Chapter I
The Peano Axioms

1 Historical Notes

In 1889 Giuseppe Peano published *The Principles of Arithmetic Presented by a New Method*[1] in which he presented axioms which were to define and codify the properties of the natural numbers, clarifying and organizing the work of Hermann Grassmann twenty years earlier and Charles Sanders Pierce in 1881.

Whole numbers and their arithmetic were studied by many people, notably the ancient Greeks, who used geometrical methods founded on Euclid's Axioms[2] to construct sums, products and deduce factorization theorems. Greek mathematics based on geometry was the ‘‘gold standard’’ of logical rigor for thousands of years and this included their number theory.

Euclid's axiomatics posited an ontology[3] consisting of points, lines and other geometrical objects and an epistemology based on Aristotelian logic of the ‘‘if-then’’ type.

Implicit in this approach was reliance on our intuition about the geometry of the space around us, and our innate sense of time, in particular the concept of ‘‘consecutive.’’ It was assumed that there were things in the ideal world, abstract

[1] This very short book, originally written in Latin as *Arithmetices Principia, Nova Methodo Exposita*, is readily available on the internet. One version with parallel English translation by Vincent Verheyen may be found (currently, 2025) at `https://github.com/mdnahas/Peano_Book/blob/master/Peano.pdf`.

[2] Euclid of Alexandria circa 300 BCE reputedly assembled and organized and improved the work of previous mathematicians in *The Elements*. Earlier mathematicians who probably contributed included Pythagoras circa 570-495 BCE, Hippocrates of Chios 470-410 BCE and Eudoxus of Cnidus circa 408-355 BCE. It is the most successful textbook ever written, having been used continuously in one form or another for over 2000 years as the primary text for mathematical instruction in Europe and the Islamic countries.

[3] The word ‘‘ontology’’ refers to the objects presumed to exist in a subject area. ‘‘Epistemology’’ on the other hand describes the means by which subject-experts acquire knowledge about these objects.

objects outside of space and time, corresponding to these geometrical lines and points. And saying ‘‘if-then’’ posits that we first declare conditions and then prove facts by consecutive logical maneuvers. This requires a concept of time which must be added to the list of abstract ideal ‘‘things.’’

Since our thoughts about points and lines are founded in our perception of space, and our arguments about them depend on time, it is quite puzzling about how, exactly, mortal humans can obtain knowledge of objects *outside* of space and time. This aspect was the focus of considerable wrangling over millennia, but we will avoid the issue here.

One of Euclid's axioms, his fifth[4], called the Parallel Postulate, implied that parallel lines never meet. This axiom was widely considered to be unnecessary, and attempts were made over thousands of years to show that the other axioms implied the Parallel Postulate, which could therefore be excised from the list of independent assumptions used to create Euclidean geometry.

In 1829 Nikolai Lobachevsky and independently in 1831 János Bolyai published accounts of geometry that satisfied all the axioms except the fifth. This called millennia of geometrical intuition into question, and was quite shocking at the time.

Also shocking were revelations by George Cantor in the period from 1874 to 1884 on infinite sets, such as the set of natural numbers, and the various ‘‘sizes of infinity’’ available to such sets. Some mathematicians accepted and others rejected his approach, but *everyone* realized that infinite sets could not be handled in a cavalier fashion and many thought merely assuming the existence of such sets would provide contradictions.

This turmoil in the geometrical roots of number theory, and concerns about the relationship between our geometrical intuition and the true nature of the world, and severe uncertainty about how to handle infinite sets, led mathematicians to contemplate axiomatics for numbers that did not rely on Euclid's Axioms but retained so far as possible the logical rigor of that subject. Peano proposed a replacement logical structure for arithmetic based on algebraic relations, not geometrical ones, which had become suspect. He also was very careful in his handling of the one infinite set presumed to exist as part of his axioms.

---

[4] The Parallel Postulate is stated as follows in Book I of *The Elements*[4].

Postulate 5.
That, if a straight line falling on two straight lines makes the interior angles on the same side less than two right angles, the two straight lines, if produced indefinitely, meet on that side on which are the angles less than the two right angles.

Parallel Lines are defined in Book I by:

Definition 23
Parallel straight lines are straight lines which, being in the same plane and being produced indefinitely in both directions, do not meet one another in either direction.

It is proved in Book I that Postulate 5 together with the other axioms implies that there are parallel lines.

These nine axioms are not statements to be proved: they are intended to represent essential features of what we imagine integers *to be*. From these axioms the ordering on the natural numbers and the arithmetical operations of addition and multiplication with their interlinked properties, are generated.

These axioms are statements about natural numbers and, in one case, sets containing natural numbers. So any ‘‘model’’ of the natural numbers, as originally conceived by Peano, must account for this. It must contain objects which are to behave as natural numbers do, reflecting our intuition about numbers. And it contains other objects, sets, which might have these natural numbers as members. It is due to these last objects, the reference to sets of natural numbers in the axioms and the means by which they may be deduced to exist, that the structure Peano created is called ‘‘second order.’’

