

Proving Bertrand's Postulate

by Andrew Boucher

created: 31 December 2007

First Draft

Bertrand's Postulate asserts that for every even natural number $n \geq 4$, there exists a prime number p such that $\frac{n}{2} < p < n$. It was originally proved by Chebyshev, working in what may be taken to be some version of Peano Arithmetic. Now Peano Arithmetic, in its second-order version, which will be our concern here, assumes induction and makes various suppositions about the successor relationship: that it is a function, that it is one-to-one, that it has 0 in its domain but not in its image, and that it is total, i.e. that every number has a successor. This last axiom, called naturally enough the *Successor Axiom*, is what endows the natural numbers with their infinitary character; it is an assumption with a different character from the rest and, in the author's eyes anyway, should not be made. The sub-theory of Peano Arithmetic which excludes it, has as models the standard one (if it exists), as well as all the finite segments. It has the property that, once a natural number n can be shown to exist or is assumed, every number less than n exists; but it is unable to deduce the existence of any number greater than n . Now the content of Bertrand's Postulate would seem not to require the existence of numbers greater than n , even though its proof always uses numbers larger, indeed much larger, than n , such as $n!$. It will be shown here that indeed the appeal to the Successor Axiom is superfluous and can be avoided. Much of the work will be to show how much larger numbers can be considered to be imaginary and representable using numbers no larger than n , thus presenting a general method of avoiding the Successor Axiom.

0. Abbreviations

$x \in P$ for Px

$Dom(R)$ for $\{x : \exists y Rx,y\}$

$Im(R)$ for $\{y : \exists x Rx,y\}$

$IsFunction(R)$ for $\forall x \forall y \forall z (Rx,y \ \& \ Rx,z \Rightarrow y = z)$

$Is1-1(R)$ for $\forall x \forall y \forall z (Rx,y \ \& \ Rz,y \Rightarrow x = z)$

$P \equiv Q$ for $\forall x (Px \Leftrightarrow Qx)$

$P \subseteq Q$ for $\forall x (Px \Rightarrow Qx)$ or $\forall x \forall y (Px,y \Rightarrow Qx,y)$

$P \cup Q$ for $\{z : Pz \vee Qz\}$ or $\{y,z : Py,z \vee Qy,z\}$ or $\{x,y,z : Px,y,z \vee Qx,y,z\}$

$P \setminus Q$ for $\{z : Pz \ \& \ \neg Qz\}$

$\{a\}$ for $\{z : z = a\}$

$\{(a,b)\}$ for $\{y,z : y = a \ \& \ z = b\}$

ϕ for $\{z : \neg z = z\}$

1. Introduction

We will be working in predicative second-order logic. That is, comprehension is restricted to predicative (arithmetic) predicates. The language will be augmented by a first-order constant 0, a second-order one-place predicate N (representing the natural numbers), and a second-order two-place predicate σ (representing succession).

The theory of Peano Arithmetic **PA** contains these axioms:

- (PA1) $\text{N}0$
 (PA2) $\forall n (\text{N}n \Rightarrow \exists m (\text{N}m \ \& \ \sigma_{n,m}))$
 (PA3) $\forall n \forall m \forall m' (\text{N}n \ \& \ \text{N}m \ \& \ \text{N}m' \ \& \ \sigma_{n,m} \ \& \ \sigma_{n,m'} \Rightarrow m = m')$
 (PA4) $\forall n \forall m \forall n' (\text{N}n \ \& \ \text{N}m \ \& \ \text{N}n' \ \& \ \sigma_{n,m} \ \& \ \sigma_{n',m} \Rightarrow n = n')$
 (PA5) $\forall n (\text{N}n \Rightarrow \neg \sigma_{n,0})$
 (PA6) Induction schema. Let ϕ be a well-formed formula. Use $\phi [x\lambda y]$ to mean x replaces all (free) instances of y . Suppose $\phi [0\lambda n]$ and $\forall n \forall m (\text{N}n \ \& \ \sigma_{n,m} \ \& \ \phi \Rightarrow \phi [m\lambda n])$. Then $\forall n (\text{N}n \Rightarrow \phi)$.

FPA is the sub-theory without axiom (PA2) - called the Successor Axiom - and (PA1), which is a trivial assumption only needed to assert that the natural numbers are not vacuous. In *Arithmetic without the Successor Axiom*, **FPA** can be seen to develop much of arithmetic. For instance, **FPA** proves Quadratic Reciprocity. The normal proof of this fact uses the Successor Axiom, because given numbers p and q , it supposes the existence of the larger p^*q [e.g. see *Hardy and Wright*]. The proof in *Proving Quadratic Reciprocity and Arithmetic* avoids the use of this larger number and shows that the underlying argument actually relies on a congruence. So to speak, the proof has the advantage of providing insight into what makes the reasoning work, but the disadvantage of not providing a general technique of how effectively to manage products without assuming their existence.

The proof of Bertrand's Postulate provided here relies instead on such a general technique, where larger numbers (up to a certain point) are represented using a second-order object. That is, given the existence of a number n , one can assert using *Comprehension* the existence of a function from $\{0,1,\dots,n\}$ to $\{0,1,\dots,n\}$, which is essentially a number of base $(n+1)$ and length $(n+1)$ or less. Once it is shown how to define addition, multiplication, and other operations and relationships on these second-order numbers, this effectively gives access to reasoning up to the number $(n+1)^{(n+1)} - 1$.

2. Defining Second-Order Numbers and Their Ordering

As remarked much of elementary arithmetic has been developed in *Arithmetic* and everything there will be assumed here, in particular addition, multiplication, exponentiation, and the normal ordering on first-order numbers.

Also, the machinery of sequences is developed in *Arithmetic* and will be assumed here. Sequences are functions R which have the numbers up to some natural number n as a domain and will be written $\text{Seq}(R,n)$ or just $\text{Seq}(R)$. When $\text{Seq}(R,n)$ and Rx,y , then $R(x)$ or R_n will be used to denote y . Sometimes smaller-case letters will be used to represent sequences.

Def 2.1. Let $\text{N}n$ and $\text{Seq}(R,n)$. R is an n -type second-order number or n -SON or simply SON (if n is unimportant or can be assumed) if and only if, $\forall x \leq n (R(x) \leq n)$. We may write either n -SON(R) or just SON(R) in this case.

If R is an n -SON, then we may write R as $R(n)R(n-1)R(n-1)\dots R(0)$. Leading 0s may be suppressed. If $R(i) = 0 \ \forall i (0 < i \leq n)$, then we may write R as $\langle R(0) \rangle$.

If R is an n -SON and $R \equiv \langle 0 \rangle$, then we will write R as 0_n or just 0 (if n is unimportant or can be assumed).

If R is an n -SON and $R \equiv \langle 1 \rangle$, then we will write R as I_n or just I (if n is unimportant or can be assumed).

If R is an n -SON and $\forall x (m < x \leq n \Rightarrow R(x) = 0) \ \& \ \neg R(m) = 0$, then we say that R is of length m and write $len(R) = m$. We stipulate that 0 has length 0 . \square

Remark that when R and S are n -SONs such that $\forall x \leq n (R(x) = S(x))$, then R and S are equivalent, and following our standard notation, we write $R \equiv S$.

Equivalence respects length; that is, if $R \equiv S$, then $len(R) = len(S)$.

Def 2.2. If R is an n -SON of length m and $\sum_{i=0}^m R_i (n+1)^i$ exists and equals y , then we write $R = y$. \square

Obviously, R can equal at most one y , and it may not equal any, should the sum not be defined. We stipulate that $0 = 0$. Evidently, $I_n = 1$, whenever $n \geq 1$.

Example 2.3. Suppose $N \equiv \{0,1,2,3,4,5,6,7,8\}$. Then the 4-SON R defined by

$$\begin{aligned} R(0) &= 2 \\ R(1) &= 1 \\ R(2) &= 0 \\ R(3) &= 0 \\ R(4) &= 0 \end{aligned}$$

has length 1. We may write it as 00012 or simply 12. Also, $2 * 5^0 + 1 * 5^1$ exists and equals 7, so $R = 7$.

On the other hand consider the 4-SON S defined by

$$\begin{aligned} S(0) &= 0 \\ S(1) &= 0 \\ S(2) &= 1 \\ S(3) &= 0 \\ S(4) &= 0. \end{aligned}$$

Then S has length 2 and may be written 00100 or just 100. $\sum_{i=0}^2 S_i 5^i$ does not exist, since it is too big.

The 4-SON 00003 may be written 3, but $\langle 3 \rangle$ will be preferred, to avoid confusion. \square

n -SONs are essentially strings representing numbers of base $n + 1$ with length (beginning the count with 1, rather than 0 as is done in the definition above) $\leq n + 1$. For instance, the 2-SONs are 0, 1, 2, 10, 11, 12, 20, 21, 22, 100, 101, 102, ..., 222. So n -SONs give

us effective access to $(n + 1)^{n+1}$ numbers, evidently much greater than n , and thus allow us to replicate and produce arithmetic arguments which require larger numbers, including that of the proof of Bertrand's Postulate. It will, of course, be necessary to show how to define and work with addition, multiplication, inequality, and other arithmetical concepts, which will take up much of this paper. Finally, remark it is not, in general, possible to speak in **FPA** of $n + 1$ knowing only that n exists, hence our manner of exposition, which mentions only n and avoids talking about base $n + 1$.

Prop 2.4. Suppose $len(R) = n > 0$. Then $R \setminus \{(x,y) : x = n\} \cup \{(n,0)\}$ has length $< n$. □

SONs can be ordered in the usual way:

Def 2.5. Let R, S be n -SONs. Write $R < S$ if and only if $\exists k \leq n$ such that both:

- a. $\forall x (k < x \leq n \Rightarrow R(x) = S(x))$ and
- b. $R(k) < S(k)$.

And we write $R \leq S$ when $R < S \vee R \equiv S$. □

Obviously, $<$ respects equivalence. That is suppose $R < S$. Then if $R \equiv T$, then $T < S$.
And if $S \equiv T$, then $R < T$.

It is easy to check:

Prop 2.6.

- a. *Transitivity.* $\forall R \forall S \forall T (R < S \ \& \ S < T \Rightarrow R < T)$
- b. *Dichotomy.* $\forall R \forall S (SON(R) \ \& \ SON(S) \Rightarrow R \leq S \vee S < R)$.

Remark: Obviously in *b.* it is meant that R and S are n -SON for the same n .

- c. *Anti-Symmetry.* $\forall R \forall S (R \leq S \ \& \ S \leq R \Rightarrow R \equiv S)$
- d. *Zero Minimal.* $\forall R (SON(R) \Rightarrow 0 \leq R)$.
- e. $\forall R (SON(R) \ \& \ \neg R \equiv 0 \Rightarrow 1 \leq R)$.
- f. $R \leq S \Rightarrow len(R) \leq len(S)$.
- g. $len(R) < len(S) \Rightarrow R < S$. □

Also:

Prop 2.7. Let R, S be n -SON.

- a. Suppose for some k , $\forall i \leq k (R(i) = 0) \& \forall i (k < i \leq n \Rightarrow R(i) \leq S(i))$. Then $R \leq S$.
- b. Suppose for some k , $\forall i \leq k (S(i) = n) \& \forall i (k < i \leq n \Rightarrow R(i) \leq S(i))$. Then $R \leq S$.
- c. Suppose $\forall i \leq n (S(i) = n)$. Then $R \leq S$.
- d. Suppose for some k , $R(k) = 1 \& \forall i (i \leq n \& \neg i = k \Rightarrow R(i) = 0)$. If $len(S) \geq k$, and if either $k > 0$ or $\neg S \equiv 0$, then $R \leq S$. □

The following is a useful meta-theorem.

Prop 2.8. (Well-Ordering) Let Nz . And let $\varphi(R)$ be a formula with the free-variable R .

- a. Suppose $\varphi(R)$ for some z -SON R . Then there is a least z -SON M such that $\varphi [MR]$.
- b. Suppose $\varphi(R)$ for some z -SON $R \leq S$. Then there is a greatest z -SON M such that $M \leq S \& \varphi [MR]$.
- c. Suppose $\varphi(R)$ for some z -SON R . Then there is a greatest z -SON M such that $\varphi [MR]$.

Pf:

- b. Proceed by induction, with ϕ as

$$n \leq z \Rightarrow \exists M \exists R (\varphi(R) \& \forall x < z - n (M(x) = z) \\ \& \forall x (z - n \leq x \leq z \Rightarrow R(x) = M(x)) \\ \& \forall T (\varphi [TR] \& T \leq S \Rightarrow T \leq M))$$

For $n = 0$, set M to $\{(x, y) : (x < z \& y = z) \vee (x = z \& y = c)\}$, where c is the greatest number such that there exists R with $\varphi(R) \& R \leq S \& R(z) = c$.

Now let $Nn \& \sigma n, m \& \phi$. If $m > z$, the result follows trivially, so assume $m \leq z$. By the Induction Hypothesis,

$$\varphi [UR] \& \forall x < z - n (N(x) = z) \& \forall x (z - n \leq x \leq z \Rightarrow U(x) = N(x)) \\ \& \forall T (\varphi [TR] \& T \leq S \Rightarrow T \leq U)$$

for some U, N . Let c be the greatest number such that there exists R with $\varphi(R) \& R \leq S \& R(z - m) = c \& \forall x (z - n < x \leq z \Rightarrow R(x) = N(x))$. Define M to be $N \setminus \{(x, y) : x = m\} \cup \{(m, c)\}$. Then $\phi [m \setminus n]$ holds.

