Arithmetic Without the Successor Axiom

by Andrew Boucher

10 February 2006

INTRODUCTION

The *Successor Axiom* asserts that every number has a successor, or in other words, that the number series goes on and on *ad infinitum*. The present work investigates a particular subsystem of Frege Arithmetic, called **F**, which turns out to be equivalent to second-order Peano Arithmetic minus the *Successor Axiom*, and shows how this system can develop arithmetic up through Gauss' *Quadratic Reciprocity Law*. It then goes on to represent questions of provability in **F**, and shows that **F** can prove its own consistency, in the fashion of Godel, and indeed the Godel consistency of stronger systems. So, arithmetic without the *Successor Axiom* has an exceptional combination of three characteristics: it is natural, it is strong, and it proves its own, as well as stronger systems', consistency.

Also exceptional is what **F** lacks - the assumption that the natural numbers go on and on *ad infinitum*. This hypothesis, while central to most mathematicians' view of their subject, is nonetheless apparently of a different character than the other axioms, which have a more logical or analytic character to them. For instance, the axiom that *P* numbers 0 if and only if *P* is empty seems to follow directly from the meaning of the words used; it is analytic. In contrast the *ad infinitum* assumption is ontological. Unlike the other axioms, it makes a statement that certain things, indeed many, many things, exist. Where, might one ask, *are* all of them and how does one know that they are there? It would seem justification can only come from some inner intuition and the imagination of adding one continually forever and ever. But it would seem our imaginations are not so clear that they can distinguish between the adding of one *ad infinitum* and adding one to a very large number. Perhaps our inner intuition is really only of the latter.

It might seem that even though the number series *does* not go on *ad infinitum*, it *might* do so. It is, one might assert, *logically possible* that it could go on and on. While apparently a weaker claim, it has the same problem of evidence. For it would seem that the only way that its logical possibility could be known is the same sort of appeal to inner intuition. But the imagining of *might* would seem to be as problematic as the imagining of *is*. So it is no more clear that the number series *could* go on *ad infinitum* than that it *does*.

Reluctance to embrace the *Successor Axiom* does not compel the acceptance of the contrary assertion, that there is a maximum number. For it would seem that there is no evidence for this position either - no one, for instance, can present a maximum number. One can perhaps imagine the numbers stopping or fading away, but there is no reason to suppose that *our* numbers stop or fade away.

So **F** assumes neither the *Successor Axiom* nor its contrary. Either assumption - the continuance of the number series *ad infinitum* or the existence of a maximum number - is not one the author would care to make, because both go beyond what he can confidently assert. He is therefore *agnostic* about the matter. **F** assumes only the existence of 0 - and it could forego even that.

Agnosticism might seem too constraining a philosophy to do any meaningful mathematics, but, as we shall see, the system **F** is capable of proving many theorems. Indeed, it is hard to see what the assumption of a maximum integer would add to the system were it included; what useful proposition could thereby be deduced which could not already be deduced without it. Its assertion would only confuse matters by making it seem it is needed in places where it is not. So even from a practical standpoint, agnosticism is a better approach than the atheistic assumption there is a maximum integer.

Belief in the infinite, whether of an infinite divine being or a number series which goes on and on, would seem to be a matter of faith. It can be accepted, its justification will be and has been often attempted, but at the end of the day, it remains a matter of faith. Still, the religious and mystical impulse should never be underestimated.

F may be described as ontologically *downward*. If a number n is assumed to exist, then all numbers less than n can be proved to exist. On the other hand, it is not possible to infer the existence of any number greater than n. **F** has as models the standard model - if, that is, one believes there *is* a standard model - as well as all initial segments, which is in harmony with our agnostic philosophy.

F is unable to prove the *Commutative Law of Addition* when it is expressed thusly:

$$\forall x \forall y(x + y = y + x).$$

For this asserts, given x and y, that $x + y$ and $y + x$ exist and are equal. But the existence claim cannot be inferred. On the other hand, **F** can prove this version of *Commutativity*:

$$\forall x \forall y \forall z(x + y = z \Rightarrow y + x = z).$$

For it is now assumed that $x + y$ exists; and given this, it can be proven that $y + x$ exists and indeed equals $x + y$.

F cannot prove that there are an infinity of prime numbers. Indeed this sentence is not true in most initial segments. For example, {0,1,2,3,4,5} has 3 prime numbers, and since 3 is one of the natural numbers in the segment, the set of prime numbers is finite in this model. Still, **F** can prove that, if n and $n! + 1$ are natural numbers, then there is a prime number between the two, which is the essential content behind the assertion that there are an infinity of primes. So, even when **F** may not be able to prove certain theorems as usually stated, it can often prove restated versions which maintain the essential core of the original.

Most sub-systems of Peano Arithmetic have focused on weakening induction. Indeed perhaps the most famous sub-system, Robinson's **Q**, lacks an induction axiom altogether. It is very weak in many respects, unable for instance to prove the *Commutative Law of Addition* (in any version). Indeed, it is sometimes taken to be the weakest viable system; if a proposition can be proved in **Q**, then that is supposed to pretty much establish that all but Berkleyan skeptics or fools are compelled to accept it.

But weakness of systems is not a linear order, and **F** is neither stronger nor weaker than **Q**. **F** has induction, indeed full induction, which **Q** does not. But **F** is ontologically much weaker than **Q**, since **Q** supposes the *Successor Axiom*. **Q** assumes the natural numbers, *all* of them, *ad infinitum*. So in terms of strength, **F** and **Q** are incomparable. In actual practice, **F** seems to generate more results of standard arithmetic; and so in that sense only, is it "stronger".

One of the most important practitioners of **Q** has been Edward Nelson of Princeton, who has developed a considerable body of arithmetic in **Q** . While Nelson's misgivings with classical mathematics seemed to have their source in doubts about the existence of the natural numbers, the brunt of his skepticism falls on induction, hence his adoption of **Q**. "The induction principle assumes that the natural number series is given." [p. 1, *Predicative Arithmetic*] Yet it would seem that induction is neither here nor there when it comes to ontological supposition. Induction states conditions for when something holds of all the natural numbers, and says nothing about how many or what numbers there are. So a skeptic about the natural numbers should put, so to speak, his money where his doubts are, and reject the assumption which is generating all those numbers - namely the *Successor Axiom* - and leave induction, which those doubts impact at worst secondarily, alone.

A number of arithmetic systems, capable of proving their own consistency, have become known over the years. Jeroslow [*Consistency Statements*] had an example, which was a certain fixed point extension of **Q** $\vee$ $\forall x \forall y(x = y)$. More recently, Yvon Gauthier [*Internal Logic* and

Internal Consistency] used indefinite descent and introduced a special, called "effinite", quantifier. And Dan Willard [*Self-Verifying Axiom Systems*] has exhibited several cases, based on seven "grounding" functions. These systems lack a certain naturalness and seem to be constructed for the express purpose of proving their own consistency. Finally, Panu Raatikainen constructed what is effectively a first-order, weaker variant of **F**; this system can prove that it has a model [*Truth in a Finite Universe*], but its weakness does not allow the author to draw conclusions about intensional correctness and so it seems to fall short of the ability to prove its own self-consistency.

A distinction needs to be made between *Godel* consistency and *real* consistency. Godel consistency is expressed in terms of Godel numbers to represent wffs and proofs, while real consistency, as far as possible, avoids Godel numbering and resorts to sequences which may be taken really to represent wffs and proofs, which are after all syntactical sequences. Real consistency is a stronger notion than Godel consistency, and while **F** can prove its own Godel consistency, the author is unable to prove that **F** can prove its own real consistency. (Versions of this treatise prior to Dec 2010 asserted such a proof, but this made a crucial, albeit simple, error.) Nonetheless, a sister version to **F**, which has effectively the same proof-theoretic strength towards arithmetic, *can* prove its real (and so Godel) consistency and so **F**'s shortcoming in this respect, if considered important, can be rectified simply by changing the system.

