APPENDIX: AXIOMS FOR ARITHMETIC ON THE NATURAL NUMBERS

1. Introduction

In this appendix we give an axiomatic system for arithmetic on the *natural numbers*, that is, the set of non-negative integers. We denote the set of natural numbers by $\bar{\mathbb{N}}$. The arithmetic functions we consider are s (successor), $+$, and $\cdot$. We also include the order relation $<$ and the constant 0 (of course, $=$ is always included). We will also use s, $+$, $\cdot$, $<$ and 0 for the corresponding symbols of the first order language $\mathcal{L}_{\mathbb{N}}$ for arithmetic on the natural numbers. We will also write $x + y$, $x < y$ (instead of $+(x, y)$, $< (x, y)$), etc. to make it easier to read formulas. We will use $\mathcal{N}$ for the $\mathcal{L}_{\mathbb{N}}$-structure $(\bar{\mathbb{N}}, s, +, \cdot, 0, <)$.

2. The Axioms

We introduce two groups of axioms. The first contains the "algebraic" properties of the basic functions and relations.

Q1. $\forall x(\neg s(x) = 0)$
Q2. $\forall x \forall y(s(x) = s(y) \to x = y)$
Q3. $\forall x(x + 0 = x)$
Q4. $\forall x \forall y(x + s(y) = s(x + y))$
Q5. $\forall x(x \cdot 0 = 0)$
Q6. $\forall x \forall y(x \cdot s(y) = x \cdot y + x)$
Q7. $\forall x(\neg x < 0)$
Q8. $\forall x \forall y(x < s(y) \leftrightarrow x < y \vee x = y)$
Q9. $\forall x \forall y(x < y \vee x = y \vee y < x)$

This collection of nine axioms will be referred to as **Q**.

The second group of axioms is infinite and consists of all instances of *induction*.

IS consists of all sentences of the following form where $\varphi(x, z_1, \ldots, z_n)$ is a formula of $\mathcal{L}_{\mathbb{N}}$:

$$\forall z_1, \ldots \forall z_n \big(\varphi(0, \bar{z}) \wedge \forall x(\varphi(x, \bar{z}) \to \varphi(s(x), \bar{z})) \to \forall x \varphi(x, \bar{z})\big)$$

Q together with **IS** is called *Peano Arithmetic*, abbreviated **PA**.

Clearly, $\mathcal{N} \models \mathbf{PA}$. Furthermore, for any sentence σ that you are likely to encounter in number theory, if $\mathcal{N} \models \sigma$ then $\mathbf{PA} \models \sigma$. However, Kurt Gödel in 1931 published his amazing Incompleteness Theorem which implies that there is some σ such that $\mathcal{N} \models \sigma$ but $\mathbf{PA} \not\models \sigma$.

3. Arithmetic in **PA**.

In this section we give a few examples of how arithmetic on the natural numbers can be developed in **PA**. Note, of course, that since $\mathcal{N} \models \mathbf{PA}$ we know that $\mathcal{N} \models \sigma$ whenever $\mathbf{PA} \models \sigma$. We define the terms 1, 2, etc to be $s(0)$, $s(s(0))$, etc., so every natural number is named by some variable-free term of $\mathcal{L}_{\mathbf{N}}$. We leave it to the reader to suppply a proof of the following fact.

Lemma 3.1. *It $k = l$ then $\mathbf{Q} \models k = l$. If $k \neq l$ then $\mathbf{Q} \models \neg k = l$.*

The next result lists some provable properties of addition.

Lemma 3.2. (a) *If $k + l = n$ then $\mathbf{Q} \models k + l = n$. If $k + l \neq n$ then $\mathbf{Q} \models \neg(k + l = n)$.*
(b) $\mathbf{PA} \models \forall x \forall y (x + y = y + x)$
(c) $\mathbf{PA} \models \forall x \forall y \forall z \big((x + y) + z = x + (y + z)\big)$

Proof. (a) We show that "for every k and n if $k+l = n$ then $\mathbf{Q} \models k+l = n$" holds for all l by induction on l. The base case is $l = 0$: if $k + 0 = n$ then $k = n$, and $\mathbf{Q} \models k + 0 = k$ as desired since this is axiom **Q3.** For the inductive step we assume for some fixed l that "for every k,n if $k + l = n$ then $\mathbf{Q} \models k + l = n$" and we show the same property for $s(l)$. Suppose that $k + s(l)) = n$. Then $n = s(m)$ where $k + l = m$. By the inductive hypothesis $\mathbf{Q} \models k + l = m$, and thus by axiom **Q4**, $\mathbf{Q} \models k + s(l) = s(m)$, as desired. The second assertion is easier (why?).