This particular model is nowadays denoted PA_2.

A certain amount of set theory with its ‘‘element of’’ relation is presupposed, **at least for finite sets,** and a certain number of facts that pertain to sets are needed, even infinite sets if any of these should appear.

For instance we say sets are equal precisely when they have all the same elements.

Making declarative statements about natural numbers evidently requires considerable amounts of finite set theory. What is such a statement but a finite ordered collecton of symbols subject to ‘‘grammar rules’’ and an interpretation? We must suppose we understand how to form finite ordered lists, such as ordered pairs of symbols (a, b), ordered triples (a, b, c), and so on.

Surprisingly, Kurt Gödel proved in 1930 that there are sensible statements in any system rich enough to be useful, and which describes natural number arithmetic with addition and multiplication, which cannot be proved to be true or false from within the model. And one of those statements is ‘‘This collection of axioms is consistent.’’

Few mathematicians believe that these simple axioms could be inconsistent: that they could be used to prove the same statement to be both true and false. But Gödel proved that is a *possibility.*

This places a permanent, if tiny, ‘‘asterisk’’ on *any* attempt to reformulate arithmetic on unimpeachable logical grounds. Caveat Emptor.

For those who wish to extend their understanding of how formulas and statements involving axioms can be created, and the nature of structures that may be derived from axioms, John Stillwell’s excellent *Reverse Mathematics* [11] is a great place to start.

The reader is also referred to Shawn Hedman’s *A First Course in Logic* [7] and, for historical context and *much* else, *Foundations of Set Theory* [2] by A.A. Fraenkel, Y. Bar-Hillel, and A. Levy.

Our immediate business is the axioms themselves, and the recognition that our understanding of the natural numbers is reflected in these axioms. No trace of our worrisome geometrical intuition remains among them.

2 The Axioms

Axiom One: There is a natural number which we denote 0. The *set* $\mathbb{N}$, whose elements are precisely these natural numbers is, therefore, nonempty. $\mathbb{N}$ will be called here **The Natural Numbers**. The natural number 0 will turn out to behave as 0 *should*, but at this point it is merely a symbol to denote a particular element of $\mathbb{N}$, with properties to be introduced in Axioms Eight and Nine.

This gets us started. At least we are talking about *something*.

The next four axioms codify what we mean by natural numbers being *equal* and how we are authorized to use the equality binary relation between them.

Axiom Two: For every $n \in \mathbb{N}$ we have $n = n$.

Axiom Three: If k and n are natural numbers and $k = n$ then $n = k$.

Axiom Four: If $k \in \mathbb{N}$ and $k = n$ then n is a natural number too.

Axiom Five: If k is a natural number and $k = j$ and $j = n$ then $k = n$.

The next axioms assert the existence of a ''successor'' for each natural number and some properties of these successors. Specifically, for each $n \in \mathbb{N}$ there is an object $S(n)$ defined for it. The association given by S has three properties.

Axiom Six: $S(n)$ is a natural number for each natural number n.

Axiom Seven: For k and n in $\mathbb{N}$, if $S(n) = S(k)$ then $n = k$.

Axiom Eight: $S(n) = 0$ is false for any natural number n.

Finally, we have the **Axiom of Induction**.

Axiom Nine: Suppose X is a set and $0 \in X$ and suppose also that whenever natural number n is in X then $S(n)$ is in X. Then X contains every natural number.

Axiom Nine is not something to be *proven.* It, or some other axiom which implies some of the same things, must be assumed to create a model for the natural numbers. Standard Zermelo-Fraenkel set theory, a *very* rich theory with extensive set-formation resources and upon which most of modern mathematics is based, can be used to create a model of the natural numbers. There, the Axiom of Infinity implies that there is a *set*, usually denoted $\mathbb{N}$, upon which a function S may be explicitly defined and which embodies the nine Peano axioms.

There is one more part of this system to consider. The existence of the set $\mathbb{N}$ is inherent in the statement of several of the axioms, but other sets are allowed in the Peano system. This is part of the ''logic'' used in this system, which connects the axioms and which are used to form statements involving them.

Using ''set builder notation'' these sets are ***only*** those of the form

$$\{ x \in \mathbb{N} \mid P(x) \}$$

where P is an explicit property of natural numbers which refers, in its statement, to natural numbers and the axioms alone, and specifically ***not*** to any set other than $\mathbb{N}$ itself.

For instance if n is a natural number the **initial and terminal segments** determined by n are defined to be

$$\mathrm{I}_{\boldsymbol{n}} = \{\, x \in \mathbb{N} \mid x < n \,\} \quad \text{and} \quad \mathrm{T}_{\boldsymbol{n}} = \{\, x \in \mathbb{N} \mid x \geq n \,\}$$

respectively, where we will define the inequalities in the condition for these sets, based on the axioms, presently.