As remarked above, **F** is a sub-system of Frege Arithmetic. Frege Arithmetic is second-order logic, with the additional axiom of *Hume's Principle*

$$\forall P \forall Q \; (\#P = \#Q \Leftrightarrow P \sim Q).$$

It is possible to prove the Peano Axioms in Frege Arithmetic, a fact which can be found in Frege himself [*Grundgesetze*], and which was brought to modern attention by Charles Parsons [*Frege's Theory*] and Crispin Wright [*Frege's Conception*]. George Boolos [*Logic*] had a role in developing and popularizing the theory. His student, Richard Heck, showed [*Cardinality*] that a finite version of *Hume's Principle* could be proved from a suitable system, a technique which is mirrored by the one here. Frege Arithmetic normally uses an axiom for successoring

$$\forall n \forall m \; (\sigma n{,}m \Leftrightarrow \exists P \exists a \; (\neg \, Pa \;\&\; \#P = n \;\&\; \#(P \cup \{a\}) = m \;) \;),$$

which while suitable for a development of arithmetic when *Hume's Principle* is assumed as well, is less suitable in the context of **F**. The axiom which **F** uses (called F3) is similar to one which Neil Tennant stated in an earlier system in his *Anti-Realism and Logic*.

The present work brings together material from four papers of the author - *Systems for a Foundation of Arithmetic*, *"True" Arithmetic Can Prove its Own Consistency*, *Proving Quadratic Reciprocity*, and *The Equivalence of **F** With a Sub-Theory of Peano Arithmetic* - which were written from 2001 through 2005. The objective is an improvement in exposition, in order to render the subject more accessible and clearer to the interested reader.

The author would like to thank contributors to sci.logic for many fruitful discussions and especially Torkel Franzen, who suggested the writing of this work, and Mike Oliver, whose skepticism towards infinity caused the author to think more deeply about the subject.

Table of Contents

A. List of Basic Symbols and Terms Used

The left-side abbreviates the right-side:

$x \in P$	Px
$P \equiv Q$	$\forall x\,(Px \Leftrightarrow Qx)$ or $\forall x \forall y\,(Px,y \Leftrightarrow Qx,y)$
$P \subseteq Q$	$\forall x\,(Px \Rightarrow Qx)$
$P \subset Q$	$\forall x\,(Px \Rightarrow Qx)\ \&\ \neg\, P \equiv Q$
$P \cup Q$	$\{z : Pz \vee Qz\}$ or $\{y,z : Py,z \vee \mathrm{Qy,z}\}$
$P \setminus Q$	$\{z : Pz\ \&\ \neg\, Qz\}$ or $\{y,z : Py,z\ \&\ \neg\, Qy,z\}$
$R \lceil A$	$\{y,z : Ry,z\ \&\ Ay\}$
$(R \circ S)$	$\{x,z : \exists y\,(Rx,y\ \&\ Sy,z)\}$
ϕ	$\{z : \neg\, z = z\}$ or $\{y,z : \neg\, z = z\}$
$\mathbb{U}$	$\{z : z = z\}$
$\{a\}$	$\{z : z = a\}$
$\{a,b\}$	$\{z : z = a \vee z = b\}$
$\{(a,b)\}$	$\{y,z : y = a\ \&\ z = b\}$
$\{(a,b,\mathrm{c})\}$	$\{x,y,z : x = a\ \&\ y = b\ \&\ z = c\}$
$\mathit{Dom}(R)$	$\{x : \exists y\ Rx,y\}$
$\mathit{Im}(R)$	$\{y : \exists x\ Rx,y\}$
$\mathit{IsFunction}(R)$	$\forall x \forall y \forall z\,(Rx,y\ \&\ Rx,z \Rightarrow y = z)$
$\mathit{Is1\text{-}1}(R)$	$\forall x \forall y \forall z\,(Rx,y\ \&\ Rz,y \Rightarrow x = z)$
$P \sim Q$	$\exists R\,(P \equiv \mathit{Dom}(R)\ \&\ Q \equiv \mathit{Im}(R)\ \&\ \mathit{IsFunction}(R)\ \&\ \mathit{Is1\text{-}1}(R))$

1. The Systems F and FPA and Some Preliminary Results

Second-order logic, considered as a deductive system, is essentially two-typed first-order logic, the types being distinguished by case. Lower-case letters may be thought to represent individuals and are called *first-order*, while upper-case letters symbolize predicates, properties, or sets, and are called *second-order*.

Along with the usual axioms and rules of inference of first-order logic with equality, second-order logic has a *Comprehension Axiom*, or more properly *Schema*:

Let ϕ be any formula not containing any free "*P*", and let $n \geq 1$. Then

$$\exists P\ \forall x_1 ... \forall x_n\ (\ P x_1,...,x_n\ \Leftrightarrow \phi\ ).$$

P, which is unique up to equivalence, will be written as $\{x_1,...,x_n : \phi\}$.

When there is no restriction on ϕ, comprehension is *full*, and the resulting second-order logic is also called *full*. *Arithmetic* or *Predicative Comprehension* restricts ϕ to wffs with no quantified upper-case variables, and the resulting logic is called *predicative*. Throughout only predicative comprehension will be used.

Second-order Peano Arithmetic has one first-order constant *0* ("zero"), and two second-order constants, σ (the successor relationship) and *N* (the set of natural numbers). Its axioms are:

(PA1) N0
(PA2) $\forall n \forall m$ (Nn & $\sigma n,m \Rightarrow$ Nm)
(PA3) $\forall n$ (N$n \Rightarrow \exists m\ \sigma n,m$)
(PA4) $\forall n \forall m \forall m'$ (Nn & $\sigma n,m$ & $\sigma n,m' \Rightarrow m = m'$)
(PA5) $\forall n \forall m \forall n'$ (Nn & Nn' & $\sigma n,m$ & $\sigma n',m \Rightarrow n = n'$)
(PA6) $\forall n$ (N$n \Rightarrow \neg\ \sigma n,0$)
(PA7) Induction schema. Let ϕ be a well-formed formula. Suppose $\phi[0\backslash n]$ and $\forall n \forall m$ *(* Nn *&* $\sigma n,m$ & $\phi \Rightarrow \phi[m\backslash n]$). Then $\forall n$ (N$n \Rightarrow \phi$).

Here $\phi[x\backslash y]$ refers to the formula ϕ, with *x* replacing all free instances of *y*.

Remark that these axioms could have been stated without the use of N, in which case the domain of quantification would be understood as the set of natural numbers, rather than everything. In such an environment both (PA1) and (PA2) would be redundant and so would be suppressed.

The conjunction of (PA2) and (PA3) will be called the *Successor Axiom*. (PA3) says that every natural number has a successor. (PA2) ensures that this successor is also a natural number, which thus in turn by (PA3) has a successor. If the axioms had been stated without the use of N and so if (PA2) had been suppressed, then (PA3) would have been, by itself, the *Successor Axiom*.

Abbreviate Second-order Peano Arithmetic by **PA2**. Abbreviate the subsystem consisting of (PA4), (PA5), (PA6), and (PA7) by **FPA**.