- c. Use part (b) and *Prop 2.7(c)*. □

3. Defining Addition.

It is not possible to define addition on second-order numbers using the standard method

of recursion, since recursion would require the existence of sequences sufficiently long to go from 0 up to any particular second-order number. But second-order numbers may be much bigger than any first-order number, and sequences are, roughly speaking, limited in length to first-order numbers (since sequences are second-order entities which must take first-order entities as arguments).

So another approach must be taken. The following definition of addition mirrors the traditional adding algorithm, which uses what is essentially an intermediary sequence consisting of all carries. Its complexity results from the need to avoid the use of numbers greater than n , since only n is being assumed.

Def 3.1. Let R, S, T be n -SON. Then $+(n, R, S, T)$ if and only if there exists n -SON C such that $\forall x \leq n (C(x) \leq 1) \ \& \ C(0) = 0$ and $\forall x \leq n$

$$\begin{aligned} &R(x) + S(x) + C(x) = T(x) \ \& \ \neg C(x+1) = 1 \ \text{or} \\ &\exists y (R(x) + y = n \ \& \ C(x+1) = 1 \ \& \\ &\quad (C(x) = 0 \Rightarrow S(x) - (y + 1) = T(x)) \ \& \ (C(x) = 1 \Rightarrow S(x) - y = T(x))). \end{aligned}$$

When the first argument is unimportant or can be assumed, we will write $+(R, S, T)$. □

The use of “ $\neg C(x+1) = 1$ ” is meant to represent two eventualities: either (1) $C(x+1) = 0$; or (2) $C(x+1)$ does not exist, which is the case when $x = n$ since C is an n -SON. Also, “ $C(x) \leq 1$ ” is shorthand for saying, $C(x) = 0$ or $C(x)$ is the successor of 0. So technically there is no assumption in the definition that 1 exists, and the definition applies even in the case when $N \equiv \{0\}$, so that $+(0, 0_0, 0_0, 0_0)$.

Example 3.2. Consider the 4-SONs R , S , and T defined by:

$R(0) = 2$	$S(0) = 3$	$T(0) = 0$
$R(1) = 3$	$S(1) = 1$	$T(1) = 0$
$R(2) = 3$	$S(2) = 0$	$T(2) = 4$
$R(3) = 2$	$S(3) = 1$	$T(3) = 3$
$R(4) = 1$	$S(4) = 3$	$T(4) = 4$

That is, R is 12332, S is 31013, and T is 43400.

Then there exists 4-SON C defined by

$$\begin{aligned} C(0) &= 0 \\ C(1) &= 1 \\ C(2) &= 1 \\ C(3) &= 0 \\ C(4) &= 0 \end{aligned}$$

such that:

$$\begin{aligned} &R(0) + 2 = 4 \ \& \ C(0) = 0 \ \& \ S(0) - (2 + 1) = T(0) \ \& \ C(1) = 1 \ \text{and} \\ &R(1) + 1 = 4 \ \& \ C(1) = 1 \ \& \ S(1) - 1 = T(1) \ \& \ C(2) = 1 \ \text{and} \\ &R(2) + S(2) + C(2) = T(2) \ \& \ \neg C(3) = 1 \ \text{and} \\ &R(3) + S(3) + C(3) = T(3) \ \& \ \neg C(4) = 1 \ \text{and} \\ &R(4) + S(4) + C(4) = T(4) \ \& \ \neg C(5) = 1. \end{aligned}$$

Remark that $\neg C(3) = 1$ since $C(3) = 0$. And $\neg C(5) = 1$ since $C(5)$ does not exist.

Of course, this mirrors the normal method of adding 23321 and 31013 in base 5:

$$\begin{array}{r}
 C \quad \quad \quad 00110 \\
 R \quad \quad \quad 12332 \\
 S \quad + \quad \quad 31013 \\
 \hline
 \quad \quad \quad 43400
 \end{array}$$

So $+(4,R,S,T)$. □

It is straightforward to check that, for any n -SON R , S , and T such that $+(R,S,T)$, then T is unique up to equivalence, i.e. if also $+(R,S,U)$, then $T \equiv U$. We are therefore justified writing $R + S \equiv T$ and using $R + S$ to refer to T . It is easily seen that if $R + S \equiv T$ & $R \equiv R'$ & $S \equiv S'$, then $R' + S' \equiv T$. So it is possible to construct terms with multiple additions in an unambiguous manner, e.g. $(R + S) + T \equiv U$ is meant to represent that there exists V such that $R + S \equiv V$ & $V + T \equiv U$.

Notice that $+$ is not necessarily total, i.e. there may exist R and S such that $(R + S)$ does not exist. For instance, if $N \equiv \{x : x \leq n\}$ for some $n > 0$, then R and S with $R(n) = S(n) = n$ are such that $(R + S)$ does not exist because it is too big.

Prop 3.3.

- a. $\forall R \forall S \forall T (R + S \equiv T \Rightarrow \max(\text{len}(S), \text{len}(R)) \leq \text{len}(T))$.
- b. $\forall R \forall S \forall T (R + S \equiv T \ \& \ \max(\text{len}(S), \text{len}(R)) + 1 \text{ exists} \Rightarrow \text{len}(T) \leq \max(\text{len}(S), \text{len}(R)) + 1)$.
- c. $\forall n \forall R \forall S (n\text{-SON}(R) \ \& \ n\text{-SON}(S) \ \& \ \text{len}(R), \text{len}(S) < n \Rightarrow \exists T R + S \equiv T)$.
- d. $\forall n \forall R (n\text{-SON}(R) \ \& \ \exists x R(x) < n \Rightarrow \exists S (R + I) \equiv S)$.
- e. $\forall n \forall R (n\text{-SON}(R) \ \& \ n > 0 \ \& \ R(1) = 1 \ \& \ \forall i (i \leq n \ \& \ \neg i = 1 \Rightarrow R(i) = 0) \Rightarrow \langle n \rangle + I \equiv R)$ □

SON addition behaves like normal addition (except of course for the property of totality).

Prop 3.4 (Commutativity of SON Addition). $\forall R \forall S \forall T (R + S \equiv T \Rightarrow S + R \equiv T)$.

Pf:

Let $R + S \equiv T$. By *Def 3.1* there exists C such that $\forall x \leq n (C(x) \leq 1) \ \& \ C(0) = 0$ and $\forall x \leq n$

$$\begin{aligned}
 & R(x) + S(x) + C(x) = T(x) \ \& \ \neg C(x+1) = 1 \ \text{or} \\
 & \exists y (R(x) + y = n \ \& \ C(x+1) = 1 \ \& \\
 & \quad (C(x) = 0 \Rightarrow S(x) - (y + 1) = T(x)) \ \& \ (C(x) = 1 \Rightarrow S(x) - y = T(x))).
 \end{aligned}$$

Let $x \leq n$.

If the first case, then obviously $S(x) + R(x) + C(x) = T(x) \ \& \ \neg C(x+1) = 1$.

Otherwise, assume the second case, i.e. for some y ,

$$R(x) + y = n \ \& \ C(x+1) = 1 \ \& \\ (C(x) = 0 \Rightarrow S(x) - (y + 1) = T(x)) \ \& \ (C(x) = 1 \Rightarrow S(x) - y = T(x)).$$

Suppose $C(x) = 0$. Then $S(x) - (y + 1) = T(x)$. S is an n -SON, so $S(x) \leq n$; thus set $y' = n - S(x)$. So $S(x) + y' = n$ and

$$T(x) = S(x) - (y + 1) \\ = (n - y') - (n - R(x)) - 1 \\ = R(x) - (y' + 1).$$

The case where $C(x) = 1$ is similar.

Hence

$$S(x) + R(x) + C(x) = T(x) \ \& \ \neg C(x+1) = 1 \ \text{or} \\ \exists y (S(x) + y = n \ \& \ C(x+1) = 1 \ \& \\ (C(x) = 0 \Rightarrow R(x) - (y + 1) = T(x)) \ \& \ (C(x) = 1 \Rightarrow R(x) - y = T(x))). \quad \square$$

Commutativity will be mostly assumed rather than cited. For instance, although the next proposition only asserts “ $\forall R (\text{SON}(R) \Rightarrow 0 + R \equiv R)$ ”, its commutative dual, “ $\forall R (\text{SON}(R) \Rightarrow 0 + R \equiv R)$,” will be assumed to be asserted as well, and subsequent citations to *Prop 3.5(a)* might be for the use of either version.

Prop 3.5. (Zero).

- a. $\forall R (\text{SON}(R) \Rightarrow 0 + R \equiv R)$
- b. $\forall R \forall S (R + S \equiv R \Rightarrow S \equiv 0)$
- c. $\forall R \forall S (R + S \equiv 0 \Rightarrow R \equiv 0 \ \& \ S \equiv 0)$
- d. $\neg (R+1) \equiv 0$

Pf:

a. Let n -SON(R). Set C to 0. Then for all $x \leq n$, $R(x) + 0(x) + C(x) = R(x) + 0 + 0 = R(x)$.

b. Let R, S be n -SON. Suppose $R + S \equiv R$. By *Def 3.1* there exists C such that $\forall x \leq n$ ($C(x) \leq 1$) & $C(0) = 0$ and $\forall x \leq n$

$$R(x) + S(x) + C(x) = R(x) \ \& \ \neg C(x+1) = 1 \ \text{or} \\ \exists y (R(x) + y = n \ \& \ C(x+1) = 1 \ \& \\ (C(x) = 0 \Rightarrow S(x) - (y + 1) = R(x)) \ \& \ (C(x) = 1 \Rightarrow S(x) - y = R(x))).$$

We claim that $C(x) = 0 \ \forall x \leq n$. If not, there exists some least $k < n$ such that $C(k+1) = 1$. Then $R(k) + y = n \ \& \ (C(k) = 0 \Rightarrow S(k) - (y + 1) = R(k)) \ \& \ (C(k) = 1 \Rightarrow S(k) - y = R(k))$, for some k, y . But $C(k) = 1$ would contradict the choice of k , so $S(k) - (y + 1) = R(k)$, hence

$S(k) - (y + 1) = n - y$, so $S(k) > n$, contradicting S being an n -SON.

Thus $C(x) = 0 \forall x \leq n$. So $R(x) + S(x) + 0 = R(x)$, $\forall x \leq n$. Thus $S(x) = 0$, $\forall x \leq n$.

c. Let R, S be z -SON. Suppose $R + S = 0$. By Def 3.1 there exists C such that $\forall x \leq z$ ($C(x) \leq 1$) & $C(0) = 0$ and $\forall x \leq z$

$$\begin{aligned} & R(x) + S(x) + C(x) = 0(x) \text{ \& } \neg C(x+1) = 1 \text{ or} \\ & \exists y (R(x) + y = z \text{ \& } C(x+1) = 1 \\ & \text{\& } (C(x) = 0 \Rightarrow S(x) - (y + 1) = 0(x)) \text{ \& } (C(x) = 1 \Rightarrow S(x) - (y + 1) = 0(x))). \end{aligned}$$

Proceed by induction, with ϕ as

$$(i \leq z \Rightarrow R(z-i) = 0 \text{ \& } S(z-i) = 0 \text{ \& } C(z-i) = 0).$$

$\neg C(z+1) = 1$, so $R(z) + S(z) + C(z) = 0(z) = 0$, forcing $R(z) = S(z) = C(z) = 0$. So the assertion holds when $i = 0$.

Now let $n \leq z$ & $\sigma n, m \leq z$. And let $m \leq z$. Then $n \leq z$ (indeed, $n < z$), so by the induction hypothesis, $C(z-n) = 0$, thus $\neg C(z-n) = 0$. So $R(z-n-1) = S(z-n-1) = C(z-n-1) = 0$, i.e. $R(z-m) = S(z-m) = C(z-m) = 0$.

d. Use (c). □

Prop 3.6. Let $n > 0$, and let $R, (R+I)$ be n -SON. Then $\exists k \leq n$ such that:

$$\begin{aligned} & R(k) + 1 = (R+I)(k) \text{ \&} \\ & \forall i < k (R(i) = n \text{ \&} (R+I)(i) = 0) \text{ \&} \\ & \forall i (k < i \leq n \Rightarrow R(i) = (R+I)(i)) \end{aligned}$$

Pf:

By Def 3.1, there exists n -SON C such that $\forall x \leq n$ ($C(x) \leq 1$) & $C(0) = 0$ and $\forall x \leq n$

$$\begin{aligned} & R(x) + I(x) + C(x) = (R+I)(x) \text{ \&} \neg C(x+1) = 1 \text{ or} \\ & \exists y (R(x) + y = n \text{ \&} C(x+1) = 1 \text{ \&} \\ & (C(x) = 0 \Rightarrow I(x) - (y + 1) = (R+I)(x)) \text{ \&} (C(x) = 1 \Rightarrow I(x) - y = (R+I)(x))). \end{aligned}$$

Since C is an n -SON, $C(n+1)$ does not exist, so $\neg C(n+1) = 1$. Thus there exists a least number $k \leq n$ such that $\neg C(k+1) = 1$. So evidently, for all $i < k$, $C(i+1) = 1$.

$R(k) + I(k) + C(k) = (R+I)(k)$ since $\neg C(k+1) = 1$. If $k = 0$, $I(k) + C(k) = 1 + 0 = 1$. And if $k > 0$, then $I(k) = 0$ and $C(k) = 1$, the latter because otherwise $k-1$ would be a number i smaller than k such that $\neg C(i+1) = 1$. So again $I(k) + C(k) = 1$. Hence $R(k) + 1 = (R+I)(k)$.