We will find that $I_0 = \varnothing$ and $T_0 = \mathbb{N}$.

3 Natural Numbers Are Ordered

Already we can create an interesting fact about $\mathbb{N}$.

3.1 **Theorem**. **Every natural number may be obtained, just once, by applying S to 0, iterating this application of S to the output a finite number of times.**

Proof. We will let A be the set consisting of 0 and also any natural number that can be created by applying S to 0 and then S to $S(0)$, iterating the application of S a finite number of times.

0 is assumed to be in A, and if $n \in A$ so is $S(n)$. **Axiom Nine**, the Axiom of Induction, implies $\mathbb{N} \subset A$ and since $A \subset \mathbb{N}$ we have $A = \mathbb{N}$.

By **Axiom Seven** when a natural number appears by this procedure it can never appear again. □

Denote $S(0)$ by the symbol 1. We will see that it does behave as 1 *should.*

Generally if a natural number is built using iterates of S from natural number 0 in the same way the numeral k is built starting from numeral 0 we associate that natural number with the ‘‘ur-symbol’’ k. Every natural number may be given such a label, a numeral, corresponding to the instructions by which it was created from 0 by application of the function S.

$$7 \longleftrightarrow S^7(0) \equiv S(S(S(S(S(S(S(0))))))).$$

$S(S(S(S(S(S(S(0)))))))$ appears on the list of natural numbers at exactly the same place as 7 appears on the list of non-negative numerals.

We are using the knowledge we have of how to create numerals, the number symbols in base 10. The implied *definition* of $\boldsymbol{S^k}$ for any numeral k is taken from our ‘‘ur-knowledge,’’ but their use only requires knowledge about the algorithm used to create numerals. We know nothing yet about the properties of these labels and how they interact with addition, multiplication and order on the natural numbers, to be defined shortly.

3.2 **Proposition**. **Every natural number can be associated with a numeral**, the base 10 representation of the procedure by which a natural number is produced. **This numeral is unique** for each natural number. And any finite ordered list of the symbols

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

that does not begin with 0 **corresponds to one nonzero natural number.**

3.3 **Definition**. If, while iterating the application of S on the natural number 0, the natural number k appears before the natural number n we write $\boldsymbol{k < n}$ or, synonymously, $\boldsymbol{n > k}$. In words, we say that $\boldsymbol{k}$ **is less than** $\boldsymbol{n}$ or, synonymously, that $\boldsymbol{n}$ **is greater than** $\boldsymbol{k}$.

Thus $0 < k$ for every non-zero natural number k. Such a k is called **positive.**

3.4 **Corollary**. **Suppose $\boldsymbol{a < b}$. Mimicking the procedure by which $\boldsymbol{a}$ and $\boldsymbol{b}$ were produced from 0 we find that applying $\boldsymbol{S}$ to $\boldsymbol{a}$ and iterating a finite number of times will eventually yield $\boldsymbol{b}$. But $\boldsymbol{a}$ never appears when applying $\boldsymbol{S}$ to $\boldsymbol{b}$ a finite number of times.**

Proof. This is the definition of inequality and **Axiom Seven**. □

3.5 **Proposition**. **Suppose $\boldsymbol{a}$ and $\boldsymbol{b}$ are two distinct natural numbers. Then one and only one of $\boldsymbol{a < b}$ or $\boldsymbol{b < a}$ is true.**

Proof. The proof of this proposition amounts to rephrasing the definition of ‘‘less than’’ and observing the result in **Theorem 3.1**. In this case ‘‘trivial’’ does not equal ‘‘unimportant.’’ □

It is convenient to expand on this slightly. We declare that $\boldsymbol{k}$ **is less than or equal to** $\boldsymbol{n}$ or, synonymously, that $\boldsymbol{n}$ **is greater than or equal to** $\boldsymbol{k}$ if $k < n$ or, possibly, $k = n$. This situation is denoted $\boldsymbol{k \le n}$ or, equivalently, $\boldsymbol{n \ge k}$.

Thus we have three properties related to this order. For any k, m and n

- **reflexivity** $k \le k$.
- **antisymmetry** Either $k \le n$ or $n \le k$.
- **transitivity** If $k \le m$ and $m \le n$ then $k \le n$.

Given nonempty set of natural numbers X, any natural number n for which $n \le x$ for every $x \in X$ is called a **lower bound** for X. If X has a lower bound n and, whenever m is *also* a lower bound for X we have $n \ge m$, then n is called the **greatest lower bound** for X.

Similarly, given nonempty X any natural number n for which $n \ge x$ for every $x \in X$ is called an **upper bound** for X. If X has an upper bound n and, whenever m is *also* an upper bound for X we have $n \le m$, then n is called the **least upper bound** for X.