(b) (outline) We first prove two preliminary facts:
(i) $\mathbf{PA} \models 0 + x = x$, and
(ii) $\mathbf{PA} \models \big((s(x) + y = s(x + y)\big)$.
Both of these use induction (in (ii) on y) and axioms **Q3** and **Q4**. Using these we then show that $\mathbf{PA} \models (x + y = y + x)$ which we do by induction on y, with x as a parameter. By Generalization this yields the conclusion. Details are left to the reader.

(c) (outline) By Generalization it suffices to prove that $\mathbf{PA} \models \big((x + y) + z = x + (y + z)\big)$, which we do by induction on z. Details are left to the reader. □

We have a similar result about multiplication.

Lemma 3.3. (a) *If $k \cdot l = n$ then $\mathbf{Q} \models k \cdot l = n$. If $k \cdot l \neq n$ then $\mathbf{Q} \models \neg(k \cdot l = n)$.*
(b) $\mathbf{PA} \models \forall x \forall y (x \cdot y = y \cdot x)$.
(c) $\mathbf{PA} \models \forall x \forall y \forall z \big((x \cdot y) \cdot z = x \cdot (y \cdot z)\big)$.

As another example we state some results about $<$.

Lemma 3.4. (a) $\mathbf{PA} \models \forall x (\neg x < x)$
(b) $\mathbf{PA} \models \forall x \forall y \forall z (x < y \wedge y < z \rightarrow x < z)$
(c) $\mathbf{PA} \models \forall x \forall y (x < y \rightarrow \neg y < x)$
(d) *For every $n > 0$,* $\mathbf{Q} \models \forall x \big(x < n \leftrightarrow (x = 0 \vee x = 1 \vee \cdots \vee x = n - 1)\big)$

Corollary 3.1. *If $k < l$ then $\mathbf{Q} \models (k < l)$. If $k \not< l$ then $\mathbf{Q} \models \neg(k < l)$.*

4. Representing Relations in **PA**

It is easy to define the set of primes or the divisibility relation in $\mathcal{N}$. We require a stronger property which implies that the properties of the defined relations depend only on the axioms in **PA**. This stronger preperty is *representability*.

Definition 4.1. An n-ary relation R on $\bar{\mathbb{N}}$ is *representable in* **PA** *by the formula* $\varphi(x_1, \ldots, x_n)$ iff for every $k_1, \ldots, k_n \in \bar{\mathbb{N}}$, if $R(k_1, \ldots, k_n)$ holds then $\mathbf{PA} \models \varphi(k_1, \ldots, k_n)$, and if $R(k_1, \ldots, k_n)$ fails then $\mathbf{PA} \models \neg\varphi(k_1, \ldots, k_n)$.

Lemma 3.1 says precisely that the relation $=$ is representable in (**Q** hence in) **PA** by the formula $x = y$. Corollary 3.1 says that the relation $<$ is representable in (**Q** hence in) **PA** by the formula $x < y$.

As a more complicated example we show that the divisibility relation is representable in **PA**.

Lemma 4.1. *There is a formula $\delta(x, y)$ representing the divisibility relation in* **PA**.

Proof. We define $\delta(x, y)$ as $\exists z(z \leq y \wedge y = x \cdot z)$. Suppose that $k|l$. Then there is some $n \leq l$ such that $l = k \cdot n$. It follows (see Lemma 3.3(a) and Corollary 3.1) that $\mathbf{PA} \models (n \leq l \wedge l = k \cdot n)$, hence $\mathbf{PA} \models \delta(k, l)$. If $k \not| l$ then for each $n \leq l$ we have $l \neq k \cdot n$, and hence $\mathbf{PA} \models (l \neq k \cdot n)$ by Lemma 3.3(a). By Lemma 3.4(d) it follows that $\mathbf{PA} \models \neg\delta(k, l)$. □

Using Lemma 4.1 we easily conclude that there is a formula $\pi(x)$ representing the set of primes in **PA**.

We say that the n-ary function F is representable in **PA** provided the $(n+1)$-ary relation $F(x_1, \ldots, x_n) = y$ is representable in **PA**. For example, Lemmas 3.2(a) and 3.3(a) imply that the functions $+$ and $\cdot$ are representable in (**Q** hence in) **PA** by the formulas $x + y = z$ and $x \cdot y = z$ respectively.