Let $i < k$. Then by the leastness of k , $C(i+1) = 1$, so for some y ,

$$\begin{aligned} & R(i) + y = n \text{ \&} C(i+1) = 1 \text{ \&} \\ & (C(i) = 0 \Rightarrow I(i) - (y + 1) = (R+I)(i)) \text{ \&} (C(i) = 1 \Rightarrow I(i) - y = (R+I)(i)) \end{aligned}$$

Since $i < k$, $C(i) = 0$ if and only if $i = 0$. Now $I(0) - (y + 1) = (R+I)(0)$ forces $y = 0$, since otherwise the left-hand side would not be defined. So $R(0) = n$ and $(R+I)(0) = 0$.

And for $i > 0$, $I(i) - y = (R+I)(i)$ also forces $y = 0$ since $I(i) = 0$, and so again $R(i) = n$ and $(R+I)(i) = 0$.

Finally, let $k < i \leq n$. So in this case, $k < n$. We claim that $C(i) = 0$. For $C(k+1) = 0$, since $\neg C(k+1) = 1$ and $k + 1 \leq n$. Using induction, suppose $C(x) = 0$ and $k + 1 \leq x < n$. But there exists no y such that $I(x) - (y + 1) = (R+I)(x)$, since $I(x) = 0$ and so the left-hand side would be undefined. Thus the only possibility is $R(x) + I(x) + C(x) = (R+I)(x)$ & $\neg C(x+1) = 1$. $x+1 \leq n$ since $x < n$, and so $C(x+1) = 0$. Hence, if $k < i \leq n$, then $C(i) = 0$.

Hence for all such i , $R(i) + I(i) + C(i) = (R+I)(i)$. But $I(i) = 0$, so $R(i) = (R+I)(i)$. \square

Corollary 3.7

a. If $(R+I)$ exists, then $R < (R+1)$

b. If $R < S$, then $(R+1) \leq S$.

Remark: Note that part of the content of (b) is that, if $R < S$, then I and $(R+I)$ exist.

Pf:

a. By *Prop 3.5(c)*.

b. Let $R < S$. So there exists $v \leq n$ such that $R(v) < S(v)$ & $\forall x (v < x \leq n \Rightarrow R(x) = S(x))$. By *Prop 3.3(d)*, $(R+1)$ exists. So, by *Prop 3.6*,

$$\begin{aligned} R(k) + 1 &= (R+I)(k) \text{ \& } \\ \forall i < k (R(i) = n \text{ \& } (R+I)(i) = 0) \text{ \& } \\ \forall i (k < i \leq n \Rightarrow R(i) = (R+I)(i)), \end{aligned}$$

for some $k \leq n$. If $v < k$, then $n = R(v) < S(v)$, contradicting S being an n -SON. If $v > k$, then $(R+I)(v) = R(v) < S(v)$ and for all $i > v$, $(R+I)(i) = R(i) = S(i)$. Hence $(R+1) \leq S$. And if $v = k$, then $(R+I)(k) = R(k) + 1$ and $R(k) < S(k)$, so $(R+I)(k) \leq S(k)$. By *Prop 2.7(a)*, $(R+1) \leq S$. \square

Theorem 3,8 (SON Induction). Let Nz and let ϕ be a well-formed formula (with no appearance of z) with a free variable R such that $S \equiv T \Rightarrow (\phi [SR] \Leftrightarrow \phi [TR])$, i.e. the formula ϕ respects equivalence. Assume $\phi [0z \setminus R]$ and $\forall R \forall S (z\text{-SON}(R) \text{ \& } (R+I) \equiv S \text{ \& } \phi \Rightarrow \phi [SR])$. Then $\forall R (z\text{-SON}(R) \Rightarrow \phi)$.

Pf:

Suppose to the contrary that $\neg \forall R (z\text{-SON}(R) \Rightarrow \phi)$. Then there exists a z -SON T such that $\neg \phi [TR]$. Let U be the greatest SON such that $\phi [UR]$ and $U \leq T$, which exists by *Prop 2.8(b)* since $\phi [0z \setminus R]$. If $U \equiv T$, then $\phi [TR]$, a contradiction. So $\neg U \equiv T$, and hence $U < T$. By *Corollary 3.7(b)*, $(U+1) \leq T$. By the induction hypothesis, $\phi [(U+1)R]$. But by *Corollary 3.7(a)*, $U < U+1$. So $U+1$ is a larger SON $\leq T$ such that ϕ , a contradiction. \square

We state without proof the important and useful:

Prop 3.9. $\forall R \forall S \forall T ((R + S) + 1 \equiv T \Leftrightarrow R + (S + 1) \equiv T)$. \square

Prop 3.10. (Associativity of SON Addition).

$$\forall R \forall T \forall U \forall V ((T + U) + R \equiv V \Leftrightarrow T + (U + R) \equiv V).$$

Pf:

Proceed by SON Induction (*Theorem*), with ϕ as

$$\forall T \forall U \forall V ((T + U) + R \equiv V \Leftrightarrow T + (U + R) \equiv V).$$

Let $R = 0$. Then, in either direction, the result follows by two applications of *Prop 3.5(a)*.
 Now let $\text{SON}(R) \& (R+1) \equiv S \& \phi$. Then, using the Induction Hypothesis and *Prop 3.9*,

$$\begin{aligned} & V \equiv (T + U) + S \\ \Leftrightarrow & V \equiv (T + U) + (R+1) \\ \Leftrightarrow & V \equiv ((T + U) + R) + 1 \\ \Leftrightarrow & V \equiv (T + (U + R)) + 1 \\ \Leftrightarrow & V \equiv T + ((U + R) + 1) \\ \Leftrightarrow & V \equiv T + (U + (R + 1)) \\ \Leftrightarrow & V \equiv T + (U + S) \end{aligned} \quad \square$$

Prop 3.11. Let R, S be n -SON. Then $R \leq S$ if and only if $\exists T (R + T) \equiv S$.
Pf:

(\Rightarrow) Let $R \leq S$. Consider $\varphi(U)$ as

$$R + U \leq S.$$

$\varphi(0)$ by *Prop 3.5(a)*. So by *Prop 2.8(b)*, there exists a greatest $T \leq S$ such that $R + T \leq S$.
 Suppose $R + T < S$. By *Prop (c)* $(R + T) + 1 \leq S$. By *Corollary 3.7(b)*, $R + (T + 1) \leq S$. By *Corollary 3.7(a)*, $T < T + 1$, contradicting the greatness of T . Thus $\neg R + T < S$, hence $R + T \equiv S$, by *Def 2.5*

(\Leftarrow) Let $R + T \equiv S$. Suppose $\neg R \leq S$. By *Prop 2.6(b)*, $S < R$. By (a) $S + U \equiv R$ for some U . Thus $(R + T) + U \equiv R$, and so by *Prop 3.10*, $R + (T + U) \equiv R$. By *Prop 3.5(b)*, $T + U \equiv 0$. And by *Prop 3.5(c)*, $U \equiv 0$. So by *Prop 3.5(a)*, $S \equiv R$, contradicting $S < R$. Thus, $R \leq S$. \square

Prop 3.12. (Cancellation) $\forall R \forall S \forall T (R + S \equiv R + T \Rightarrow S \equiv T)$

Pf:

Let $R + S \equiv R + T$. By *Prop 2.6(b)*, $S \leq T$ or $T \leq S$. WLOG let $S \leq T$. Then by *Prop 3.11*, $S + U \equiv T$, for some U . Substituting and using *Associativity (Prop 3.10)*,
 $R + S \equiv (R + S) + U$. Thus by *Prop 3.5(b)*, $U \equiv 0$ and so $S \equiv T$ by *Prop 3.5(a)*. \square

Prop 3.13. (Anti-Symmetry) $\forall R \forall S (R \leq S \& S \leq R \Rightarrow R \equiv S)$

Pf:

Let $R \leq S \& S \leq R$. By *Prop 3.11*, $R + T \equiv S$ and $S + U \equiv R$, for some T, U .
 Substituting and using *Associativity (Prop 3.10)*, $R + (T + U) \equiv R$. So by *Prop 3.5(b)*, $3.5(c)$, and *3.5(a)*, $R \equiv S$. \square

Prop 3.14.

a. $\forall A \forall B \forall X \forall Y \forall Z (A \leq X \& B \leq Y \& (X + Y) \equiv Z \Rightarrow (A + B) \leq Z)$

b. $\forall A \forall X \forall Y \forall Z (X \leq Y \ \& \ (Y + Z) \equiv A \Rightarrow (X + Z) \leq (Y + Z))$

c. $\forall X \forall Y \forall Z ((X + Z) \leq (Y + Z) \Rightarrow X \leq Y)$

d. $\forall A \forall B \forall X \forall Y (X + Y \equiv A + B \ \& \ X < A \Rightarrow B < Y)$ □

Prop 3.15. $\forall R \forall S (R < S \Leftrightarrow R + I \leq S)$

Pf.

The \Rightarrow direction is just *Corollary 3.7(b)*.

Now suppose $R + I \leq S$. Then $R \leq S$ by *Corollary 3.7(a)* and *Transitivity (Prop 2.6(a))*. Also, $(R + I) + T \equiv S$, for some T , by *Prop 3.11*. Re-arranging by *Commutativity* and *Associativity*, $R + (T + I) \equiv S$. If $R \equiv S$, then $(T + I) \equiv 0$ by *Prop 3.5(a)*, contradicting *Prop 3.5(d)*. Thus $\neg R \equiv S$, and so $R < S$, by *Def 2.5*. □

Corollary 3.16. $\forall R \forall S (R < S \Leftrightarrow \exists T (T > 0 \ \& \ R + T \equiv S))$ □

When SONs coincide with numbers, SON addition coincides with normal addition:

Prop. Let $R = n$ and $S = m$, and suppose $n + m = k$. Then $(R + S) = k$. □

Propositions 3.11 and *3.12* show that when $R \leq S$, there is a unique (up to equivalence) T such that $R + T \equiv S$. This allows the definition of subtraction.

Def. Suppose $R \leq S$. Let $(R - S)$ denote that T such that $R + T \equiv S$. □

All properties of subtraction will be assumed to hold.

4. Sequences of Sequences and Sums

Recall from *Arithmetic without the Successor Axiom Section 11A* that it is possible to speak of sequences of sequences:

Def 4.1. Let N_n . B is a sequence to n of sequences - written $SeqOfSeq(B,n)$ - if and only if

$$\forall i \forall j \forall k (B_{i,j,k} \Rightarrow i \leq n) \\ \& \forall i (i \leq n \Rightarrow \text{Seq}(\{(j,k) : B_{i,j,k}\}))$$

$\text{SeqOfSeq}(B)$ if and only if $\exists n \text{SeqOfSeq}(B,n)$. □

Def 4.2. Suppose $\text{SeqOfSeq}(B)$. We say X is the i^{th} sub-sequence of B if and only if

$$\text{Seq}(X) \& \forall j \forall k (B_{i,j,k} \Leftrightarrow X_{j,k}).$$

Obviously X is unique up to equivalence. By an abuse of notation, B_i will be used to refer to X . □

With sequences of sequences it is possible to define the sum of a sequence:

Def 4.3. Let \mathbb{N}_z , $z\text{-SON}(T)$, and $\text{SeqOfSeq}(B,n)$, where $\forall i \leq n z\text{-SON}(B_i)$. Suppose there exists S where $\text{SeqOfSeq}(S,n) \& \forall i \leq n z\text{-SON}(S_i)$ such that $S_0 \equiv B_0 \& \forall i < n S_{i+1} \equiv B_{i+1} + S_i \& S_n \equiv T$. Then we write

$$T \equiv \sum_{i=0}^n B_i. \quad \square$$

By induction it is easy to see that $\sum_{i=0}^n B_i$, if it exists, must be unique up to equivalence.

And if $B_i \equiv C_i$ for all i , then $\sum_{i=0}^n B_i \equiv \sum_{i=0}^n C_i$. Also, the sum inherits all the properties of addition (such as commutativity) that one would expect.

Def 4.4. Let \mathbb{N}_z , $z\text{-SON}(R)$, and $\text{SeqOfSeq}(B,n)$, where $\forall i \leq n B_i \equiv R$. And suppose that $\sum_{i=0}^{n-1} R_i$ exists. Then write it as $n * R$, stipulating that $0 * R$ is 0 . □

Again, $n * R$ is unique up to equivalence. Also, if $R \equiv S$, then $n * R \equiv n * S$ (if existing).

Prop 4.5. Let R,S be $z\text{-SONs}$.

a. $0 * R \equiv 0$

b. If 1 exists, then $1 * R \equiv R$.

c. Let $n > 0$, and suppose either: $(n * m) * R$ exists; or both $n * (m * R)$ and $(n * m)$ exist. Then $(n * m) * R \equiv n * (m * R)$.

Remark: It is possible that $n * (m * R)$ exists, but that $(n * m)$ is too big as a first-order number and so does not exist. It is also possible, if $n = 0$, that $(n * m) * R$ exists but that $m * R$ is too big and so does not exist. Hence the use of “ $n > 0$ ”.

d. Suppose either: $(n + m) * R$ exists; or both $n * R + m * R$ and $(n + m)$ exist. Then $(n + m) * R \equiv n * R + m * R$.

e. Suppose either: $n * (R + S)$ exists; or both $n * R + n * S$ and $(R + S)$ exist. Then $n * (R + S) \equiv n * R + n * S$.

f. If $R \leq S$ and $n * S$ exists, then $n * R \leq n * S$.

g. If $\text{len}(R) \leq z - k$, then $k * R$ exists.

h. Suppose $n \leq z$. Then $n * 1 = \langle n \rangle$.