X is called **bounded** if it has both an upper bound and a lower bound.

***3.6* Theorem. Every nonempty set of natural numbers contains its greatest lower bound. Every nonempty set of natural numbers with an upper bound contains its least upper bound.**

Proof. If X is a nonempty subset of $\mathbb{N}$ then it has a member n. This element must appear on the finite list of iterates of S applied to 0. Using numerals to designate natural numbers we have

$$0,\ 1,\ 2,\ 3,\ \ldots,\ n$$

Examining the elements on this list one at a time starting from 0 we will eventually encounter a member of X, possibly n itself. This first encounter is the greatest lower bound of X.

The second part of this theorem is argued similarly. □

The least upper bound of a set X of natural numbers is often called the **greatest** or **largest** member of X.

The greatest lower bound of a set X of natural numbers is often called the **least** or **smallest** member of X.

4 Addition for Natural Numbers

***4.1* Definition.** If $n, k \in \mathbb{N}$ **define** $\boldsymbol{n + 0 = n}$ **and**

$$\boldsymbol{n + S(k) = S(n + k)}.$$

This is the *definition* of the **addition** symbol, **and is not to be construed (yet) as something having to do with manipulation of the digits in numerals**, the labels for n and k which may be used to specify these natural numbers.

The properties of addition are yet to be determined.

***4.2* Proposition. Addition is defined for every pair of natural numbers.**

Proof. For each natural number n let A_n be the set of those k for which $n + k$ is defined. $0 \in A_n$ and if $k \in A_n$ then $n+k$ is defined so $n+S(k) = S(n+k)$ so $S(k) \in A_n$. Thus $A_n = \mathbb{N}$ by **Axiom Nine.** □

***4.3* Proposition.** $\boldsymbol{a + (b + c) = (a + b) + c}$ for natural numbers a, b and c.

Proof. Let C be the set of those c for which $(a + b) + c = a + (b + c)$ for all a, b. So $0 \in C$. Suppose $c \in C$. Then

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

So $S(c) \in C$ and therefore $C = \mathbb{N}$ by **Axiom Nine**. $\square$

Thus, this **addition is associative.**

***4.4* Lemma**. $\boldsymbol{0 + b = b}$ for every $b \in \mathbb{N}$.

Proof. Let B be the set of those b for which $0 + b = b$. So $0 \in B$. If $k \in B$ then

$$0 + S(k) = S(0 + k) = S(k).$$

So $S(k) \in B$ and then $B = \mathbb{N}$ by **Axiom Nine**. $\square$

***4.5* Lemma**. $\boldsymbol{S(x) = x + 1}$ and $\boldsymbol{a + 1 = 1 + a}$ for all x and a.

Proof. First, $x + 1 = x + S(0) = S(x + 0) = S(x)$. Second, if $a = 0$ we already know $a + 1 = 1 + a$. Third, suppose $a > 0$. So $a = S(j)$ for some j. Suppose we know $j + 1 = 1 + j$. Then

$$1 + a = S(1 + j) = S(j + 1) = S(a) = a + 1.$$

Again we invoke **Axiom Nine** to conclude that $1 + a = a + 1$ for any a. $\square$

***4.6* Proposition**. $\boldsymbol{b + a = c + a \iff b = c}$.

Proof. The equation obviously holds when $a = 0$ so any counterexample must have $a = S(j) = j + 1$ for some j. Let a be the least possible natural number which has a counterexample, if any. But then there are unequal b and c for which $b + a = c + a$ and then

$$b + a = S(b + j) = c + a = S(c + j).$$

Since S is one-to-one by **Axiom Seven** we have $b + j = c + j$. This contradicts minimality of the choice of a, so no counterexamples exist and the desired conclusion follows. $\square$

So addition is **cancellative**, at least on the right. We will see next that **addition is commutative** so addition will be cancellative on the left as well.

***4.7* Proposition**. $\boldsymbol{a + b = b + a}$ for all a, b.

Proof. This is obviously true when $b = 0$ and any a. Suppose we know $x + j = j + x$ for some positive j and all x. Let $b = j + 1$. Then

$$\begin{aligned} a + b &= a + (j + 1) = a + (1 + j) = (a + 1) + j \\ &= j + (a + 1) = j + (1 + a) = (j + 1) + a = b + a. \end{aligned}$$

The result follows. $\square$

At this point we have invoked Axiom Nine several times and will, henceforth, use it without comment.

5 Multiplication for Natural Numbers

***5.1* Definition**. For any a we define $\boldsymbol{a \cdot 0} = 0$ and, for any j define

$$\boldsymbol{a \cdot S(j)} = a + a \cdot j$$

where, to reduce the number of parentheses required, we give precedence to multiplication over addition, as usual.