Now introduce into the language one more constant, M. M has two arguments, the first being first-order and the second being second-order, e.g. Mx,*P*. It can be taken to say, "the size of *P* is *x*." Consider the axioms:

(F1) $\forall n\forall m\forall P\ (\ \mathrm{M}n,P\ \&\ \mathrm{M}m,P \Rightarrow n = m\ )$
(F2) $\forall P\ (\ \mathrm{M}0,P \Leftrightarrow \neg\, \exists x\, Px\ )$
(F3) $\forall n\forall m\forall P\forall Q\forall a\ (\ \mathrm{N}n\ \&\ \sigma n,m\ \&\ \neg Pa\ \&\ Q \equiv\ (P \cup \{a\})$
$\Rightarrow (\mathrm{M}n,P \Leftrightarrow \mathrm{M}m,Q)\ )$
(F4) Induction schema. Let ϕ be a well-formed formula. Suppose $\phi[0\backslash n]$ and
$\forall n\forall m\ (\ \mathrm{N}n\ \&\ \sigma n,m\ \&\ \phi \Rightarrow \phi[m\backslash n]\ )$. Then $\forall n\ (\ \mathrm{N}n \Rightarrow \phi\ )$.
(F5) N0
(F6) $\forall n\forall P\forall a\ (\ \mathrm{N}n\ \&\ \mathrm{M}n,P\ \&\ \neg\ Pa \Rightarrow \exists m\ (\mathrm{N}m\ \&\ \mathrm{M}m,(P \cup \{a\}))\ )$

Call the system with these axioms ***FF***. (F6) is the *Ad Infinitum Axiom* and it plays the same role for **FF** as the *Successor Axiom* does for **PA2**. Accordingly, let **F** be the system with the axioms (F1), (F2), (F3), and (F4).

FF is a cousin of Frege Arithmetic, which shares the same language as **PA2**, except that in addition it has a second-order function, #. '*#*(*P*)', which can be read as "the size of *P*," plays the same role as M in **F** and **FF**, except that, because it is a function, it makes implicit two assumptions: first, that each *P* has at most one size; and secondly, that each *P* does have a size. The **F** and **FF** systems make the first assumption explicitly, with (F1). **F** foregoes the second, while **FF** in (F6) makes a weaker ontological claim.

It will be shown that (1) **F** and **FPA** and (2) **FF** and **PA2** are equivalent systems. **PA2** being obviously well understood, the efforts of this monograph will almost exclusively be to investigate the first pair of systems, which are less, even much less, known. One special feature of both **F** and **FPA**, which makes them worthy of attention, is that they have as models not only the standard one, but also all initial segments of the standard model. The last claim will be substantiated later, but it is enough to notice now that both **F** and **FPA** have as a model the domain with only one first-order element, 0, where 0 has no successor.

The rest of the chapter will be devoted to comments pertaining to all four systems, **F**, **FF**, **FPA**, and **PA2**.

First, remark that the Induction Schema can be replaced by a stronger Schema:

(F4*) Let ϕ be a well-formed formula. Suppose $\mathrm{N}0 \Rightarrow \phi[0\backslash n]$
and $\forall n\forall m\ (\ \mathrm{N}n\ \&\ \mathrm{N}m\ \&\ \neg\ m = 0\ \&\ \sigma n,m\ \&\ \phi \Rightarrow \phi[m\backslash n]\ )$.
Then $\forall n\ (\ \mathrm{N}n \Rightarrow \phi\ )$.

For each instance of (F4*) can be deduced from an instance of (F4) using ($\mathrm{N}n \Rightarrow \phi[0\backslash n]$) as its ϕ.

The axiom "N0" is not assumed in the subsystems **F** and **FPA** because it is rarely needed, so it is simply better to append it when the need arises. Its near-vacuity follows from the fact that the existence of any natural number implies that 0 is a natural number:

Prop 1.1. $\forall n\ (\ \mathrm{N}n \Rightarrow \mathrm{N}0\ )$
Pf:

Use (F4*), with ϕ as N0. □

Prop 1.2. $\forall n\ (\ \mathrm{N}n\ \&\ \neg\ n = 0 \Rightarrow \exists k\ (\mathrm{N}k\ \&\ \sigma k,n)\ )$, i.e. every non-zero natural number is preceded by a natural number.

Pf:

By induction, with ϕ as

$$(\neg\, n = 0 \Rightarrow \exists k\, (\mathrm{N}k \,\&\, \sigma k{,}n)\,). \qquad \square$$

Prop 1.2 brings to mind a slight generalization of the natural numbers, appropriate for the systems **F** and **FPA**.

Def 1.3. A *generalized natural number* is either 0 or preceded by a natural number. That is, Γx if and only if

$$x = 0 \vee \exists k\, (\mathrm{N}k \,\&\, \sigma k{,}x) \qquad \square$$

It follows immediately from the definition and *Prop 1.2* that:

Corollary 1.4. $\forall n\, (\, \mathrm{N}n \Rightarrow \Gamma n)$. □

Def 1.5. $one(u)$ if and only if $\mathrm{N}u \,\&\, \sigma 0{,}u$. □

Prop 1.6. $\forall n \forall k\, (\, \mathrm{N}n \,\&\, \mathrm{N}k \,\&\, \sigma n{,}k \Rightarrow \exists u\; one(u)\,)$, i.e. if at least one natural number has a natural number as a successor, then 0 has a successor which is a natural number.

Pf:

By induction, with ϕ as

$$\forall k\, (\, \mathrm{N}n \,\&\, \mathrm{N}k \,\&\, \sigma n{,}k \Rightarrow \exists u\, (\mathrm{N}u \,\&\, \sigma 0{,}u)\,). \qquad \square$$

Def 1.7.

$x \leq y$ if and only if $\mathrm{N}x \,\&\, \mathrm{N}y \,\&\, \exists P \exists Q\, (P \subseteq Q \,\&\, \mathrm{M}x{,}P \,\&\, \mathrm{M}y{,}Q)$

$x < y$ if and only if $x \leq y \,\&\, \neg\, x = y$ □

The manner of treating the ontological implication of terms in this work may be new to the reader and so merits some remarks. The assertion of an atomic wff with a term is held to assert that the term refers successfully, or speaking loosely that the term exists. The assertion of the negative of an atomic wff with a term or terms makes one of two assertions: that one of the terms does not refer successfully - speaking loosely, that the term does not exist - or that the terms all exist but just do not satisfy the predicate of the wff. So for instance, if one assumes that $\mathrm{M}(x + y){,}P$, then one can infer that $(x + y)$ exists. And if one assumes that $\neg\, \mathrm{M}(x + y){,}P$ for some *P*, then either $(x + y)$ does not exist, or it does exist but it is simply not such that it is the size of *P*.

Generally speaking one must be careful with definitions which create new symbols and predicates which look atomic, e.g. ≤ in *Def 1.7*. It would be possible to define predicates which contain a negation - e.g. define *Rx* to mean ¬ M*x*,*P* - , in which case one would have to decide whether such predicates filled with a term which does not exist, are true or not. That is, there are two possible conventions: (1) treat the new symbol as a new predicate and follow the rule that a positive assertion of the symbol with a term pre-supposes that the term exists; or (2) demand that the new symbol be unpacked in terms of its definition, and *then* apply the rule that a term in an atomic wff implies the existence of the term. Fortunately, none of the definitions in this work are such that conventions (1) and (2) result in different conclusions, so it is not necessary to choose between them.

Terms may be defined with pre-suppositions. For instance, the greatest common divisor of *x* and *y* is defined in the case when *x* and *y* are natural numbers and not both are 0. When one asserts an atomic wff containing the greatest common divisor term, one can therefore conclude that *x* and *y* are natural numbers and not both 0.