Pf:

g. Let $\text{len}(R) \leq z - k$. If $k = 0$, then the result follows triivially from (a). So let $k > 0$, and thus $\text{len}(R) < z$. Proceed by induction, with ϕ as

$$n \leq k \Rightarrow \text{len}(n * R) \leq z - k + n.$$

$0 * R \equiv 0$ by (a), and $\text{len}(0) = 0 \leq z - k$, so ϕ holds when $n = 0$.

Now let $Nn \ \& \ \sigma n, m \ \& \ \phi$. And suppose $m \leq k$. Then $n \leq k$ (indeed, $n < k$), so by the Induction Hypothesis, $\text{len}(n * R) \leq z - k + n$. Thus $\text{len}(n * R) < z$. By Prop (b), $n * R + R$ exists and $\text{len}(n * R + R) \leq z$ by Prop 3.3(b). By (b) and (d), $m * R \equiv n * R + R$, so $\text{len}(m * R) \leq z$.

Hence by Induction, $\forall n (Nn \Rightarrow \phi)$. Thus $\text{len}(k * R) \leq z - k + k$, and in particular, $k * R$ exists. \square

5. Shifts and Multiplication

Def 5.1. Let R be an n -SON, and let $k \leq n$. Suppose S is an n -SON such that all of:

a. $i < k \Rightarrow S(i) = 0$ and

b. $k \leq i \leq n \Rightarrow S(i) = R(i - k)$ and

c. $(n - k) < i \leq n \Rightarrow R(i) = 0$.

Then we call S the k shift of R and write $S \equiv R // k$. \square

Remark that clause (c) holds if and only if $\text{len}(R) \leq n - k$, and so n -SON R has a k shift if and only if $\text{len}(R) \leq n - k$.

As usual a shift is unique up to equivalence and is equivalent for equivalent SONs.

Example 5.2. Consider 4-SONs 00012 (R) and 12000 (S), and $k = 3$. Then $00012 // 3 = 12000$, since:

a. $i < 3 \Rightarrow i = 0, 1, \text{ or } 2 \Rightarrow S(i) = 0$

b. $3 \leq i \leq 4 \Rightarrow i = 3 \text{ or } i = 4. S(3) = 2 = R(0) \text{ and } S(4) = 1 = R(1).$

c. $1 < i \leq 4 \Rightarrow i = 2, 3, \text{ or } 4 \Rightarrow R(i) = 0.$

□

Prop 5.3. Let R, S be z -SON.

a. $R // 0 \equiv R$

b. Suppose $n \leq z$. Then $0 // n \equiv 0$.

c. Suppose for some k , $R(k) = 1$ & $\forall i (i \leq n \ \& \ \neg i = k \Rightarrow R(i) = 0)$. Then $R \equiv I // k$.

d. If $I // k$ exists, then $\text{len}(I // k) = k$.

e. Suppose $\text{len}(R) \leq z - (n + m)$. Then $(R // n) // m \equiv R // (n + m)$.

f. Suppose $\text{len}(R + S) \leq z - n$. Then $(R + S) // n \equiv (R // n) + (S // n)$.

g. Suppose $\text{len}(n * R) \leq z - m$ & $n > 0$. Then $(n * R) // m \equiv n * (R // m)$.

h. Suppose $z \geq 1$. Then $z * I + I \equiv I // 1$.

i. Suppose $z \geq 1$ and $(z + 1)$ exists. Then $(z + 1) * I \equiv I // 1$.

j. If $\text{len}(R) \leq z - 1$, then $z * R + R \equiv R // 1$.

k. $R \equiv \sum_{i=0}^z (< R(i) > // i)$

Pf:

h. By Prop 4.5(h) $z * I \equiv <z>$. By Prop 3.3(e), $z * I + I \equiv 000\dots010$. But this is just $I // 1$, by (c).

i. By (h) $z * I + I \equiv I // 1$. By Prop 4.5(b), $1 * I \equiv I$. By Prop 4.5(d), $(z + 1) * I \equiv z * I + 1 * I$.

j. Proceed by SON Induction (*Theorem 3.8*), with ϕ as

$$\text{len}(R) \leq z - 1 \Rightarrow z * R + R \equiv R // 1.$$

Suppose $\text{len}(0) \leq z - 1$. Then $1 \leq z$. So $0 * 0 + 0 \equiv 0$, by Prop 3.5(a) and Prop 4.5(a).

And $0 // 1 \equiv 0$ by (b). Thus $0 * 0 + 0 \equiv 0 // 1$.

Now let $\text{SON}(R) \& (R+I) \equiv S \& \phi$. And assume $\text{len}(S) \leq z - 1$, which again implies $1 \leq z$. Then:

$$\begin{aligned} (R + I) // 1 &\equiv (R // 1) + (I // 1) && \text{by (f)} \\ &\equiv z * R + R + z * I + I && \text{by (h)} \\ &\equiv z * (R + I) + (R + I) && \text{by Prop 4.5(e)} \end{aligned}$$

k. Proceed by induction, , with ϕ as

$$\forall R (\text{len}(R) \leq n \Rightarrow R \equiv \sum_{i=0}^n (< R(i) > // i)).$$

If $\text{len}(R) = 0$, then $R \equiv <R(0)>$. By (a) $R \equiv <R(0)> // 0$.

Now let $\text{Nn} \& \sigma n, m \& \phi$. Assume $\text{len}(R) = m$. Set S to $R \setminus \{(x,y) : x = m\} \cup \{(m,0)\}$. Then $\text{len}(S) < \text{len}(R)$ by Prop 2.4, so $\text{len}(S) \leq n$. By the Induction Hypothesis,

$$S \equiv \sum_{i=0}^n (< S(i) > // i).$$

By definition of S , $S(i) = R(i)$ for all $i \leq n$. So

$$S \equiv \sum_{i=0}^n (< R(i) > // i).$$

It can be checked that $S + (<R(m)> // m) \equiv R$, whence

$$R \equiv \sum_{i=0}^m (< R(i) > // i) \quad \square$$

It is now possible to introduce multiplication:

Def 5.4. Let R, S be n -SON. Suppose $\sum_{i=0}^n (R(i) * S) // i$ exists. Then we call this sum $R * S$. □

Evidently, $R * S$ is unique up to equivalence and is equivalent for equivalent SONs. As usual, $*$ will have precedence over $+$ in formulas; so e.g. we will write $R * S + T$ instead of $(R * S) + T$.

Prop 5.5. Let R be a SON. Then $R * 0 \equiv 0 * R \equiv 0$. □

Prop 5.6. Suppose either:

a. $R * (S + I)$ exists; or

b. $R * S + R$ and $S + I$ exist.

Then:

$$R * (S + I) \equiv R * S + R.$$

Remark: If $R * S + R$ exists and $\neg R \equiv 0$, then $S + I$ exists.

Pf:

Suppose $R * S + R$ and $S + I$ exist. Then

$$\begin{aligned} R * S + R &\equiv \sum_{i=0}^n (R(i) * S) // i + \sum_{i=0}^n \langle R(i) \rangle // i && \text{by Def 5.4, Prop 5.3(k)} \\ &\equiv \sum_{i=0}^n (R(i) * S) // i + \sum_{i=0}^n (R(i) * 1) // i && \text{by Prop 4.5(h)} \\ &\equiv \sum_{i=0}^n (R(i) * S + R(i) * 1) // i && \text{by Prop 5.3(f)} \\ &\equiv \sum_{i=0}^n (R(i) * (S + I)) // i && \text{by Prop 4.5(e)} \\ &\equiv R * (S + I) && \text{by Def 5.4.} \end{aligned}$$

Remark the reverse direction holds should $R * (S + I)$ exist. □

Prop 5.7. Suppose either:

a. $(T + I) * R$ exists; or

b. $T * R + R$ and $(T + I)$ exist.

Then:

$$(T + I) * R \equiv T * R + R.$$

Remark: If $T * R + R$ exists and $\neg R \equiv 0$, then $T + I$ exists.

Pf:

We will prove the proposition when case (a) obtain. Proceed by SON Induction (*Theorem 3.8*), with ϕ as

$$\forall T (\exists U (T + I) * R \equiv U \Rightarrow (T + I) * R \equiv T * R + R).$$

For let $\exists U (T + 1) * 0 \equiv U$. Then $(T + 1)$ exists, so $(T + 1) * 0 \equiv 0 \equiv (T * 0) + 0$, by *Prop 5.5* and *Prop 3.5(a)*.

Now let $\text{SON}(R) \ \& \ (R + 1) \equiv S \ \& \ \phi$. And assume $(T + 1) * S \equiv U$. Then:

$$\begin{aligned}
 (T + 1) * S &\equiv (T + 1) * (R + 1) \\
 &\equiv (T + 1) * R + (T + 1) && \text{by Prop 5.6} \\
 &\equiv (T * R + R) + (T + 1) && \text{by the Induction Hypothesis} \\
 &\equiv (T * R + T) + (R + 1) && \text{by Commutativity and} \\
 &&& \text{Associativity of SON Addition} \\
 &\equiv T * (R + 1) + (R + 1) && \text{by Prop 5.6} \\
 &\equiv T * S + S && \square
 \end{aligned}$$

Prop 5.8. Let R be a n -SON, with $n \geq 1$. Then: $1 * R \equiv R \equiv R * 1$. \square

Prop 5.9. (Commutativity of SON Multiplication) Let R, T be SON, where $T * R$ exists. Then $T * R \equiv R * T$.

Pf:

Proceed by SON Induction (*Theorem 3.8*), with ϕ as

$$\forall T (\exists V (T * R \equiv V) \Rightarrow T * R \equiv R * T).$$

$T * 0 \equiv 0 \equiv 0 * T$ by *Prop 5.5*.

Now let $\text{SON}(R) \ \& \ (R + 1) \equiv S \ \& \ \phi$. And assume $T * S \equiv V$. Then:

$$\begin{aligned}
 T * S &\equiv T * (R + 1) \\
 &\equiv T * R + R && \text{by Prop 5.6} \\
 &\equiv R * T + R && \text{by the Induction Hypothesis} \\
 &\equiv (R + 1) * T && \text{by Prop 5.7} \quad \square
 \end{aligned}$$

Prop 5.10. (Distributive Law) Suppose either:

- a. $(U + T) * R$ exists; or
- b. $(U * R) + (T * R)$ and $(U + T)$ exist.

Then:

$$(U + T) * R \equiv (U * R) + (T * R).$$

Remark: If $(U * R) + (T * R)$ exists and $\neg R \equiv 0$, then $U + T$ exists.

Pf:

We will prove the proposition when case (a) obtain. Proceed by SON Induction (*Theorem 3.8*), with ϕ as

$$\forall T \forall U (\exists V (U + T) * R \equiv V \Rightarrow (U + T) * R \equiv (U * R) + (T * R)).$$

If $\exists V (U + T) * 0 \equiv V$, then $(U + T)$, U , and T are SON, so $(U + T) * 0 = 0$ and $U * 0 + T * 0 \equiv 0 + 0 \equiv 0$ by *Props 5.5* and *3.5(a)*.

Now let $\text{SON}(R) \& (R + I) \equiv S \& \phi$. And assume $(U + T) * S \equiv V$. Then:

$$\begin{aligned}
(U + T) * S &\equiv (U + T) * (R + I) \\
&\equiv (U + T) * R + (U + T) && \text{by Prop 5.6} \\
&\equiv (U * R + T * R) + (U + T) && \text{by the Induction Hypothesis} \\
&\equiv (U * R + R) + (T * R + T) && \text{by Commutativity and} \\
&&& \text{Associativity of SON Addition} \\
&\equiv U * (R + I) + T * (R + I) && \text{by Prop 5.6} \\
&\equiv U * S + T * S && \square
\end{aligned}$$

Prop 5.11. (Associativity of SON Multiplication) Suppose $(U * T) * R$ and $(T * R)$ exist. Then $(U * T) * R \equiv U * (T * R)$.

Remark: If $(U * T) * R$ exists and $\neg U \equiv 0$, then $(T * R)$ exists.