***5.2* Proposition**. **Multiplication is defined for every pair of natural numbers.**

Proof. This is proved by means identical to that in the proof of **Proposition 4.2**. □

***5.3* Definition**. If $m = a \cdot b$ for certain natural numbers a and b then a is called the **product** of a and b and a and b are called **factors** of m.

***5.4* Lemma**. $\boldsymbol{0 \cdot x = x \cdot 0 = 0}$ **and** $\boldsymbol{x \cdot 1 = 1 \cdot x}$ for all x.

Proof. $x \cdot 0 = 0$ by definition.

Now suppose $x = S(j)$ and $0 \cdot j = 0$. Then $0 \cdot x = 0 + 0 \cdot j = 0 + 0 = 0$.

$x \cdot 1 = x + x \cdot 0 = x$ and if $x = S(j) = 1 + j$ then $1 \cdot x = 1 + 1 \cdot j = 1 + j = x$. □

***5.5* Lemma**. $\boldsymbol{(a+b) \cdot x = a \cdot x + b \cdot x}$ for all a, b, x.

Proof. This is obviously true if $c = 0$ or 1. If $(a+b) \cdot j = a \cdot j + b \cdot j$ holds for j and all a, b then

$$\begin{aligned}(a+b) \cdot S(j) &= (a+b) + (a+b) \cdot j = (a+b) + (a \cdot j + b \cdot j) \\ &= (a + a \cdot j) + (b + b \cdot j) = a \cdot S(j) + b \cdot S(j).\end{aligned}$$

□

So multiplication is **right-distributive over addition.**

***5.6* Proposition**. $\boldsymbol{a \cdot b = b \cdot a}$ for all a, b.

Proof. We already have the result when either a or b are 0 or 1. Suppose $b = S(j)$ and $a \cdot j = j \cdot a$ for all a.

$$a \cdot S(j) = a + a \cdot j = a + j \cdot a = 1 \cdot a + j \cdot a = (1 + j) \cdot a = S(j) \cdot a.$$

The result follows. □

5.7 **Remark**. Since we now know that **multiplication is commutative** we have both **left and right distributive properties of multiplication over addition**.

$$\boldsymbol{(a+b)\cdot x = a\cdot x + b\cdot x} \quad \text{and} \quad \boldsymbol{x\cdot(a+b) = x\cdot a + b\cdot x} \quad \text{for all } \boldsymbol{a,b,x.}$$

We can now show that **multiplication is associative.**

5.8 **Proposition**. $\boldsymbol{(a\cdot b)\cdot c = a\cdot(b\cdot c)}$ for all a,b,c.

Proof. We already have the result when any of a,b or c are 0 or 1.

Suppose $c = S(j) = 1+j$ and $(a\cdot b)\cdot j = a\cdot(b\cdot j)$.

$$\begin{aligned}(a\cdot b)\cdot c &= (a\cdot b)\cdot(1+j) = (a\cdot b)+(a\cdot b)\cdot j = a\cdot b + a\cdot(b\cdot j)\\ &= a\cdot(b+b\cdot j) = a\cdot(b\cdot(1+j)) = a\cdot(b\cdot c).\end{aligned}$$

The result follows. □

5.9 **Lemma**. $\boldsymbol{a\cdot b = 0}$ **and** $\boldsymbol{a \neq 0 \implies b = 0}$.

Proof. Let b be the least counterexample to this lemma, if any. Then $b = S(j)$ for some $j > 0$. But then $a\cdot b = a\cdot S(j) = a + a\cdot j$. We cannot have $a\cdot j = 0$ because $j < b$ so $a\cdot j = S(k)$ for some k. But then $a + a\cdot j = S(a+k) \neq 0$ by **Axiom Eight**.

So no counterexample exists: that is, the lemma holds. □

5.10 **Lemma**. $\boldsymbol{a\cdot b = a}$ **and** $\boldsymbol{a \neq 0 \implies b = 1}$.

Proof. As in the last lemma, let b be the least counterexample, if any. Then $b = S(j)$ for some $j > 0$. But then

$$a\cdot b = a\cdot S(j) = a + a\cdot j = a = a + 0$$

so $a\cdot j = 0$ by **Proposition 4.6**. This implies $j = 0$ by **Lemma 5.9**, contrary to choice of b.

So no counterexample exists and the lemma holds. □

5.11 **Proposition**. $\boldsymbol{(a\cdot b = a\cdot c}$ **and** $\boldsymbol{a\neq 0) \iff (b = c}$ **and** $\boldsymbol{a \neq 0).}$

Proof. By the previous lemmas we know there can be no counterexample if b or c are 0 or 1. Let b be the least natural number involved in any counterexample. We have then $a\cdot b = a\cdot c$ and $1 < b < c$. So $b = S(j)$ and $c = S(k)$ for some least j where $0 < j < k$.

But then $a\cdot b = a + a\cdot j = a\cdot c = a + a\cdot k$ which implies $a\cdot j = a\cdot k$, providing a counterexample smaller than that given by b and c, assumed to be the least such.