2. Equivalence of the Systems I

The principal object of this chapter is to show that **F** proves the axioms of **FPA**, and that **FF** proves those of **PA2**. In passing a few other assertions will be deduced from **F**.

For simplicity's sake, the axioms of **F** will be assumed for the entire chapter.

2A. Finite Hume's Principle and the Pigeon Hole Principle.

Prop 2.1. $\forall P \forall n$ ($\mathrm{M}n,P$ & $\neg\, n = 0 \Rightarrow \exists x\, Px$)
Pf:

Assume $\mathrm{M}n,P$. Suppose $\neg\, \exists x\, Px$. Then $\mathrm{M}0,P$ by (F2). So by (F1), $n = 0$. □

Prop 2.2. $\forall P \forall Q$ ($\mathrm{M}0,P \Rightarrow (P \sim Q \Leftrightarrow \mathrm{M}0,Q)$)
Pf:

Assume $\mathrm{M}0,P$. By (F2), $\neg\, \exists x\, Px$. Suppose $P \sim Q$. Then evidently $\neg\, \exists x\, Qx$. By (F2), $\mathrm{M}0,Q$. On the other hand, suppose $\mathrm{M}0,Q$. Then by (F2) $\neg\, \exists x\, Qx$. So $P \sim Q$. □

Prop 2.3. (*Finite Hume's Principle*) $\forall n \forall P \forall Q$ ($\mathrm{N}n$ & $\mathrm{M}n,P \Rightarrow (P \sim Q \Leftrightarrow \mathrm{M}n,Q)$).
Pf:

By induction, (F4*), with ϕ as

$$\forall P \forall Q \ (\mathrm{M}n,P \Rightarrow (P \sim Q \Leftrightarrow \mathrm{M}n,Q)).$$

Prop 2.2 proves the case for $n = 0$. Assume $\mathrm{N}n$ & $\mathrm{N}m$ & $\sigma n,m$ & $\neg\, m = 0$ & $\forall P \forall Q$ ($\mathrm{M}n,P \Rightarrow (P \sim Q \Leftrightarrow \mathrm{M}n,Q)$). And suppose $\mathrm{M}m,P$. By *Prop 2.1*, Pa for some a. Consider $P' = P \setminus \{a\}$. By (F3), $\mathrm{M}n,P'$.

Suppose $P \sim Q$. Let R be a one-to-one function from P onto Q. Then Ra,b for some b such that Qb. Set Q' equal to $Q \setminus \{b\}$. Evidently, $R \setminus \{(a,b)\}$ is a one-to-one function from P' onto Q', so $P' \sim Q'$. By the induction hypothesis, $\mathrm{M}n,Q'$. By (F3), $\mathrm{M}m,Q$.

Now suppose $\mathrm{M}m,Q$. Since $\neg\, m = 0$, Qb for some b, by *Prop 2.1*. Consider $Q' = Q \setminus \{b\}$. By (F3), $\mathrm{M}n,Q'$. By the induction hypothesis, $P' \sim Q'$. Let R' be a one-to-one function from P' onto Q'. Then $R' \cup \{(a,b)\}$ is a one-to-one function from P onto Q. So $P \sim Q$. □

Corollary 2.4 $\forall n \forall P \forall Q$ ($\mathrm{N}n$ & $\mathrm{M}n,P$ & $P \equiv Q \Rightarrow \mathrm{M}n,Q$) □

Note that *Corollary 2.4* could have been proved by logic alone if there had been an equality relationship between second-order things and extensionality

$$\forall P \forall Q \, (\, P \equiv Q \Rightarrow P = Q \,)$$

had been assumed.

It will be useful later to have a slightly stronger version of *Finite Hume's Principle*.

Corollary 2.5. $\forall x \forall P \forall Q \, (\, \Gamma x \,\&\, \mathrm{M}x,P \Rightarrow (P \sim Q \Leftrightarrow \mathrm{M}x,Q) \,)$
Pf:

If $x = 0$ then the result follows by *Prop 2.2*. So it suffices to prove

$$\forall x \forall P \forall Q \, (\, \Gamma x \,\&\, \neg\, x = 0 \,\&\, \mathrm{M}x,P \Rightarrow (P \sim Q \Leftrightarrow \mathrm{M}x,Q) \,),$$

i.e.

$$\forall x \forall k \forall P \forall Q \, (\, \mathrm{N}k \,\&\, \sigma k,x \,\&\, \neg\, x = 0 \,\&\, \mathrm{M}x,P \Rightarrow (P \sim Q \Leftrightarrow \mathrm{M}x,Q) \,).$$

So let $\mathrm{N}k \,\&\, \sigma k,x \,\&\, \neg\, x = 0 \,\&\, \mathrm{M}x,P$. By *Prop 2.1*, Pa, for some a.

Suppose $P \sim Q$. Then Qb, for some b. So $P \setminus \{a\} \sim Q \setminus \{b\}$. By (F3), $\mathrm{M}k,(P \setminus \{a\})$. By *Prop 2.4*, $\mathrm{M}k,(Q \setminus \{b\})$. By (F3) again $\mathrm{M}x,Q$.

Suppose $\mathrm{M}x,Q$. By *Prop 2.1* again, Qb, for some b. By (F3) $\mathrm{M}k,(P \setminus \{a\})$ and $\mathrm{M}k,(Q \setminus \{b\})$. By *Prop 2.4* $P \setminus \{a\} \sim Q \setminus \{b\}$, and thus $P \sim Q$. □

Prop 2.6. (*Pigeon Hole Principle*) $\forall n \forall P \forall Q \, (\, \mathrm{N}n \,\&\, \mathrm{M}n,P \,\&\, \mathrm{M}n,Q \,\&\, P \subseteq Q \Rightarrow P \equiv Q \,)$
Pf:

By induction (F4*), with ϕ as

$$\forall P \forall Q \, (\, \mathrm{N}n \,\&\, \mathrm{M}n,P \,\&\, \mathrm{M}n,Q \,\&\, P \subseteq Q \Rightarrow P \equiv Q \,).$$

Obvious for n = 0, using (F2).

Assume then that $\mathrm{N}n \,\&\, \mathrm{N}m \,\&\, \sigma n,m \,\&\, \neg\, m = 0 \,\&\, \phi$, and suppose $\mathrm{M}m,P \,\&\, \mathrm{M}m,Q \,\&\, P \subseteq Q$. By *Prop 2.1*, Px for some x. Set P' to $P \setminus \{x\}$ and Q' to $Q \setminus \{x\}$. By (F3), $\mathrm{M}n,P' \,\&\, \mathrm{M}n,Q'$. Clearly $P' \subseteq Q'$, so by the induction hypothesis, $P' \equiv Q'$. Hence $P \equiv Q$. □

Corollary 2.7. Suppose $\mathrm{N}n \,\&\, \mathrm{M}n,P \,\&\, \mathrm{M}n,Q$. If $\neg\, P \equiv \mathbb{U}$, then $\neg\, Q \equiv \mathbb{U}$.
Pf:

Suppose $\neg\, P \equiv \mathbb{U}$ but $Q \equiv \mathbb{U}$. $P \equiv Q$ follows immediately from *Prop 2.6*, but this is a contradiction. □

2B. F + *POTINF* proves FPA.