Pf:

Proceed by SON Induction (*Theorem 3.8*), with ϕ as

$$\forall T \forall U (\exists V (U * T) * R \equiv V \Rightarrow (U * T) * R \equiv U * (T * R)).$$

Suppose $\exists V (U * T) * 0 \equiv V$. Then $(U * T) * 0 \equiv 0$ and $U * (T * 0) \equiv 0$, by *Prop 5.5*. Now let $\text{SON}(R) \& (R + I) \equiv S \& \phi$. And assume $(U * T) * S \equiv V$. Then:

$$\begin{aligned}
(U * T) * S &\equiv (U * T) * (R + I) \\
&\equiv (U * T) * R + U * T && \text{by Prop 5.6} \\
&\equiv U * (T * R) + U * T && \text{by the Induction Hypothesis} \\
&\equiv U * (T * R + T) && \text{by Prop 5.10} \\
&\equiv U * (T * (R + I)) && \text{by Prop 5.6} \\
&\equiv U * (T * S) && \square
\end{aligned}$$

Prop 5.12. Suppose $S * T$ exists. Then:

a. $R \leq S \Rightarrow R * T \leq S * T$. In particular, $R \leq S \Rightarrow R * T$ exists.

b. $R < S \& \neg T \equiv 0 \Rightarrow R * T < S * T$. In particular, $R < S \& \neg T \equiv 0 \Rightarrow R * T$ exists.

c. $S > I \Rightarrow T < S * T$

Pf:

a. Suppose $R \leq S$. By *Prop 3.11*, $R + U \equiv S$, for some U . Then $(R + U) * T \equiv S * T$, so $R * T + U * T \equiv S * T$. By *Prop 3.11* again, $R * T \leq S * T$.

b. Suppose $R < S \& \neg T \equiv 0$. By *Corollary 3.7(b)*, $R + I \leq S$. By (a) $(R + I) * T \leq S * T$. By *Prop 5.7* and *Prop 3.11*, $R * T + T + U \equiv S * T$ for some U . By *Prop 3.11* again, $R * T \leq S * T$. Suppose $R * T \equiv S * T$. Then $T \equiv 0$ by two applications of *Prop 3.5(c)*.

c. Suppose $S > I$. Then $S * T > I * T$, by (b). Thus $S * T > T$ by *Prop 5.8*. □

Intelligent manipulation allows one to skirt too big numbers and arrive at the normal conclusion. For instance:

Corollary 5.13. Suppose $A \leq X$ and $B \leq Y$ and $C \leq A * B$ and $0 < D$. And suppose $C \equiv QC * D$ and $A \equiv QA * D$. And finally suppose $QA * B$ exists. Then $QC \leq QA * B$.

Remark: The normal reasoning would say that $C \leq X * Y$, and then divide both sides by D . However, one may not know that $X * Y$ exists.

Pf:

Suppose $\neg QC \leq QA * B$. Then $QC > QA * B$. Then $QC * D > QA * B * D$ by *Prop 5.12(b)*, hence $C > A * B$, a contradiction. \square

Lemma 5.14. Let R, S be z -SON where $len(R * S) \leq z - k$. Then $(R * S) // k \equiv R * (S // k)$.

Pf:

Apply *Prop 5.3(e)*. \square

Prop 5.15. Let Nz , and let R and S be z -SON. Suppose $len(R) + len(S) \leq z - 1$. Then $R * S$ exists.

Pf:

Set $n = len(R)$ and $m = len(S)$. $n + 1 \leq z$, so $I // (n + 1)$ exists. By *Prop 5.3(d)* and *Prop 2.6(g)*, $R \leq I // (n + 1)$. Define S' as $\{(x, y) : (x \leq m \Rightarrow y = z) \ \& \ (m < x \leq z \Rightarrow y = 0)\}$. Then evidently $len(S') = m$. By *Prop 2.7(b)*, $S' \geq S$. $len(S') + (n + 1) \leq z$, so $S' // (n + 1)$ exists. But

$$\begin{aligned} S' // (n + 1) &\equiv (S' * I) // (n + 1) && \text{by Prop 5.8} \\ &\equiv S' * (I // (n + 1)) && \text{by Lemma 5.14.} \end{aligned}$$

So, by *Prop 5.12(a)*, $R * S$ exists. \square

Prop 5.16.

a. $R * T \equiv S * T \ \& \ \neg T \equiv 0 \Rightarrow R \equiv S$.

b. $R * T \leq S * T \ \& \ \neg T \equiv 0 \Rightarrow R \leq S$.

c. $R * T < S * T \Rightarrow R < S$.

Pf:

a. If $R < S$, then $R * T < S * T$ by *Prop 5.12(b)*, so $\neg R < S$. Similarly, $\neg S < R$. By *Prop 2.6* and *Def 2.5*, $R \equiv S$. \square

Lemma 5.17. Suppose $(1 // n) * (1 // m)$ or $1 // (n + m)$ exists. Then $(1 // n) * (1 // m) \equiv 1 // (n + m)$. □

Prop 5.18. Let \mathbb{N}_z , and let R and S be z -SON. Suppose $len(R) = n$ and $len(S) = m$ and that $R * S$ exists. Then $len(R * S) = n + m$ or $len(R * S) = n + m + 1$.

Pf:

By *Prop 2.7(a)* $R \geq 1 // n$ and $S \geq 1 // m$. By *Prop 5.12*, $R * S \geq (1 // n) * (1 // m)$. By *Lemma 5.17*, $R * S \geq 1 // (n + m)$. But by *Prop 5.3(d)*, $len(1 // (n + m)) = n + m$. So by *Prop 2.6(f)*, $len(R * S) \geq n + m$.

Suppose $n + m$ is the largest number, so $len(R * S) \leq n + m$, which forces $len(R * S) = n + m$.

Otherwise suppose $n + m + 1$ is the largest number. Then $len(R * S) \leq n + m + 1$, which forces $len(R * S) = n + m$ or $len(R * S) = n + m + 1$.

Otherwise, $n + m + 1$ exists but is not the largest number. So $n + m + 2$ exists. In $z \leq n + m + 1$, then $len(R * S) \leq n + m + 1$ since $R * S$ exists and is a z -SON. This would again force $len(R * S) = n + m$ or $len(R * S) = n + m + 1$.

Otherwise, $z \geq n + m + 2$. So $1 // (n + m + 2)$ exists.

Thus $len(1 // (n + 1)) = n + 1 > len(R)$ and $len(1 // (m + 1)) = m + 1 > len(S)$, by *Prop 5.3(d)*. Hence $1 // (n + 1) > R$ and $1 // (m + 1) > S$, by *Prop 2.6(g)*. But

$$(1 // (n + 1)) * (1 // (m + 1)) \equiv 1 // (n + m + 2)$$

by *Lemma 5.17*. $(1 // (n + 1)) * (1 // (m + 1)) > R * S$, by *Prop 5.12(b)*. Thus $1 // (n + m + 2) > R * S$. By *Prop 2.7(d)*, $n + m + 2 > len(R * S)$. □

Corollary 5.19. Suppose $A \equiv Q * B + R$ and $len(B) \geq 1$. Then $len(Q) < len(A)$. □

Prop 5.20. (Division Algorithm)

a. (Existence) $\forall A \forall B (SON(A) \& SON(B) \& \neg B \equiv 0 \Rightarrow \exists Q \exists R (A \equiv Q * B + R \& R < B))$.

b. (Uniqueness). $\forall A \forall B \forall Q \forall R \forall Q' \forall R' (A \equiv Q * B + R \& R < B \& A \equiv Q' * B + R' \& R' < B \Rightarrow Q \equiv Q' \& R \equiv R')$.

Pf:

a. Assume $SON(A) \& SON(B) \& \neg B \equiv 0$. Consider $\varphi(R)$ as

$$\exists Q A \equiv Q * B + R.$$

Now $A \equiv 0 * B + A$ by *Props 3.5(a)* and *5.5*, so by *Well-Ordering (Prop 2.8(a))*, there exists a least R such that $\exists Q A \equiv Q * B + R$. Hence, $A \equiv Q * B + R$, for some Q .

Suppose $\neg R < B$. By *Prop 2.6(b)*, $B \leq R$. By *Prop 3.11*, $B + C \equiv R$, for some C . But $\neg B \equiv 0$, so $C < R$ by *Corollary 3.16*. Then $A \equiv Q * B + B + C \equiv (Q + 1) * B + C$, which contradicts the assumption of the leastness of R . Hence $R < B$. □

Corollary 5.21. Suppose $Q * X + R < A * X + B \& R < X \& B < X$. Then $Q \leq A$.

Pf:

$A * X + B \equiv Q * X + R + S$ for some $S > 0$, by *Corollary 3.16*. If $R + S < X$, then by the uniqueness of the *Division Algorithm (Prop 5.20(b))*, $A \equiv Q$. Otherwise, $R + S \geq X$ and so $> B$, and thus $Q * X < A * X$ by *Corollary 3.16*. Hence by *Prop 5.16(c)*, $Q < A$. \square

SON Multiplication co-incides where possible with other multiplications.

Prop 5.22.

a. Suppose $A = a$ and $B = b$ and $a * b = c$. Then $A * B = c$.

b. Let B, C be n -SON and let $a \leq n$. Then $\langle a \rangle * B \equiv C$ if and only if $a * B \equiv C$. \square

6. Products of Sequences

Def 6.1. Let Nz , z -SON(T), and $SeqOfSeq(B, n)$, where $\forall i \leq n$ z -SON(B_i). Suppose also $SeqOfSeq(S, n)$ and $\forall i \leq n$ z -SON(S_i) such that $S_0 \equiv B_0$ & $\forall i < n$ $S_{i+1} \equiv B_{i+1} * S_i$ & $S_n \equiv T$. Then we write

$$T \equiv \prod_{i=0}^n B_i. \quad \square$$

By induction it is easy to see that $\prod_{i=0}^n B_i$, if it exists, must be unique up to equivalence.

And if $B_i \equiv C_i$ for all i , then $\prod_{i=0}^n B_i \equiv \prod_{i=0}^n C_i$. Also, the product inherits all the properties of addition (such as commutativity) that one would expect.

Consider z -SONs, where $z > 0$. Set B_0 to 1 and B_i to $\langle i \rangle$ for $0 < i \leq z$. And consider $T_k \equiv \prod_{i=0}^k B_i$. Now T_0 is just 1 , so $len(T_0) = 0$. And $len(B_i) = 0$ for all i with $0 < i \leq z$, so by an easy induction, and using *Corollary ??* and *Prop ??*, T_n exists and indeed $len(T_n) \leq n$, for any $n \leq z$. Hence, we define:

Def 6.2. Let $0 < z$. For $n \leq z$, set $n!_z$ (read n factorial) to $\prod_{i=0}^n B_i$, where the B_i are z -SON and $B_0 \equiv 1$ and $B_i \equiv \langle i \rangle$ for $0 < i \leq z$. When the subscript z can be understood, it will be dropped. \square

The usual properties of factorials will be assumed.

Remark that the definition of $n!$ uses recursion in the standard fashion, which is possible since factorial here is being defined only for first-order numbers, and so there indeed exist sequences of the required length.

Exponentiation will prove more difficult to define, since we need to define it for second-order numbers, but recursion is nonetheless the most convenient method. Fortunately, because exponentiation increases the size of the results very quickly, the length of the sequence required is nonetheless limited, and a piecemeal definition suffices. That is, exponentiation will be defined in a series of steps, where officially we are overloading the exponential function with several different meanings, which in practice should not cause any problems since the results always co-incide.

First, define the exponential when the exponent is a first-order number:

Def 6.3. Let $0 < z$, z -SON(R), $n \leq z$, and $SeqOfSeq(B, n)$, where $B_0 \equiv 1$ and $\forall i (0 < i \leq n \Rightarrow B_i \equiv R)$. And suppose $\prod_{i=0}^n B_i$ exists. And finally suppose either $n > 0$ or $R > 0$ (in order to leave undefined 0^0). Then we set R^n to $\prod_{i=0}^n B_i$. □

R^n does not always exist, since it may be too big. Nonetheless, by *Props 5.15* and *5.18*, R^n exists should $len(R) = 0$ (and either $n > 0$ or $R > 0$). Remark that, for any z -SON(R) with $z > 0$, R^1 exists and indeed $R^1 \equiv R$; and if R^n exists for $n > 0$, then $R^n \equiv R^{n-1} * R$. From these facts the usual properties of the first-order exponential follow.

Remark, however, that, $R^n * R$ may exist without R^{n+1} existing, since $n+1$ may not exist. For instance, consider 5-SONs where 5 is the largest number. Then $\langle 2 \rangle^5 * 2 \equiv 144$, but $\langle 2 \rangle^6$ does not exist since 6 does not.

It remains to define the exponential for second-order and not just first-order exponents. In fact, it suffices to define the exponential for second-order exponents of the form $\langle a \rangle * \langle b \rangle + \langle c \rangle$, since otherwise the result would be too big. First, it is necessary to show that any such result is unique (up to equivalence).

Prop 6.4. Let $R > 0$. If $S \equiv \langle a \rangle * \langle b \rangle + \langle c \rangle \equiv \langle d \rangle * \langle e \rangle + \langle f \rangle$ & $c < a$ & $f < d$ and $(R^a)^b * R^c$ exists, then $(R^a)^b * R^c \equiv (R^d)^e * R^f$.

Pf:

Suppose the assertion is not true. Then for some least S it is not true, i.e.

$S \equiv \langle a \rangle * \langle b \rangle + \langle c \rangle \equiv \langle d \rangle * \langle e \rangle + \langle f \rangle$ & $c < a$ & $f < d$ & $(R^a)^b * R^c$ exists, but not $(R^a)^b * R^c \equiv (R^d)^e * R^f$.

Suppose $a = 0$ or $b = 0$. Then $S \equiv \langle c \rangle$, so $c = d * e + f$. But then $(R^a)^b * R^c \equiv (R^d)^e * R^f$ by the standard properties of the first-order exponential, a contradiction. Similarly, a contradiction results if $d = 0$ or $e = 0$.

Hence assume $a, b, d, e > 0$. Then

$$S \equiv \langle a \rangle * \langle b-1 \rangle + \langle a \rangle + \langle c \rangle,$$

by the *Distributive Law* (Prop 5.10), and $S > \langle a \rangle * \langle b-1 \rangle + \langle c \rangle$ by *Corollary 3.16*.

$(Ra)^{b-1} * Rc$ exists since $(Ra)^b * Rc$ does, and indeed $(Ra)^b * Rc \equiv (Ra)^{b-1} * Ra * Rc$.

