m \in N$.

Successor. Assume P(n) holds. That is, $mn \in \mathbb{N}$. Consider $m(n+1)$. By our axioms for the integers, we may rewrite this as $mn + m$. By induction, $mn \in N$, and we already know $m \in N$. Thus, by the first part of this proposition and induction, $mn + n \in N$.

(3) By our axiom $(*)$, we know $0 \notin N$.

(4) Take $x \in \mathbb{Z}$. Suppose toward a contradiction $x \notin N$, $-x \notin N$, and $x \neq 0$. By axiom $(**)$, there is $m \geq 0$ such that $s^m(x) = 0$ or $s^m(0) = x$. Take x such that $s^m(0) = x$, then by our definition of N, $x \in N$, which contradicts our initial assumption.

$\square$