Def 2.8. POTINF_n abbreviates

$$\exists P \exists a\ (\mathrm{M}n,P \ \&\ \neg\, Pa).$$

POTINF abbreviates

$$\forall n\ (\ \mathrm{N}n \Rightarrow POTINF_n\ ).$$ □

POTINF asserts that there are n things and one more thing, for every natural number n. It is therefore asserting a kind of potential infinity. It plays an important intermediate role in the objective of this chapter. It will be shown below that *POTINF* (along with the axioms of **F**, which remember are being assumed) implies the axioms of **FPA**. Later, in Section 2D, it will be shown that **F** proves *POTINF*.

Prop 2.9. *POTINF* ⇒ (PA4) & (PA5).
Pf:

Assume *POTINF*.

Let Nn & Nn' & $\sigma n,m$ & $\sigma n',m'$.

Suppose $n = n'$. By *POTINF* and (F3), Mn,P & $\neg\, Pa$ & M$m,(P \cup \{a\})$ & M$m',(P \cup \{a\})$ for some P,a. Now apply (F1).

Suppose $m = m'$. By *POTINF* and (F3), Mn,P & $\neg\, Pa$ & M$m,(P \cup \{a\})$ & Mn',P' & $\neg\, P'a'$ & M$m,(P' \cup \{a'\})$ for some P,P',a,a'. Γm, so by *Corollary 2.5*, $(P \cup \{a\}) \sim (P' \cup \{a'\})$. Hence evidently $P \sim P'$. By *Prop 2.3*, Mn,P'. By (F1), $n = n'$. □

Prop 2.10. *POTINF* ⇒ (PA6).
Pf:

Assume *POTINF*.

Let Nn & $\sigma n,0$. Then by *POTINF* Mn,P & $\neg\, Pa$. Applying (F3), M$0,(P \cup \{a\})$, contradicting (F2). □

Since (PA7) is just (F4), **F** + *POTINF* proves the axioms of **FPA**.

2C. FF + *POTINF* proves PA2 and PA3.

Prop 2.11. *POTINF* + (F6) ⇒ (PA2).
Pf:

Assume *POTINF* and (F6).

Let Nn & $\sigma n,m$. By *POTINF*, Mn,P & $\neg\, Pa$ for some P,a. By (F3), M$m,(P \cup \{a\})$. By (F6), Nm' & Mm',(P ∪ {a}) for some m'. By (F1), $m = m'$. □

Lemma 2.12. $\forall n \forall m \forall P \forall a$ ($\mathrm{N}n$ & $\mathrm{N}m$ & $\mathrm{M}n,P$ & $\mathrm{M}m,(P \cup \{a\})$ & $\neg\, Pa \Rightarrow \sigma n,m$).
Pf:

Assume $\mathrm{N}n$ & $\mathrm{N}m$ & $\mathrm{M}n,P$ & $\mathrm{M}m,(P \cup \{a\})$ & $\neg\, Pa$. By (F2), $\neg\, m = 0$, so by *Prop 1.2*, $\mathrm{N}k$ & $\sigma k,m$ for some k. By (F3), $\mathrm{M}k,P$. By (F1), $n = k$. □

Prop 2.13. *POTINF* + (F6) $\Rightarrow$ (PA3).
Pf:

Assume *POTINF* and (F6).
Let $\mathrm{N}n$. By *POTINF*, $\mathrm{M}n,P$ & $\neg\, Pa$ for some P,a. By (F6), $\mathrm{N}m$ & $\mathrm{M}m,(\mathrm{P} \cup \{\mathrm{a}\})$ for some m. By *Lemma 2.12*, $\sigma n,m$. □

Since (PA1) is just (F5), **FF** + *POTINF* proves the axioms of **PA2**.

2D. F proves *POTINF*.

In the previous two sections, it has been shown that **F** + *POTINF* implies the axioms of **FPA**, and **FF** + *POTINF* implies the axioms of **PA2**. In order to show that **F** $\Rightarrow$ **FPA** and **FF** $\Rightarrow$ **PA2**, it therefore suffices to show that **F** proves *POTINF*.

POTINF asserts that, for every natural number n, there exists a P of size n such that something a is not P. In the proof below, the set of numbers less than n will be used as P, and a will be the number n itself, which, since it is not less than itself, does not belong to P.

Recall that "$x \le y$" abbreviates:

$$\mathrm{N}x \;\&\; \mathrm{N}y \;\&\; \exists P \exists Q\, (P \subseteq Q \;\&\; \mathrm{M}x,P \;\&\; \mathrm{M}y,Q)$$

As usual, use $x < y$ to abbreviate ($\neg\, x = y$ & $x \le y$).

The next proposition groups some elementary assertions about $\le$ and $<$:

Prop 2.14.

a. If $\mathrm{N}n$ & $\mathrm{M}n,P$, then $0 \le n$ and $n \le n$.

b. If $\exists x\, \mathrm{N}x$, then both $0 \le 0$ and $\forall z\, ((0 \le z \;\&\; z \le 0) \Leftrightarrow z = 0)$.

c. Let $n < m$. Then $\mathrm{N}n$ & $\mathrm{N}m$ & $\exists P \exists Q\, (P \subset Q \;\&\; \mathrm{M}n,P \;\&\; \mathrm{M}m,Q)$.

d. Assume $\mathrm{N}n$ & $\sigma n,m$. If $k < m$, then $k \le n$.

Note: Once *POTINF* is proved, then *a*. can be restated as: if $\mathrm{N}n$, then $0 \le n$ and $n \le n$.

Pf:

a. Suppose $\mathrm{N}n \ \& \ \mathrm{M}n,P$. By (F2), $\mathrm{M}0,\phi$. By *Prop 1.1,* N0. Thus $\mathrm{N}0 \ \& \ \mathrm{N}n \ \& \ \phi \subseteq P \ \& \ \mathrm{M}0,\phi \ \& \ \mathrm{M}n,P$. So $0 \leq n$, by *Def 1.7*. Also, $\mathrm{N}n \ \& \ \mathrm{N}n \ \& \ P \subseteq P \ \& \ \mathrm{M}n,P \ \& \ \mathrm{M}n,P$. So $n \leq n$, again by *Def 1.7*.

b. Assume $\exists x \ \mathrm{N}x$. By *Prop 1.1*, N0. Of course $\mathrm{M}0,\phi$ by (F2). So by (*a*), $0 \leq 0$. Now suppose $0 \leq z \ \& \ z \leq 0$. By the second inequality and *Def 1.7*, $\mathrm{N}z \ \& \ \mathrm{N}0 \ \&$ $\exists P \exists Q \ (P \subseteq Q \ \& \ \mathrm{M}z,P \ \& \ \mathrm{M}0,Q)$. By (F2), $Q \equiv \phi$. Hence $P \equiv \phi$, so by *Prop 2.1,* $z = 0$.

c. $n \leq m$, so $\mathrm{N}n \ \& \ \mathrm{N}m \ \& \ P \subseteq Q \ \& \ \mathrm{M}n,P \ \& \ \mathrm{M}m,Q$, for some P and Q, by *Def 1.7*. Suppose $P \equiv Q$. By *Corollary 2.4*, $\mathrm{M}m,P$. By (F1), $n = m$, contradicting the definition of $n < m$.

d. Let $k < m$. By (*c*), $\mathrm{N}k \ \& \ \mathrm{N}m \ \& \ P \subset Q \ \& \ \mathrm{M}k,P \ \& \ \mathrm{M}m,Q$, for some P and Q. Then $\exists a \ (Qa \ \& \ \neg \ Pa)$. By (F3), $\mathrm{M}n,(Q \setminus \{a\})$. Evidently, $P \subseteq Q \setminus \{a\}$. So $k \leq n$, by *Def 1.7*. □

Prop 2.15. Assume $\mathrm{N}n \ \& \ \mathrm{N}m \ \& \ \sigma n,m \ \& \ \neg \ m = 0 \ \& \ \mathit{POTINF}_m$. Then POTINF_n.