By the *Division Algorithm* (Prop 5.20), there exist T, U such that

$$\langle a \rangle * \langle b-1 \rangle + \langle c \rangle = T * \langle d \rangle + U \ \& \ U < \langle d \rangle.$$

Since U is less than $\langle d \rangle$ it has length 0 by Prop 2.6(f), so $U \equiv \langle u \rangle$ for some u , with $u < d$.

Also, $\langle d \rangle * \langle e \rangle + \langle f \rangle > T * \langle d \rangle + \langle u \rangle$ by *Corollary 3.16*. Both $f, u < d$, so $\langle e \rangle \geq T$ by *Corollary 5.21*, which likewise forces $T \equiv \langle t \rangle$, for some t . Thus

$$\langle a \rangle * \langle b-1 \rangle + \langle c \rangle \equiv \langle d \rangle * \langle t \rangle + \langle u \rangle \ \& \ u < d.$$

By leastness of S ,

$$(Ra)^{b-1} * Rc \equiv (Rd)^t * Ru.$$

Thus

$$(Ra)^b * Rc \equiv (Rd)^t * Ru * Ra.$$

By the *Division Algorithm* for first-order numbers, $u = x * d + y$, for some x, y where $y < d$, and $a = p * d + q$, where $q < d$. So $Ru \equiv (Rd)^x * Ry$ and $Ra \equiv (Rd)^p * Rq$, and thus

$$(Ra)^b * Rc \equiv (Rd)^t * (Rd)^x * (Rd)^p * Ry * Rq$$

Adding and grouping, $\langle u \rangle + \langle a \rangle = (\langle x \rangle + \langle p \rangle) * \langle d \rangle + (\langle y \rangle + \langle q \rangle)$. Noting that

$$\langle d \rangle * \langle e \rangle + \langle f \rangle \equiv \langle d \rangle * \langle t \rangle + \langle u \rangle + \langle a \rangle,$$

substitution yields

$$\langle d \rangle * \langle e \rangle + \langle f \rangle \equiv (\langle t \rangle + \langle x \rangle + \langle p \rangle) * \langle d \rangle + (\langle y \rangle + \langle q \rangle).$$

Either $\langle y \rangle + \langle q \rangle < \langle e \rangle$ or $\langle y \rangle + \langle q \rangle - \langle e \rangle < \langle e \rangle$. Consider the first case (the second case is similar). By the uniqueness of the *Division Algorithm*, $y + q = f$ and $t + x + p = e$. Hence

$$(Ra)^b * Rc \equiv (Rd)^{(t+x+p)} * R^{(y+q)} \equiv (Rd)^e * R^f,$$

the desired contradiction. □

The previous proposition means the following definition is permissible:

Def 6.5. Let $0 < z$. Let R, S be z -SON. If $R \equiv 0$ and $S > 0$, or if $R \equiv 1$, then set R^S to 1 . And if $R > 1$ and $S \equiv \langle a \rangle * \langle b \rangle + \langle c \rangle$ where $c < a$, then use R^S to denote $(Ra)^b * Rc$, if this latter exists. □

Prop 6.6. Let $0 < z$. Let R, S, T be z -SON. Then:

- a. If $S > 0$, then $0^S \equiv 1$.
- b. $1^S \equiv 1$.
- c. Let $R > 1$. If R^{S+1} or $R^S * R$ exists, then $R^{S+1} \equiv R^S * R$.
- d. Let $R, S, T > 0$. If $(R * S)^T$ or $R^T * S^T$ exists, $(R * S)^T \equiv R^T * S^T$.
- e. Let $R > 1$. If $R^S * R^T$ or $R^{(S+T)}$ exists, then $R^S * R^T \equiv R^{(S+T)}$.
- f. Let $R > 1$. If $(R^S)^T$ or $R^{(S^*T)}$ exists, then $(R^S)^T \equiv R^{(S^*T)}$.

Pf:

a,b. These follow directly from the definition.

c. Consider the case where R^{S+1} exists. Then $S + 1 \equiv \langle a \rangle * \langle b \rangle + \langle c \rangle$, for some a, b, c with $c < a$, and $R^{S+1} \equiv (R^a)^b * R^c$. If $c > 0$, then $S \equiv \langle a \rangle * \langle b \rangle + \langle c-1 \rangle$, and $R^S \equiv (R^a)^b * R^{c-1}$, and so $R^{S+1} \equiv R^S * R$.

Otherwise, $c = 0$ and so $S + 1 \equiv \langle a \rangle * \langle b \rangle$ and $R^{S+1} \equiv (R^a)^b$. Both $a, b > 0$ by *Props 5.5* and *3.5(d)*, so $S + 1 \equiv \langle a \rangle * \langle b-1 \rangle + \langle a \rangle$ by the *Distributive Law (Prop 5.10)*. But then $S \equiv \langle a \rangle * \langle b-1 \rangle + \langle a-1 \rangle$ and obviously $a-1 < a$, so $R^S \equiv (R^a)^{b-1} * R^{a-1}$. But then $R^S * R \equiv (R^a)^{b-1} * R^{a-1} * R \equiv (R^a)^{b-1} * R^a \equiv (R^a)^b \equiv R^{S+1}$.

Now consider the case where $R^S * R$ exists. Then $S \equiv \langle a \rangle * \langle b \rangle + \langle c \rangle$, for some a, b, c with $c < a$, and $R^S \equiv (R^a)^b * R^c$. If $c+1 < a$, then $S + 1 \equiv \langle a \rangle * \langle b \rangle + \langle c+1 \rangle$ and $R^S * R \equiv (R^a)^b * R^c * R \equiv (R^a)^b * R^{c+1} \equiv R^{S+1}$.

Otherwise, $c+1 = a$. If $a < b$, then $c+1 < b$ and similar reasoning to that of the last paragraph implies the result. So assume $b \leq a$. Now R, S , and R^S are z -SON, for some $z > 0$ (since 1 exists).

Suppose $b = z$. Then $a = z$.

Consider the case where $z = 1$. Then $a = b = 1$ and $c = 0$, so $S \equiv 10$. Also, $R \geq 10$ since $R > 1$. But then $R^S \geq 10 * 10$, which is not a 1-SON, a contradiction.

Consider the case where $z = 2$. Then $a = b = 2$ and $c = 1$, so $R^S \equiv (R^2)^2 * R$. $R \geq 2$ since $R > 1$. Thus $R^S \geq (2^2)^2 * 2$, which is not a 2-SON, a contradiction.

Thus $\hat{z} > 2$. An easy induction shows, since $R > 1$, that $R^{z-1} > \langle z \rangle$, so that $len(R^{z-1}) \geq 1$. *A fortiori*, $len(R^z) \geq 1$. By *Prop 5.18* and an easy induction, $len((R^z)^z) \geq z$. But $c = z - 1$, so by *Prop 5.18* again, $len((R^z)^z * R^{z-1}) \geq z + 1$, contradicting $(R^a)^b * R^c$ being a z -SON.

All this goes to show that $b < z$. Then $S + 1 \equiv \langle a \rangle * \langle b \rangle + \langle c+1 \rangle \equiv \langle a \rangle * \langle b \rangle + \langle a \rangle \equiv \langle a \rangle * \langle b+1 \rangle$, the latter existing since $b+1 \leq z$. So $R^S * R \equiv (R^a)^b * R^c * R \equiv (R^a)^b * R^a \equiv (R^a)^{b+1} \equiv R^{S+1}$.

d,e,f. Proceed by SON Induction (*Theorem 3.8*) and use (c). □

7. Division.

Def 7.1. $R \mid S$ abbreviates $\exists T (R * T \equiv S)$. □

Equivalence respects division. That is, suppose $R \mid S$. Then if $R \equiv T$, $T \mid S$. And if $T \equiv S$, $R \mid T$.

The following proposition lists many properties of division. Their proofs may be found in *Arithmetic without the Successor Axiom*, as the version for SONs does not change noticeably from that for natural numbers.

Prop 7.2.

a. $\forall R (\text{SON}(R) \Rightarrow R \mid 0)$

b. $\forall R (\text{SON}(R) \Rightarrow R \mid R)$

c. $\forall n \forall R (n\text{-SON}(R) \ \& \ n > 0 \Rightarrow 1 \mid R)$

d. $\forall R (0 \mid R \Rightarrow R = 0)$

e. $\forall R \forall S (R \mid S \ \& \ \neg S \equiv 0 \Rightarrow R \leq S)$

f. (Anti-Symmetry) $\forall R \forall S (R \mid S \ \& \ S \mid R \Rightarrow R \equiv S)$

g. (Transitivity) $\forall R \forall S \forall T (R \mid S \ \& \ S \mid T \Rightarrow R \mid T)$

h. $\forall R \forall S \forall T \forall A \forall B \forall C (R \mid S \ \& \ R \mid T \ \& \ A * S + B * T \equiv C \Rightarrow R \mid C)$

i. $\forall R \forall S \forall T \forall A \forall B \forall C (R \mid S \ \& \ R \mid T \ \& \ A * S - B * T \equiv C \Rightarrow R \mid C)$

j. $\forall R \forall S (R \mid S \ \text{and} \ S * T \text{ exists} \Rightarrow R * T \mid S * T)$ □

The greatest common divisor of two SONs exists and is unique up to equivalence:

Prop 7.3. (Existence and Uniqueness of a Greatest Common Divisor). Suppose A, B are SONs, where either $\neg A \equiv 0$ or $\neg B \equiv 0$. Then, there exists some D such that,

$$D \mid A \ \& \ D \mid B \ \& \ \forall C (C \mid A \ \& \ C \mid B \Rightarrow C \leq D).$$

If $D' \mid A \ \& \ D' \mid B \ \& \ \forall C (C \mid A \ \& \ C \mid B \Rightarrow C \leq D')$, then $D' \equiv D$. □

The previous proposition justifies the following definition:

Def 7.4. Suppose A, B are SONs, where either $\neg A \equiv 0$ or $\neg B \equiv 0$. Use $A \Delta B$ to refer to that unique (up to equivalence) D guaranteed to exist by the previous proposition. \square

As usual equivalence respects Δ .

Prop 7.5.

a. $\forall A \forall B (\text{SON}(A) \ \& \ \text{SON}(B) \ \& \ (\neg A \equiv 0 \vee \neg B \equiv 0) \Rightarrow A \Delta B \equiv B \Delta A)$

b. $\forall A \forall B \neg A \Delta B \equiv 0$

c. $\forall A \forall B (\text{SON}(A) \ \& \ \text{SON}(B) \ \& \ (\neg A \equiv 0 \vee \neg B \equiv 0) \Rightarrow A \Delta B \mid A)$

d. $\forall A \forall B (\text{SON}(A) \ \& \ \text{SON}(B) \ \& \ (\neg A \equiv 0 \vee \neg B \equiv 0) \Rightarrow A \Delta B \leq A)$

e. $\forall A \forall B (\neg A \equiv 0 \ \& \ A \mid B \Rightarrow A \Delta B \equiv A)$

f. $\forall X \forall Y \forall Z \forall A \forall B ((\neg X \equiv 0 \vee \neg Y \equiv 0) \ \& \ A * X + B * Y \equiv Z \Rightarrow X \Delta Y \mid Z)$

g. $\forall X \forall Y \forall Z \forall A \forall B ((\neg X \equiv 0 \vee \neg Y \equiv 0) \ \& \ A * X - B * Y \equiv Z \Rightarrow X \Delta Y \mid Z)$

h. $\forall Q \forall R \forall A \forall B (\neg B \equiv 0 \ \& \ A \equiv Q * B + R \Rightarrow A \Delta B \equiv B \Delta R)$

i. $\forall A (A > 0 \Rightarrow A \Delta 0 \equiv A)$

j. $\forall A (\text{SON}(A) \ \& \ \text{SON}(I) \Rightarrow A \Delta I \equiv I)$

k. $\forall A \forall B \forall C (C \mid A \ \& \ C \mid B \ \& \ (\neg A \equiv 0 \vee \neg B \equiv 0) \Rightarrow C \mid A \Delta B)$

l. $\forall X \forall Y \forall A \forall B (A * (X \Delta Y) \equiv X \ \& \ B * (X \Delta Y) \equiv Y \Rightarrow A \Delta B \equiv I)$ \square

8. Prime Numbers and Unique Prime Factorization

Def 8.1. Let $R > 1$. Then R is *prime* and write $\pi(R)$ if and only if $\forall S (S \mid R \Rightarrow S \equiv R \vee S \equiv I)$. \square

The proofs of the following assertions are like those for the first-order case. (See *Prop 6.20* in *Arithmetic without the Successor Axiom*.)

Prop 8.2.