No counterexample exists and the Proposition holds. □

So multiplication is **cancellative for nonzero products.**

6 Order and the Arithmetic of Natural Numbers

***6.1* Lemma**. $\boldsymbol{b > 0 \quad \Longleftrightarrow \quad a < a + b.}$

Proof. Let X be the set of those j for which $a < a + S(j)$. Since $S(a) = a + 1$ we know $0 \in X$. Now suppose $j \in X$.

$$a < a + S(j) < S(a + S(j)) = a + S(S(j)).$$

So $S(j) \in X$ and therefore $X = \mathbb{N}$. □

***6.2* Proposition**. **Suppose $\boldsymbol{0 < k \leq n}$. There is a unique $\boldsymbol{s \in \mathbb{N}}$ for which $\boldsymbol{k + s = n}$.**

Proof. Let $A_n = \{x \in \mathbb{N} \mid k + x \geq n\}$. Since $n \in A_n$ we know A_n is nonempty. So it has a least member s.

If $s = 0$ then $k \geq n$. But also $k \leq n$ by assumption so $k = n$ and 0 is the unique natural number for which $n + s = n$.

Dealing with the other possibility, suppose $s = S(j) > 0$. If $k + s > n$ then

$$k + s = k + S(j) = S(k + j) > n.$$

But then $k + j \geq n$ and $j < s$ and $j \in A_n$, contrary to choice of s as the least member of A_n. So $k + s = n$.

And if $k + s = k + t$ we have $s = t$ by **Proposition 4.6**, so s is unique. □

***6.3* Definition**. We now define **subtraction** for certain pairs of natural numbers.

If $n \geq k$ we define $\boldsymbol{n - k}$ to be the unique s for which $k + s = n$.

***6.4* Exercise**. (i) If $n > k > s \iff n - k < n - s$.

(ii) If $n \geq k + s$ then $n - (k + s) = (n - k) - s = (n - s) - k$.

(iii) Suppose $n + s \geq k$. Then $n - (k - s) = (n + s) - k$.

***6.5* Lemma**. $(\boldsymbol{a > 0}$ **and** $\boldsymbol{b > 1}) \quad \Longleftrightarrow \quad \boldsymbol{a < a \cdot b}$.

Proof. If $b > 1$ then $b = S(j)$ for some $j > 0$ and so $a \cdot j > 0$ by **Lemma 5.9**. The reverse implication is even easier.

Using **Lemma 6.1**, $a \cdot b = a + a \cdot j > a$. □

***6.6* Proposition**. $\boldsymbol{c + a < c + b \iff a < b}$.

Proof. Suppose $a < b$. If $a = 0$ then $c + a = c + 0 < c + b$ by **Lemma 6.1**. So suppose $0 < a < b$. If, for some c we have $c + a \geq c + b$ there would be an inequality of this type for a least nonzero a. So $a = S(j)$ and $b = S(k)$ and $j < k$. But then

$$S(c + j) = c + S(j) \geq c + S(k) = S(c + k)$$

which implies $c + j \geq c + k$. Such a j cannot be 0, and this contradicts the minimality of a among such counterexamples. Therefore no such counterexample can exist.

We will now suppose $c + a < c + b$ and show $a < b$.

Let A be the set $\{ j \in \mathbb{N} \mid j + a < j + b \implies a < b \}$. Obviously $0 \in A$. Note that for any j we have $j + a < j + b$ if and only if $S(j + a) < S(j + b)$. But then if $j \in A$

$$a + S(j) = S(a + j) < S(b + j) = b + S(j).$$

So $S(j) \in A$ and therefore $A = \mathbb{N}$. □

***6.7* Proposition**. $\boldsymbol{c \cdot a < c \cdot b \iff (a < b \text{ and } c \neq 0)}$.

Proof. Suppose $c \cdot a < c \cdot b$. Then neither b nor c can be 0. If $a = 0$ we have, then, that $a < b$. So we consider the case of $a \neq 0$.

If there is any a, b with $c \cdot a < c \cdot b$ but $a \geq b$ there would have to be a least a providing such a counterexample. But $a = j + 1$ and $b = k + 1$ for certain j, k with $j > k$. So

$$c \cdot a = c \cdot j + c < c \cdot b = c \cdot k + c$$

and by **Proposition 6.6** we have $c \cdot j < c \cdot k$ and $j < a$, contrary to choice of a. So no counterexample can exist.

We now consider the reverse implication. Suppose $a < b$, so b must be nonzero, and suppose c is also nonzero. If $a = 0$ the inequality $c \cdot a < c \cdot b$ clearly holds. But what if $a = S(x)$ and $b = S(y)$. Note $x < y$.