Pf:

$\mathrm{M}m,P$ for some P, since POTINF_m. By *Prop 2.1*, Pa for some a. Then by (F3), $\mathrm{M}n,(P \setminus \{a\})$. Evidently, $\neg \ (P \setminus \{a\})a$. Hence POTINF_n. □

Prop 2.16. Assume $\mathrm{N}m \ \& \ \sigma n,m \ \& \ \mathit{POTINF}_n$.

a. If $k \leq n$, then $k < m$.

b. $\neg \ m \leq n$.

Pf:

a. Let $k \leq n$. Then $\mathrm{N}k \ \& \ \mathrm{N}n \ \& \ P \subseteq Q \ \& \ \mathrm{M}k,P \ \& \ \mathrm{M}n,Q$, for some P and Q, by *Def 1.7*. By POTINF_n, there are Q' and a' such that $\neg \ Q'a' \ \& \ \mathrm{M}n,Q'$. So $Q \sim Q'$ by *Prop 2.3*. Evidently $\neg \ Q' \equiv \mathbb{U}$, and thus by *Corollary 2.7*, $\neg \ Q \equiv \mathbb{U}$. Hence $\neg \ Qa$ for some a. By (F3), $\mathrm{M}m,(Q \cup \{a\})$. Of course $P \subseteq (Q \cup \{a\})$, so $k \leq m$. If $k = m$, then $P \equiv (Q \cup \{a\})$ by *Prop 2.6*, which contradicts $P \subseteq Q \ \& \ \neg \ Qa$.

b. If $m \leq n$, then by (*a*) $m < m$, a contradiction. □

Prop 2.17. Assume $\mathrm{N}n \ \& \ \mathrm{N}m \ \& \ \sigma n,m \ \& \ \mathit{POTINF}_n$. Then:

a. $\forall z \ ((0 \leq z \ \& \ z \leq m) \Leftrightarrow (0 \leq z \ \& \ z \leq n) \vee z = m)$.

b. $\neg \ (0 \leq m \ \& \ m \leq n)$.

Pf:

a. Suppose $0 \leq z \ \& \ z \leq m$. By *Prop 2.14d*, either $z = m$ or $z \leq n$.

Now suppose $0 \le z \,\&\, z \le n$. By *Prop 2.16a*, $z < m$ so $z \le m$.

Finally, suppose $z = m$. By $POTINF_n$ and (F3), $\mathrm{M}m,Q$ for some Q. By *Prop 2.14a*, $m \le m$.

b. A direct consequence of *Prop 2.16b*.

□

Prop 2.18. $\mathrm{N}n \,\&\, POTINF_n \;\Rightarrow \exists P \forall z\,(\,0 \le z \,\&\, z \le n \Leftrightarrow Pz\,)$

Pf:

Proceed by induction, (F4*), with ϕ as

$$(\,POTINF_n \Rightarrow \exists P\, \forall z\,(0 \le z \,\&\, z \le n \Leftrightarrow Pz)\,).$$

Suppose N0 & $POTINF_0$. By *Prop2.14b*, for any z,

$$0 \le z \,\&\, z \le n \Leftrightarrow z = 0 \Leftrightarrow z \in \{x : x = 0\}.$$

Now assume $\mathrm{N}n \,\&\, \mathrm{N}m \,\&\, \sigma n,m \,\&\, \neg\, m = 0 \,\&\, \phi$. And suppose $POTINF_m$. By *Prop 2.15*, $POTINF_n$, so by the induction hypothesis, for some P,

$$\forall z\,(\,0 \le z \,\&\, z \le n \Leftrightarrow Pz\,)).$$

By *Prop2.17a*, for all z,

$$(0 \le z \,\&\, z \le m) \Leftrightarrow ((0 \le z \,\&\, z \le n) \vee z = m) \Leftrightarrow z \in \{x : Px \vee x = m\}.$$ □

Def 2.19. Suppose $\mathrm{N}n \,\&\, POTINF_n$. *{0 _ n}* will represent a predicate *P* (clearly unique up to equivalence) promised by *Prop 2.18*. □

Prop 2.17 can now be restated to say:

Corollary 2.20. Assume $\mathrm{N}n \,\&\, \mathrm{N}m \,\&\, \sigma n,m \,\&\, POTINF_n \,\&\, POTINF_m$. Then $\{0 \_ m\} \equiv \{0 \_ n\} \cup \{m\}$, where in fact $\neg\, m \in \{0 \_ n\}$. □

Prop 2.21. Let Nn. If $POTINF_n$, then:

$$\forall k \in \{0 \_ n\}\; \forall P\,(\,\{0 \_ n\} \subseteq P \Rightarrow \neg\, \mathrm{M}k,P\,).$$

Pf:

By induction, (F4*) with ϕ as

$$\mathit{POTINF}_n \Rightarrow \forall k \in \{0 \_ n\}\ \forall P\ (\ \{0 \_ n\} \subseteq P \Rightarrow \neg\, \mathrm{M}k,P\ ).$$

Suppose N0 & POTINF_0 , and let $k \in \{0 \_ 0\}$. Then by *Prop 2.14b*, $k = 0$. If $\{0 \_ 0\} \subseteq P$, then P0, and so by (F2), $\neg\, \mathrm{M}0,P$.

Now assume Nn & Nm & $\sigma n,m$ & $\neg\, m = 0$ & ϕ . Suppose POTINF_m , and let $p \in \{0 \_ m\}$ and $\{0 \_ m\} \subseteq P$. It suffices to show that $\neg\, \mathrm{M}p,P$.

By *Prop 2.15*, POTINF_n , and so by the induction hypothesis,

$$\forall k \in \{0 \_ n\}\ \forall P\ (\ \{0 \_ n\} \subseteq P \Rightarrow \neg\, \mathrm{M}k,P\ ).\ \ (*)$$

By *Corollary 2.20*, $\{0 \_ m\} \equiv \{0 \_ n\} \cup \{m\}$, but $\neg\, m \in \{0 \_ n\}$. Then either $p \in \{0 \_ n\}$ or $p = m$.

Suppose $p = m$. By *Prop 2.14a*, $m \in \{0 \_ m\} \subseteq P$, so Pm. By (F3), $\mathrm{M}n,(P \setminus \{m\})$. Evidently, $\{0 \_ n\} \subseteq P \setminus \{m\}$. By *Prop 2.14a* again, $n \in \{0 \_ n\}$. But then by (*), $\neg\, \mathrm{M}n,(P \setminus \{m\})$, a contradiction.

Hence $p \in \{0 \_ n\}$. Clearly $\{0 \_ n\} \subseteq \{0 \_ m\} \subseteq P$. So by (*) $\neg\, \mathrm{M}p,P$. □

Corollary 2.22. $\forall n\ (\ \mathrm{N}n\ \&\ \mathit{POTINF}_n \Rightarrow \forall k \in \{0 \_ n\}\ \neg\, \mathrm{M}k,\{0 \_ n\}\ )$.

Prop 2.23. $\forall n \forall p\ (\ \mathrm{N}n\ \&\ \sigma n,p\ \&\ \mathit{POTINF}_n \Rightarrow \mathrm{M}p,\{0 \_ n\}\ )$.

Pf:

Proceed by induction, (F4*), with ϕ as

$$\forall p\ (\ \sigma n,p\ \&\ \mathit{POTINF}_n \Rightarrow \mathrm{M}p,\{0 \_ n\}\ ).$$

Suppose N0 & $\sigma 0,p$ & POTINF_0. By *Prop 2.14b*, $\{0 \_ 0\} \equiv \{0\}$. By (F2) and (F3), $\mathrm{M}p,\{0\}$.