- a. $\forall R (R > 1 \Rightarrow \exists S (\pi(S) \& S \mid R))$
b. $\forall R \forall S (\pi(R) \& \text{SON}(S) \Rightarrow (R \Delta S) \equiv 1 \vee (R \Delta S) \equiv R)$
c. $\forall R \forall S (\pi(R) \& R \mid (R \Delta S) \Rightarrow R \mid S)$
d. $\forall R \forall S (\text{SON}(R) \& \text{SON}(S) \& (\neg R \equiv 0 \vee \neg S \equiv 0) \& \forall P (\pi(P) \& P \mid R \Rightarrow \neg P \mid S) \Rightarrow (R \Delta S) \equiv 1)$ \square

Theorem 8.3 (Prime Factorization, Existence) Let $z > 0$ and R a z -SON with $R > 1$. Then $\exists n \exists m \exists B \exists C \exists k \exists j$ such that all of the following hold:

- $\text{SeqOfSeq}(B, n)$
- $\text{SeqOfSeq}(C, m)$
- $\text{Seq}(k, n)$
- $\text{Seq}(s, m)$
- $B_0 \equiv 1$
- $s_0 = 1$
- $\pi(B_i)$ for all $i, 0 < i \leq n$
- $\pi(\langle s_i \rangle)$ for all $i, 0 < i \leq m$
- $B_i < B_{i+1}$ for all $i, 0 \leq i < n$
- $s_i < s_{i+1}$ for all $i, 0 \leq i < m$
- $\text{len}(B_i) \geq 1$ for all $i, 0 < i \leq n$
- $n \leq \text{len}(R)$

$$R \equiv \prod_{i=0}^n B_i^{k_i} * \prod_{i=0}^m \langle s_i \rangle^{C_i}$$

Remark: There are two products of sequences, in order most easily to ensure that the length of the sequences is $\leq z$.

Pf:

Let $R > 1$ be the least number for which the assertion does not hold.

Suppose R is prime. If $\text{len}(R) \geq 1$, then set $n = 1, m = 0, B_0 \equiv 1, B_1 \equiv R, k_0 = 1, k_1 = 1, s_0 = 1$, and $C_0 \equiv 1$. And if $\text{len}(R) = 0$, then $R = \langle r \rangle$ for some r , so set $n = 0, m = 1, B_0 \equiv 1, s_0 = 1, s_1 = r, k_0 = 1, C_0 \equiv 1$, and $C_1 = 1$. But then there is a contradiction in either case.

So it may supposed that R is not prime.

By Prop 8.2(a), $R \equiv S * T$ for some S, T where $\pi(S)$. Then $S > 1$ by Def 8.1, so $T < R$ by Prop 5.12(c). Hence there exist n, m, B, C, k, s such that

$$T \equiv \prod_{i=0}^n B_i^{k_i} * \prod_{i=0}^m \langle s_i \rangle^{C_i}$$

and the conditions stated in the theorem hold. In particular, $n \leq \text{len}(T)$.

Suppose $\text{len}(S) \geq 1$. By Prop 5.18, $\text{len}(T) \leq \text{len}(R) - 1$. By Prop 5.18 again, $k_i \leq \text{len}(T)$ for all $i \leq n$, and so $k_i + 1$ exists. Thus, if $S \equiv B_i$ for some i , R may be factorized like T above, except with $k_i + 1$ as the exponent of B_i instead of k_i , by the usual properties of the first-order exponential. On the other hand, if $\neg S \equiv B_i$ for any i , then $n \leq \text{len}(T) \leq \text{len}(R) - 1$, so $n+1$

exists, and then R may be factorized like T above, except $n+1$ replaces n , the B sequence is redefined to include S in the proper place, and the k sequence is redefined to include 1 in the same position as S in the B sequence.

Similar reasoning applies should $len(S) = 0$, only that the s and C sequences are adjusted. Remark that since there are only z numbers with 0 length > 0 , forcibly $m \leq z$. \square

The proof of *Uniqueness of Prime Factorization* relies on the following proposition, which is stated here but proved later:

Prop 8.4. If $\pi(P) \ \& \ P \mid (X * Y)$, then $P \mid X$ or $P \mid Y$. \square

The proof of this lemma is exactly the same as the one for first-order numbers (see *Arithmetic without the Successor Axiom*, Section 7D). Nonetheless, because it is a bit convoluted, it is copied in full and put here.

Lemma 8.5. If $K \mid (X * Y) \ \& \ (K \Delta Y) \equiv 1 \ \& \ (K * X)$ exists, then $K \mid X$.

Note: It will be shown later that the condition that $(K * X)$ exists, can be eliminated.

Pf:

Suppose to the contrary that the assertion is not true. By the *Well-Ordering Principle* (*Prop 2.8(a)*), there exists a least Y such that for some X, K

$$K \mid (X * Y) \ \& \ (K \Delta Y) \equiv 1 \ \& \ (K * X) \text{ exists} \ \& \ \neg K \mid X.$$

If $Y \equiv 0$, then $K \equiv 1$ by *Prop 7.5(a)*, contradicting *Prop 7.2(c)*.

So $\neg Y \equiv 0$. By the *Division Algorithm* (*Prop 5.2(a)*), there exist Q, R such that:

$$K \equiv Q * Y + R \ \& \ R < Y.$$

By *Prop 7.5(h)*, $(K \Delta Y) \equiv (K \Delta R)$. Thus $(K \Delta R) \equiv 1$.

By assumption, $X * K$ exists, so by the *Distributive Law* (*Prop 5.10*),

$$X * K \equiv X * Q * Y + X * R.$$

Now $K \mid (X * K)$ by *Def 7.1*, and $K \mid (X * Q * Y)$ by *Transitivity of \mid* (*Prop 7.2(g)*). So

$$K \mid (X * R),$$

by *Prop 7.2(i)*. But then by the assumption of the leastness of Y , $K \mid X$, a contradiction.

Thus the assertion is true. \square

Prop 8.6. Assume $\pi(R) \ \& \ R \mid (X * Y)$. And suppose that either $(R * X)$ or $(R * Y)$ exists. Then $R \mid X$ or $R \mid Y$.

Pf:

WLOG by symmetry, suppose $(R * X)$ exists. By *Prop 8.2(b)*, $(R \Delta Y) \equiv 1$ or

$(R \Delta Y) \equiv R$. If $(R \Delta Y) \equiv R$, then by *Props 7.5(c)*, $R \mid Y$. Otherwise, suppose $(R \Delta Y) \equiv I$. By *Lemma 8.5*, $R \mid X$. □

Pf of Prop 8.4:

Let $\pi(P) \& P \mid (X * Y)$.

If $X \equiv 0$, then $P \mid X$ by *Prop 7.2*.

Otherwise, assume $\neg X \equiv 0$.

If $P \leq X$, then $P * Y \leq X * Y$ by *Prop 5.12(a)*, so $(P * Y)$ exists. Then by *Prop 8.6*, the result follows.

So assume $P > X$. By the *Division Algorithm (Prop 5.20)*,

$$P \equiv Q * X + R \ \& \ R < X$$

for some Q, R . By *Prop 7.5(h)*, $(P \Delta X) \equiv (X \Delta R)$. If $\neg (P \Delta X) \equiv I$, then $(P \Delta X) \equiv P$ by *Prop 8.2(b)*. So $P \mid X$, by *Def 7.4*.

So assume $(P \Delta X) \equiv I$. Hence $(X \Delta R) \equiv I$. Now $P \mid (X * Y)$, so $P * A \equiv X * Y$ for some A . In particular $(P * A)$ and so $((Q * X + R) * A)$ exists. Thus

$$P * A \equiv Q * X * A + R * A,$$

by the *Distributive Law (Prop 5.10)*. Of course $X \mid (X * Y) \equiv (P * A)$ and $X \mid (Q * X)$. By *Prop 7.2(i)*, $X \mid (R * A)$. Now $(P * A)$ exists and $X \leq P$, so $(X * A)$ exists, by *Prop 5.12(a)*. By *Lemma 8.5*, $X \mid A$. So $X * V \equiv A$ for some V . So

$$P * (X * V) \equiv P * A \equiv X * Y.$$

If $V \equiv 0$, then $A \equiv 0$, and $X * Y \equiv 0$; so $X \equiv 0$ or $Y \equiv 0$, so $P \mid X$ or $P \mid Y$. Otherwise, $\neg V \equiv 0$ and *Associativity of Multiplication* applies. By *Associativity and Cancellation*, $P * V \equiv Y$. Therefore, $P \mid Y$. □

Theorem 8.7 (Prime Factorization, Uniqueness). Let $z > 0$ and R a z -SON with $R > I$. Suppose all of the following hold:

$SeqOfSeq(B, n)$

$SeqOfSeq(C, m)$

$Seq(k, n)$

$Seq(s, m)$

$B_0 \equiv I$

$s_0 = 1$

$\pi(B_i)$ for all $i, 0 < i \leq n$

$\pi(\langle s_i \rangle)$ for all $i, 0 < i \leq m$

$B_i < B_{i+1}$ for all $i, 0 \leq i < n$

$s_i < s_{i+1}$ for all $i, 0 \leq i < m$

$len(B_i) \geq 1$ for all $i, 0 < i \leq n$

$n \leq len(R)$

$$R \equiv \prod_{i=0}^n B_i^{k_i} * \prod_{i=0}^m \langle s_i \rangle^{C_i}$$

and

$$\begin{aligned}
& \text{SeqOfSeq}(D,p) \\
& \text{SeqOfSeq}(E,q) \\
& \text{Seq}(x,p) \\
& \text{Seq}(t,q) \\
& D_0 \equiv 1 \\
& t_0 = 1 \\
& \pi(D_i) \text{ for all } i, 0 < i \leq p \\
& \pi(\langle t_i \rangle) \text{ for all } i, 0 < i \leq q \\
& D_i < D_{i+1} \text{ for all } i, 0 \leq i < p \\
& t_i < t_{i+1} \text{ for all } i, 0 \leq i < q \\
& \text{len}(D_i) \geq 1 \text{ for all } i, 0 < i \leq p \\
& p \leq \text{len}(R) \\
& R \equiv \prod_{i=0}^p D_i^{x_i} * \prod_{i=0}^q \langle t_i \rangle^{E_i}
\end{aligned}$$

Then all of the following hold:

$$\begin{aligned}
n &= p \\
m &= q \\
B &\equiv D \\
C &\equiv E \\
k &\equiv x \\
s &\equiv t
\end{aligned}$$

Pf:

Use *Prop 8.4* and the Well-Ordering Principle. □

Here are some consequences of *Prime Factorization*:

Corollary 8.8. Let $R \mid (X * Y)$ and $(R \Delta Y) \equiv 1$. Then $R \mid X$. □

Corollary 8.9. Let $R > 0$, $X \mid Z$, $Y \mid Z$, and $(X \Delta Y) \equiv 1$. Then $(X * Y) \mid Z$. □

Corollary 8.10. Let $R > 0$, $\text{SeqOfSeq}(X,n)$, $(X_i \Delta X_j) \equiv 1$ for all $i,j \leq n$, and $X_i \mid Z$ for all $i \leq n$.

Then $\prod_{i=0}^n X_i \mid Z$. □

9. Lemmas for the Proof of Bertrand's Postulate

Prop 9.1. Let $n, p \leq z$ & p prime. Let X be the greatest z -SON such that $\langle p \rangle^X \mid n!_z$. Then

$$X \equiv \sum_{j=1}^n \left\langle \frac{n}{p^j} \right\rangle.$$

Remarks: $\left\langle \frac{a}{b} \right\rangle$ takes its normal meaning as the unique number q guaranteed by the Division Algorithm for first-order numbers, i.e. $q * b + r = a$ where $r < b$.

Notice that the sum is a sum of second-order numbers of length 0.

Pf:

An easy proof by induction suffices. □

Prop 9.2. Let $1 \leq k$ & $k + 1 \leq n$ & $n \leq z$. Then, $(n - k)!_z * k!_z \mid n!_z$.

Pf:

The subscript z shall be dropped for the entirety of the proof.

By induction on n . Consider the case $n = 2$. If $k = 1$, then $(n - k)! * k! \equiv 1$, and by *Prop 7.2(c)*, $1 \mid n!$. And if $k = 2$, then $(n - k)! * k! \equiv \langle 2 \rangle \equiv n!$.

Now assume the proposition holds for n , and consider $m = n + 1$. Let $1 \leq k$ & $k + 1 \leq m$ & $m \leq z$. If $m = k + 1$ or $k = 1$, then $(m - k)! * k! \equiv (m - 1)!$, which clearly divides $m!$.

Otherwise, suppose $k + 1 < m$ and $1 < k$. Then $k + 1 \leq n$ and $1 \leq k - 1$. So by the induction hypothesis,

$$\frac{(k - 1)! * (n - k + 1)! \mid n!}{k! * (n - k)! \mid n!} \quad \text{and}$$

Recall that $m!$ exists, since $m \leq z$. Now $k \leq m$ and $n - k + 1 \leq m$, so by *Prop 5.12(a)*, $n! * k$ and $n! * (n - k + 1)$ both exist. By *Prop 7.2(j)*,

$$\frac{(k - 1)! * (n - k + 1)! * k \mid n! * k}{k! * (n - k)! * (n - k + 1) \mid n! * (n - k + 1)} \quad \text{and}$$

That is,

$$\frac{k! * (m - k)! \mid n! * k}{k! * (m - k)! \mid n! * (n - k + 1)} \quad \text{and}$$

Now $m = k + (n - k + 1)$, so $m! \equiv n! * k + n! * (n - k + 1)$. Hence by *Prop 7.2(h)*, $k! * (m - k)! \mid m!$. □

The previous proposition justifies:

Def 9.3. Let $1 \leq k$ & $k + 1 \leq n$ & $n \leq z$. Use $\binom{n}{k}_z$ to refer to the up-to-equivalence unique z -SON T such that $(n - k)!_z * k!_z * T \equiv n!_z$. When it can be understood, the subscript z will be dropped. □

A consideration of the proof of *Prop 9.2* shows that we have in fact proved as well:

Prop 9.4. Let $1 \leq k$ & $k + 1 \leq n \leq z$. Then $\binom{n}{k}_z \equiv \binom{n-1}{k-1}_z + \binom{n-1}{k}_z$. □

Standard inductions prove:

Prop 9.5.

a. Let $2, n \leq z$. Then $\langle 2 \rangle^n \equiv \sum_{k=0}^n \binom{n}{k}_z$.

b. Let $k \leq 2 * n \leq z$. Then $\binom{2 * n}{k}_z \leq \binom{2 * n}{n}_z$ □

Def 9.6. Let $x \leq y \leq z$. Let *SeqOfSeq*(B, z), where z -SON(B_i) for all $i \leq z$ and $B_i \equiv \langle i \rangle$ if $\pi(\langle i \rangle)$ and $x < i \leq y$ and $B_i \equiv 1$ otherwise. Then set $\theta_z(x, y)$ to $\prod_{i=0}^n B_i$ and $\theta_z(x)$ to $\theta_z(0, x)$. The subscript z will be dropped when it can be understood. □

Remark that $\theta_z(x, y) \leq z!$, so induction with *Prop 5.12(a)* can prove its existence.