If there is any counterexample for some c we would have a least a providing that counterexample. Specifically we would have a smallest nonzero a and nonzero b and c with $a < b$ but $c \cdot a \geq c \cdot b$. But the calculation above gives us

$$c \cdot x + c \geq c \cdot y + c \quad \text{so} \quad c \cdot x \geq c \cdot y,$$

again by by **Proposition 6.6**. Since a is defined as part of the smallest counterexample for a given c, and $x < a$, we have a contradiction. No such counterexample can exist. □

***6.8* Proposition**. **If $\boldsymbol{c = a \cdot b \neq 0}$ then both $\boldsymbol{a \leq c}$ and $\boldsymbol{b \leq c}$.**

Proof. If a or b is 1 the result is trivial so eliminate these cases from consideration.

Suppose, for some other a, b pair we have $c = a \cdot b$ but $a > c$. So $b = S(k)$. So

$$c = a \cdot b = a \cdot S(k) = a + a \cdot k \geq a > c.$$

This is impossible, so $a \leq c$. Commutativity of multiplication implies the same result for b. □

6.9 **Proposition**. **If $c = a \cdot b \neq 0$ and $a > 1$ then $0 < b < c$.**

Proof. Suppose there is an a, b pair with $c = a \cdot b$ and $a = S(j)$ for some $j > 0$ and $b \geq c$. Then

$$c = a \cdot b = b \cdot a = b \cdot S(j) = b + b \cdot j \geq c + b \cdot j > c.$$

This is impossible, so $b < c$. □

6.10 **Theorem**. **Archimedean Order Property**:

For each pair a, b in $\mathbb{N}$ with $a > 0$ there is a least n such that $a \cdot n > b$.

Proof. If $b = 0$ choose $n = 1$. If $b > 0$ and $a = 1$ choose $n = S(b)$.

If $a > 1$ and $b > 0$ then $a = S(j)$ for some $j > 0$. So if $n \neq 0$ we have

$$a \cdot n = n \cdot a = n + j \cdot n > n.$$

Let A be the set of those n for which $n \cdot a > b$. We know A is nonempty since $b \in A$. So A has a least member x. Thus $a \cdot x > b$ but if $y < x$ then y cannot be in A so $a \cdot y \leq b$. Thus x is the least natural number for which $a \cdot x > b$. □

6.11 **Theorem**. **The Division Algorithm**:

For each pair a, b of nonzero natural numbers there is a unique pair of natural numbers q and r for which

$$a = b \cdot q + r \quad \text{and} \quad 0 \leq r < b.$$

Proof. If $b > a$ choose $q = 0$ and $r = a$. If $q > 0$ then $b \cdot q + r \geq b > a$ for any r, so $q = 0$ is the only choice here. Similarly, if $a = b \cdot m$ for $m \geq 1$ then $q = m$ and $r = 0$ satisfies the condition of the theorem.

Adapting the proof of **Theorem 6.10** there is a unique natural number q for which $b \cdot q \leq a$ and $b \cdot S(q) = b \cdot (q + 1) = b \cdot q + b > a$.

By **Proposition 6.2** there is a unique r for which $b \cdot q + r = a$. Combining these facts we have

$$b \cdot q \leq b \cdot q + r = a < b \cdot q + b.$$

If $r \geq b$ there would be unique $t \geq 0$ with $r = b + t$. But then

$$b \cdot q + r = b \cdot q + b + t > a,$$

which is impossible. So $0 \leq r < b$ and $a = b \cdot q + r$ is a decomposition of a of the type we are looking for, and r is unique for this q.

It remains to consider the possibility of $a = b \cdot p + w$ for $p \neq q$.

Suppose first that $p < q$. So $p + j = q$ for some $j > 0$. But then

$$a = b \cdot q + r = b \cdot p + b \cdot j + r \text{ so } w = b \cdot j + r \geq b.$$

And if $p > q$ then for some $j > 0$ we have $p = q + j$.

$$a = b \cdot p + w = b \cdot q + b \cdot j + w$$

This would imply, by uniqueness of r, that $r = b \cdot j + w \geq b$. This too is impossible. So the conditions on r imply that q is unique as well. □

The word ''algorithm'' in the name of the last theorem implies a procedure by which q and r may be found.

Euclid had a method involving repeated subtraction of b, as can be found in Book VII Proposition 1 of *Euclid's Elements* [5]. This used the Greek geometrical method of arithmetic and was inefficient but effective. Ordinary long division will accomplish this using numerals, and the number of operations required to carry that out (worst case) is a (fixed) multiple of the number of digits required to represent a, proportionate to the logarithm of the numeral for a.

''Algorithm D,'' created by Donald Knuth, may be found in his *The Art of Computer Programming Volume 2 Seminumerical Algorithms* [9] and is considerably better. Many others have been created since.