Now assume Nn & Nm & $\sigma n,m$ & $\neg\, m = 0$ & ϕ . And suppose $\sigma m,p$ & POTINF_m . By *Prop 2.15*, POTINF_n . By the induction hypothesis, $\mathrm{M}m,\{0 \_ n\}$. By *Corollary 2.20*, $\{0 \_ m\} \equiv \{0 \_ n\} \cup \{m\}$, but $\neg\, m \in \{0 \_ n\}$. So by (F3), $\mathrm{M}p,\{0 \_ m\}$. □

Theorem 2.24. (*POTINF*). $\forall n\ (\ \mathrm{N}n \Rightarrow \mathit{POTINF}_n\ )$.

Pf:

Proceed by induction, (F4), with ϕ as POTINF_n .

POTINF_0 , since $\mathrm{M}0,\phi$ and $\neg\, 0 \in \phi$.

Suppose Nn & $\sigma n,m$ & POTINF_n . By *Prop 2.23*, $\mathrm{M}m,\{0 \_ n\}$. By *Corollary 2.22*, $\forall k \in \{0 \_ n\}\ \neg\, \mathrm{M}k,\{0 \_ n\}$. So $\neg\, m \in \{0 \_ n\}$. Thus POTINF_m . □

Corollary 2.25. (PA4) & (PA5) & (PA6) □

3. Equivalence of the Systems II

It was shown in the last chapter that **F** and **FF** prove the axioms of **FPA** and **PA2**, respectively. In this chapter the effective converse will be shown. Of course, **F** contains a predicate (M) which is not even part of **FPA**'s language, and so strictly **FPA** is not able to prove any assertions containing this symbol. However, a natural definition of "M" in the language of **FPA** will be provided so that the axioms of **F** and **FF** can be proven, respectively, in **FPA** and **PA2**.

For the rest of the chapter assume the axioms of **FPA**. To emphasize this point, propositions will be preceded with "(**FPA**)". Indeed, the reader can verify that until the definition of "<<", no appeal is made to (PA6), and the only axioms used are (PA4), (PA5), and (PA7).

(**FPA**) *Prop 3.1*. $\forall n$ (Nn & $\neg\, n = 0 \Rightarrow \neg\, \sigma n,n$)
Pf:

By induction (F4*), with ϕ as ($\neg\, n = 0 \Rightarrow \neg\, \sigma n,n$).

Vacuously, ($\neg\, 0 = 0 \Rightarrow \neg\, \sigma 0,0$).

Now assume Nn & Nm & $\neg\, m = 0$ & $\sigma n,m$ & ($\neg\, n = 0 \Rightarrow \neg\, \sigma n,n$) . Suppose to the contrary $\sigma m,m$. Then by (PA5), $m = n$. So $\neg\, n = 0$, so $\neg\, \sigma n,n$, so $\neg\, \sigma m,m$, a contradiction. Hence $\neg\, \sigma m,m$. □

(**FPA**) *Corollary 3.2*. $\forall k$ (Nk & $\sigma k,k \Rightarrow \forall n$ (N$n \Rightarrow n = 0$)).
Pf:

Suppose Nk & $\sigma k,k$. By *Prop 3.1* $k = 0$, so $\sigma 0,0$. Proceed by induction, with ϕ as $n = 0$.

Obviously $0 = 0$.

Now assume Nn & $\sigma n,m$ & $n = 0$. By *Prop 1.1* N0. Then by (PA4) $m = 0$. □

Following John Burgess (*Fixing Frege*) following Dedekind, define:

Def 3.3. ++(a,b,c) if and only if Na & Nb & Nc &

$\exists R$ ($Ra,0,a$ & Ra,b,c &
$\forall v$ ($Ra,0,v \Rightarrow a = v$) &
$\forall u \forall u' \forall w$ (Nu & $\sigma u,u'$ & $Ra,u',w \Rightarrow \exists v$ (Nv & Ra,u,v)) &
$\forall u \forall u' \forall v \forall w$ (Nu & $\sigma u,u'$ & Ra,u,v & $Ra,u',w \Rightarrow \sigma v,w$)) □

'++' is used instead of '+' in order to reserve the latter for a later use, when addition will be defined in the context of the **F** axioms and language.

(**FPA**) *Prop 3.4*. Suppose $\mathrm{N}n \;\&\; \sigma n{,}m \;\&\; {+}{+}(a{,}m{,}b)$. Then there exists v s.t. $\sigma v{,}b \;\&\; {+}{+}(a{,}n{,}v)$.
Pf:

${+}{+}(a{,}m{,}b)$, so

$\mathrm{N}a \;\&\; \mathrm{N}m \;\&\; \mathrm{N}b \;\&\; Ra{,}0{,}a \;\&\; Ra{,}m{,}b \;\&$
$\forall v\,(Ra{,}0{,}v \Rightarrow a = v) \;\&$
$\forall u \forall u' \forall w\,(\mathrm{N}u \;\&\; \sigma u{,}u' \;\&\; Ra{,}u'{,}w \;\Rightarrow \exists v\,(\mathrm{N}v \;\&\; Ra{,}u{,}v)) \;\&$
$\forall u \forall u' \forall v \forall w\,(\mathrm{N}u \;\&\; \sigma u{,}u' \;\&\; Ra{,}u{,}v \;\&\; Ra{,}u'{,}w \;\Rightarrow \sigma v{,}w)$,

for some R. Then $\mathrm{N}n \;\&\; \sigma n{,}m \;\&\; Ra{,}m{,}b$ and so $\mathrm{N}v \;\&\; Ra{,}n{,}v$, for some v. Hence ${+}{+}(a{,}n{,}v)$. Also, $\mathrm{N}n \;\&\; \sigma n{,}m \;\&\; Ra{,}n{,}v \;\&\; Ra{,}m{,}b$, so $\sigma v{,}b$. □

(**FPA**) *Prop 3.5*. $\forall a \forall c\,({+}{+}(a{,}0{,}c) \Rightarrow a = c)$
Pf:

Suppose ${+}{+}(a{,}0{,}c)$. Then $Ra{,}0{,}a \;\&\; \mathrm{R}a{,}0{,}c \;\&\; \forall v\,(Ra{,}0{,}v \Rightarrow a = v))$, for some R. But then $a = c$. □

(**FPA**) *Prop 3.6*. $\forall n \forall c\,({+}{+}(0{,}n{,}c) \Rightarrow n = c)$
Pf:

By induction, with ϕ as

$\forall c\,({+}{+}(0{,}n{,}c) \Rightarrow n = c)$.

Then ϕ holds when $n = 0$, by *Prop 3.5*.