Obviously, $\theta_z(x, y)$ is unique up to equivalence for any given x, y, z . Also, if $v \leq x \leq y \leq z$, then $\theta_z(v, y) \equiv \theta_z(v, x) * \theta_z(x, y)$.

Prop 9.7. Let $x \leq z$, and suppose $R = 4$. Then $\theta_z(x) \leq R^x$.

Note: The first-order exponential is being used here.

Pf:

The subscript z will be dropped for the entirety of the proof.

Let $2 = 2$.

If $x = 0$, then $\theta(x) \equiv 1 \leq 1 \equiv R^0$.

If $x = 1$, then $\theta(x) \equiv 1 \leq R \equiv R^1$.

If $x = 2$, then $\theta(x) \equiv 2 \leq R \leq R^2$. (Remark that $R^2 \leq 222$, so it exists.)

If x is even and $x > 2$, then $\theta(x) = \theta(x-1)$, since the only even prime is 2.
 So it suffices to show that if x is odd and $x > 2$ and the assertion holds for all natural numbers less than x , then $\theta(x) \leq R^x$.

So let $x > 2$ be odd. Then there exists $y \geq 1$ such that $2 * y + 1 = x$. So

$$\theta(x) \equiv \theta(y+1) * \theta(y+1, x).$$

By supposition, since $y + 1 < x$,

$$\theta(y+1) \leq R^{y+1}.$$

Suppose p is a prime and $y+1 < p \leq x$. Then $\langle p \rangle \mid x!$ but $\neg \langle p \rangle \mid (y+1)!$ and $\neg \langle p \rangle \mid y!$, by *Prop 8.4*. By another application of *Prop 8.4*, $\langle p \rangle \mid \binom{x}{y}$. So by *Corollary 8.10*,

$\theta(y+1, x) \mid \binom{x}{y}$. By *Prop 7.2(e)*, $\theta(y+1, x) \leq \binom{x}{y}$. But by *Prop 9.4*,

$$\begin{aligned} \binom{x}{y} &\equiv \binom{2 * y}{y-1} + \binom{2 * y}{y} \\ &\leq \sum_{k=0}^{2 * y} \binom{2 * y}{k} \equiv 2^{2 * y} \equiv R^y \quad \text{the first equivalence by Prop 9.5(b).} \end{aligned}$$

So $\theta(y+1, x) \leq R^y$. Hence

$$\theta(x) \leq R^y * R^{y+1} \equiv R^x. \quad \square$$

10. Proof of Bertrand's Postulate

Theorem 10.1. Let $n \geq 4$ be even. Then there exists a prime number p such that $\frac{n}{2} < p < n$.

Pf:

Assume to the contrary that $n \geq 4$ is even and there exists no prime p such that $m < p < n$, where we set $m = \frac{n}{2}$.

Consideration of cases shows that $n \geq 4096$.

Consider n -SONs (n subscripts will be dropped). Let $2 \equiv \langle 2 \rangle$.

By *Prop 9.5(a)*, $\langle 2 \rangle^{2 * m} \equiv \sum_{k=0}^n \binom{n}{k}$. But $\binom{n}{k} \leq \binom{n}{m}$, for all $k \leq n$, by *Prop 9.5(b)*. So

$\langle 4 \rangle^m \leq (\langle n \rangle + 1) * \binom{n}{m}$. Note that this latter exists, since

$$(\langle n \rangle + 1) * \binom{n}{m} \leq (\langle n \rangle + 1) * n! \leq n^n,$$

since $2 * (\langle n \rangle + 1) \leq \langle n \rangle^2$ because $n \geq 3$.

For prime $p \leq n$ and SON Y , define $S(p, Y)$ to be the greatest X such that $\langle p \rangle^X \mid Y$, and set $R(p)$ to be $S(p, \binom{n}{m})$.

Let prime $p \leq n$. By Prop 9.1, $S(p, n!) \equiv \sum_{j=1}^n \left\langle \frac{n}{p^j} \right\rangle$ and

$S(p, m!) \equiv \sum_{j=1}^m \left\langle \frac{m}{p^j} \right\rangle$. Let $c(p) =$ greatest x such that $p^x \leq n$. Then the sums may be taken to

$c(p)$, for beyond $c(p)$ the terms must be 0. That is, $S(p, n!) = \sum_{j=1}^{c(p)} \left\langle \frac{n}{p^j} \right\rangle$ and

$S(p, m!) = \sum_{j=1}^{c(p)} \left\langle \frac{m}{p^j} \right\rangle$.

Now $m! * m! * \binom{n}{m} \equiv n!$, so by the *Existence and Uniqueness of Prime Factorization* (Theorems 8.3 and 8.7),

$$S(p, m!) + S(p, m!) + S(p, \binom{n}{m}) \equiv S(p, n!).$$

So

$$S(p, \binom{n}{m}) \equiv S(p, n!) - 2 * S(p, m!).$$

That is,

$$\begin{aligned} R(p) &\equiv \sum_{j=1}^{c(p)} \left\langle \frac{n}{p^j} \right\rangle - 2 * \sum_{j=1}^{c(p)} \left\langle \frac{m}{p^j} \right\rangle \\ &\equiv \sum_{j=1}^{c(p)} \left(\left\langle \frac{n}{p^j} \right\rangle - 2 * \left\langle \frac{m}{p^j} \right\rangle \right). \end{aligned}$$

But $n = 2 * m$, so $\left\langle \frac{n}{p^j} \right\rangle - 2 * \left\langle \frac{m}{p^j} \right\rangle = 0$ or 1 , for all j where $1 \leq j \leq c(p)$. Thus $R(p) \leq \langle c(p) \rangle$,

and so $\langle p \rangle^{R(p)} \leq \langle n \rangle$.

Now let p be prime, with $p \leq m$ and $\langle n \rangle < \langle 3 \rangle * \langle p \rangle$. Then $\langle n \rangle^2 < \langle 9 \rangle * \langle p \rangle^2$. But $\langle n \rangle^2 > \langle 9 \rangle * \langle n \rangle$ since $n \geq 4096 \geq 10$. So $\langle p \rangle^2 > \langle n \rangle$. But then $c(p) \leq 1$, so

$$R(p) \equiv \sum_{j=1}^1 \left\langle \frac{n}{p^j} \right\rangle - 2 * \sum_{j=1}^1 \left\langle \frac{m}{p^j} \right\rangle \equiv \left\langle \frac{n}{p} \right\rangle - 2 * \left\langle \frac{m}{p} \right\rangle.$$

But $\langle n \rangle^2 > \langle 9 \rangle * \langle n \rangle$ since $n \geq 10$. Also $2 * p \leq n$. So $\left\lfloor \frac{n}{p} \right\rfloor = 2$ and $\left\lfloor \frac{m}{p} \right\rfloor = 1$, and $R(p) \equiv 0$.

Therefore 0 is the greatest number X such that $\langle p \rangle^X \mid \binom{n}{m}$. In particular this implies that

$$\neg \langle p \rangle \mid \binom{n}{m}.$$

So, if P is a prime with $P \mid \binom{n}{m}$, then $P \leq \langle n \rangle$ by *Props 8.4 and 7.2(e)*. So $P = \langle p \rangle$ for some prime p . $\neg p = n$ since n is even, and $\neg m < p < n$ by assumption. So $p \leq m$. But then the previous paragraph implies that $n \geq 3 * p$.

Let y be the greatest number such that $y * y \leq n$. Then, by the *Existence and Uniqueness of Prime Factorization*, and abusing notation of the product symbol in the normal way to mean that the product is only over primes satisfying the particular condition,

$$\begin{aligned} \binom{n}{m} &\equiv \prod_{p \leq n} \langle p \rangle^{R(p)} \\ &\equiv \prod_{p \leq y} \langle p \rangle^{R(p)} * \prod_{y < p \leq n} \langle p \rangle^{R(p)} \end{aligned}$$

Now

$$\prod_{p \leq y} \langle p \rangle^{R(p)} \leq \prod_{p \leq y} \langle n \rangle \leq \langle n \rangle^y$$

Also

$$\begin{aligned} \prod_{y < p \leq n} \langle p \rangle^{R(p)} &\equiv \prod_{y < p \leq n} \langle p \rangle \text{ since } p > y \\ &\leq \prod_{p \leq z} \langle p \rangle \end{aligned}$$

where $z =$ the greatest natural number such that $3 * z \leq n$. But then

$$\prod_{y < p \leq n} \langle p \rangle^{R(p)} \leq \langle n \rangle^z, \text{ by Prop 9.7.}$$

Thus

$$\langle n \rangle^m \leq (\langle n \rangle + 1) * \binom{n}{m}$$

and so

$$\langle n \rangle^{m-z} \leq (\langle n \rangle + 1) * \langle n \rangle^y \text{ by Corollary 5.13.}$$

Cubing both sides (and noting that both $3 * (m-z) < n$ and $3 * y < n$),

$$\langle 4 \rangle^{3^{*(m-z)}} \leq (\langle n \rangle + 1)^3 * \langle n \rangle^{3^*y}.$$

Now $(\langle n \rangle + 1)^3 \leq \langle n \rangle^y$, so

$$\langle 4 \rangle^{3^{*(m-z)}} \leq \langle n \rangle^y * \langle n \rangle^{3^*y} \text{ by Prop 5.12(a).}$$

Hence, by the normal properties of the first-order exponential (and noting that $4^*y \leq n$),

$$\langle 4 \rangle^{3^{*(m-z)}} \leq \langle n \rangle^{4^*y}.$$

Let t be the least natural number such that $n < \langle 4 \rangle^t$. $t > 6$ since $n > 4096$. Then $y + 1 > 8^*t$, so

$$n > 64^*t^2.$$

Dividing both sides by 2 and multiplying both sides by m (and now having to use second-order numbers since the first-order ones may be too big)

$$\langle m \rangle^2 > \langle 16 \rangle * \langle n \rangle * \langle t \rangle^2.$$

Hence

$$m > 4^*y^*t.$$

Now $3^*z \leq n = 2^*m$, so $m \leq 3^*m - 3^*z = 3^*(m - z)$. Thus

$$3^*(m - z) > 4^*y^*t.$$

And so

$$\langle 4 \rangle^{3^{*(m-z)}} > \langle 4 \rangle^{4^*y^*t}.$$

By choice $n < \langle 4 \rangle^t$, so

$$\langle 4 \rangle^{3^{*(m-z)}} > \langle n \rangle^{4^*y},$$

the desired contradiction. □

9. Conclusion.

In this paper second-order numbers have been restricted to strings of digits. It is possible to extend the definition to include strings of formula, consisting of strings of digits and certain permissible operations. For instance, “ 324^*236 ” and “ $324^{\wedge}236$ ” might be acceptable strings, in the first case with the product operation used, and in the second the exponential operation. The result of sums or products of strings is a string of no greater length - e.g. 324^*236 , a string of length 7 (beginning the count with 1), in base 10 equals 76464, a string of length 5 - and so limiting the operations to sums and products not does extend the universe of expressible numbers. But once the exponential operation is allowed, new numbers may be written, since e.g. $324^{\wedge}236$ equals a number requiring a vastly longer string of digits (in base 10). This new universe brings with it new challenges, such as how to define equality so that it is transitive. Also, gaps exist in these second-order numbers, since, if for instance strings are limited to length 7, $324^{\wedge}236$ exists but does not have an immediate predecessor. Still, with

induction on the length of the string, one has a powerful tool for reasoning about them.

While the largest effective number used here is $(n+1)^{(n+1)} - 1$, it is clearly possible, albeit obviously more complicated, to use two sequences to represent a single number, thereby doubling the length of representable numbers and increasing the effective numbers available. Indeed, there is no reason to stop with two; three or even a hundred sequences could be used. Essentially, one can use as many sequences as are necessary in order to arrive at the largest number one needs for any particular proof.

Still, these are finitary universes, so unlike that of the Successor Axiom, whose ontological assumptions are infinitary. The Successor Axiom is not satisfied with a largest number; it assumes there are always more. It does seem that the Successor Axiom is inessential for number theory, but, given the use of the Successor Axiom in analysis, and the role of analysis in number theory, more needs to be done before this can be confirmed.

Bibliography

Boucher, Andrew. *Proving Quadratic Reciprocity*, 2003. On web site, www.andrewboucher.com/papers.

Boucher, Andrew. *Arithmetic without the Successor Axiom*, 2006. On web site, www.andrewboucher.com/papers.

Wikipedia, en.wikipedia.org/wiki/Bertrand's_postulate