7 Numerals and the Arithmetic of Natural Numbers

We learned, as children, a procedure to calculate sums and products of numerals. These procedures can be converted to highly organized deeply nested applications of the distributive property, the associative property and repeated addition of the numeral 1. Doing the same calculations in a different order has always produced the same answer, in my experience.[5]

We have now defined addition and multiplication on natural numbers. Presumably these operations are related to the similarly named operations on numerals.

---

[5] According to Gödel's Theorem there can be no proof that this will always be the case.

So as not to beg the question, we will use $\odot$ and $\oplus$ to denote the ordinary operations on numerals and use $S(0)$ to denote the natural number which we have previously designated as 1, retaining the use of 1 for numerals.

7.1 **Lemma**. **Suppose natural number m is associated with the numeral j as discussed previously. Then $m+S(0)=S(m)$ is associated with the numeral $j\oplus 1$.**

Proof. Let A be the set of integers for which this is true. Obviously $0\in A$. If $m\in A$ is associated with numeral j then $m+S(0)=S(m)$ and is formed using one more iteration of S from 0 than used to form m itself. The next numeral after j is $j\oplus 1$, which is therefore the numeral associated with $m+S(0)$. So $S(m)\in A$ and then $A=\mathbb{N}$. □

7.2 **Proposition**. **If, for numerals j and k, we always have**

$$(j\oplus k)\oplus 1 = j\oplus(k\oplus 1)$$

then numerals can be used to calculate sums of natural numbers. Specifically, suppose j and k are numerals associated with natural numbers m and n. Then

$$j\oplus k \quad \text{is the numeral associated with natural number} \quad m+n.$$

Proof. Fix j and associated natural number m. Let A be the set of those natural numbers n, with associated numeral k, for which $j\oplus k$ is the numeral associated with $m+n$. 0 is obviously in A. And if $n\in A$ then

$$m+S(n)=S(m+n) \text{ which is associated with } (j\oplus k)\oplus 1 = j\oplus(k\oplus 1).$$

So $S(n)\in A$ and we conclude that $A=\mathbb{N}$. □

7.3 **Proposition**. **If, for numerals j and k, we always have**

$$j\otimes(k\oplus 1) = (j\otimes k)\oplus j$$

then numerals can be used to calculate products of natural numbers. Specifically, suppose j and k are numerals associated with natural numbers m and n. Then

$$j\otimes k \quad \text{is the numeral associated with natural number} \quad m\cdot n.$$

Proof. Fix j and associated natural number m. Let A be the set of those natural numbers n, with associated numeral k, for which $j\otimes k$ is the numeral associated with $m\cdot n$. 0 is obviously in A. And if $n\in A$ then

$$m\cdot S(n) = m\cdot(n+S(0)) = m\cdot n+m.$$

$m\cdot n$ is associated with $j\odot k$ and m is associated with j so by **Proposition 7.2**

$$m \cdot S(n) \text{ is associated with } (j \odot k) \oplus j = j \otimes (k \oplus 1).$$

Since $k \oplus 1$ is associated with $S(n)$ we have $S(n) \in A$ and we conclude that $A = \mathbb{N}$. $\square$

We will now drop the annoying distinction between operations on numerals and operations on natural numbers.

***7.4* Remark**. With **Propositions 7.2** and **7.3** we have shown that if you can prove, or believe, that for *numerals* we have

$$(j + k) + 1 = j + (k + 1) \text{ and } j \cdot (k + 1) = (j \cdot k) + j$$

then arithmetic among natural numbers can be performed by doing the corresponding arithmetic on their representative numerals.

With that conclusion in hand, we can then go on to deduce that PA_2 is **categorical.** That is a term used by philosophers to indicate that there is, essentially, only one structure defined by a logic and a collection of axioms.

More explicitly, suppose two instantiations of the natural numbers are formed using the Peano Axioms but with different background sets $\mathbb{N}_1$ and $\mathbb{N}_2$ and different successor functions S and T. Operations of addition and multiplication are defined in each ''universe.''

The function $\Psi\colon \mathbb{N}_1 \to \mathbb{N}_2$ given by $\Psi(0_1) = 0_2$ and $\Psi(S(k)) = T(\Psi(k))$ for $k \in \mathbb{N}_1$ is defined on all of $\mathbb{N}_1$, one-to-one and onto $\mathbb{N}_2$. And

$$\Psi(k \cdot s + t) = \Psi(k) \cdot \Psi(s) + \Psi(t) \quad \text{for all } k, s, t \in \mathbb{N}_1.$$

***7.5* Exercise**. At which point, exactly, in this chapter could **Propositions 7.2** and **7.3** and the statements in **Remark 7.4** be proved?

As a final point, we have not proved that the arithmetic of numerals or natural numbers are consistent. According to Gödel's Theorem we can never prove this. What we *have* claimed is that the two structures are **equiconsistent.** They are both consistent or both inconsistent.

And the Peano Axioms, devoid of geometrical reference, can have no inconsistency from that source.