Now assume $\mathrm{N}n \;\&\; \sigma n{,}m \;\&\; \phi$, i.e. $\forall c\,({+}{+}(0{,}n{,}c) \Rightarrow n = c)$. And suppose ${+}{+}(0{,}m{,}c)$. By *Prop 3.4* there exists v s.t. $\sigma v{,}c \;\&\; {+}{+}(0{,}n{,}v)$. By the induction hypothesis, $n = v$. By (PA4) $m = c$. □

(**FPA**) *Prop 3.7*. $\forall a\,(\mathrm{N}a \Rightarrow {+}{+}(0{,}a{,}a))$
Pf:

Let $\mathrm{N}a$. Note that N0 by *Prop 1.1*.
Set $R = \{x{,}y{,}z : \mathrm{N}y \;\&\; x = 0 \;\&\; y = z\}$. Then $R0{,}0{,}0 \;\&\; R0{,}a{,}a \;\&\; \forall v\,(R0{,}0{,}v \Rightarrow v = 0)$.
Suppose $\mathrm{N}u \;\&\; \sigma u{,}u' \;\&\; Ra{,}u'{,}w$. Then $a = 0 \;\&\; u' = w$. So $Ra{,}u{,}u$.
Suppose $\mathrm{N}u \;\&\; \sigma u{,}u' \;\&\; Ra{,}u{,}v \;\&\; Ra{,}u'{,}w$. Then $u = v$ and $u' = w$, so $\sigma v{,}w$.
Thus ${+}{+}(0{,}a{,}a)$. □

(**FPA**) *Prop 3.8*. $\forall a\,(\mathrm{N}a \Rightarrow {+}{+}(a{,}0{,}a))$
Pf:

Proceed by induction (F4*), with ϕ as ${+}{+}(n{,}0{,}n)$.
The case where $n = 0$ follows from *Prop 3.7*.
Now assume $\mathrm{N}n \;\&\; \mathrm{N}m \;\&\; \neg\, m = 0 \;\&\; \sigma n{,}m \;\&\; \phi$. Hence ${+}{+}(n{,}0{,}n)$, so

$\mathrm{N}0 \;\&\; Rn{,}0{,}n \;\&\; Rn{,}0{,}n \;\&$
$\forall v\,(Ra{,}0{,}v \Rightarrow a = v) \;\&$

$$\forall u\forall u'\forall w\ (\mathrm{N}u\ \&\ \sigma u,u'\ \&\ Ra,u',w\ \Rightarrow \exists v\ (\mathrm{N}v\ \&\ Ra,u,v))\ \&$$
$$\forall u\forall u'\forall v\forall w\ (\mathrm{N}u\ \&\ \sigma u,u'\ \&\ Ra,u,v\ \&\ Ra,u',w\ \Rightarrow \sigma v,w),$$

for some R. Define

$$S = \{x,y,z : \mathrm{N}z\ \&\ x = m\ \&\ \exists c\ (\mathrm{N}c\ \&\ \sigma c,z\ \&\ Rn,y,c)\}.$$

Now $\mathrm{N}n\ \&\ \sigma n,m\ \&\ Rn,0,n$, so $Sm,0,m$.

Suppose $Sa,0,v$. Then $a = m$ and $\mathrm{N}c\ \&\ \sigma c,v\ \&\ Rn,0,c$, for some c. But then $n = c$, so $\sigma n,v$. By (PA4) $m = v$, so $a = v$.

Suppose $\mathrm{N}u\ \&\ \sigma u,u'\ \&\ Sa,u',w$. Then $a = m$ and $\mathrm{N}c\ \&\ \sigma c,w\ \&\ Rn,u',c$, for some c. So $\mathrm{N}v\ \&\ Rn,u,v$, for some v. Thus $\sigma v,c$. So $\mathrm{N}v\ \&\ \sigma v,c\ \&\ \mathrm{R}n,u,v$. Thus Sm,u,c, so Sa,u,c.

Suppose $\mathrm{N}u\ \&\ \sigma u,u'\ \&\ Sa,u,v\ \&\ Sa,u',w$. Then $\mathrm{N}c\ \&\ \sigma c,v\ \&\ Rn,u,c$ and $\mathrm{N}d\ \&\ \sigma d,w\ \&\ Rn,u',d$, for some c,d. Thus $\sigma c,d$. By (PA4) $v = d$. And thus $\sigma v,w$.

Therefore $++(m,0,m)$. □

(**FPA**) *Prop 3.9*. Let $++(a,n,b)\ \&\ ++(a,n,c)$. Then $b = c$.
Pf:

By induction, with ϕ as

$$\forall a\forall b\forall c\ (++(a,n,b)\ \&\ ++(a,n,c) \Rightarrow b = c).$$

Suppose $++(a,0,b)\ \&\ ++(a,0,c)$. Then by *Prop 3.5*, $a = b$ and $a = c$. So $b = c$.

Now assume $\mathrm{N}n\ \&\ \sigma n,m\ \&\ \phi$. And suppose $++(a,m,b)\ \&\ ++(a,m,c)$. Then there exists v,u s.t. $\sigma v,b\ \&\ ++(a,n,v)$ and $\sigma u,c\ \&\ ++(a,n,u)$. By the induction hypothesis $u = v$. By (PA4) $b = c$. □

(**FPA**) *Prop 3.10*. Let $++(a,n,c)\ \&\ ++(b,n,c)$. Then $a = b$.
Pf:

By induction, with ϕ as

$$\forall a\forall b\forall c\ (++(a,n,c)\ \&\ ++(b,n,c) \Rightarrow a = b).$$

Suppose $++(a,0,c)\ \&\ ++(b,0,c)$. Then by *Prop 3.5*, $a = c$ and $b = c$. So $a = b$.

Now assume $\mathrm{N}n\ \&\ \sigma n,m\ \&\ \phi$. And suppose $++(a,m,c)\ \&\ ++(b,m,c)$. Then there exists v,u s.t. $\sigma v,c\ \&\ ++(a,n,v)$ and $\sigma u,c\ \&\ ++(b,n,u)$. By (PA5) $v = u$. By the induction hypothesis $a = b$. □

(**FPA**) *Prop 3.11*. Let $++(a,b',c')\ \&\ \mathrm{N}b\ \&\ \mathrm{N}c\ \&\ \sigma b,b'\ \&\ \ \&\ \sigma c,c'$. Then $++(a,b,c)$.
Pf:

By *Prop 3.4* there exists v s.t. $\sigma v,c'\ \&\ ++(a,b,v)$. By (PA5) $v = c$. □

(**FPA**) *Prop 3.12*. Let $++(a,b,c)\ \&\ \mathrm{N}b'\ \&\ \mathrm{N}c'\ \&\ \sigma b,b'\ \&\ \ \&\ \sigma c,c'$. Then $++(a,b',c')$.
Pf:

Because $++(a,b,c)$

$$\mathrm{N}a \;\&\; \mathrm{N}b \;\&\; \mathrm{N}c \;\&\; Ra,0,a \;\&\; Ra,b,c \;\&$$
$$\forall v\,(Ra,0,v \Rightarrow a = v) \;\&$$
$$\forall u\forall u'\forall w\,(\mathrm{N}u \;\&\; \sigma u,u' \;\&\; Ra,u',w \;\Rightarrow \exists v\,(\mathrm{N}v \;\&\; Ra,u,v)) \;\&$$
$$\forall u\forall u'\forall v\forall w\,(\mathrm{N}u \;\&\; \sigma u,u' \;\&\; Ra,u,v \;\&\; Ra,u',w \;\Rightarrow \sigma v,w),$$

for some R. Define

$$S = R \cup \{(a,b',c')\}$$

Note first that $\mathrm{N}a \;\&\; \mathrm{N}b' \;\&\; \mathrm{N}c'$.

Also that $Sa,0,a$ (because true for R) and Sa,b',c'.

Suppose $Sa,0,v$. If $Ra,0,v$, then $a = v$. Otherwise, $0 = b' \;\&\; v = c'$. Now by *Prop 3.8*, $++(c',0,c')$. So by *Prop 3.4*, $\sigma u,c' \;\&\; ++(c',b,u)$, for some u. By (PA5) $c = u$, so $++(a,b,u)$. By *Prop 3.10* $a = c'$, so $a = v$.

Suppose $\mathrm{N}u \;\&\; \sigma u,u' \;\&\; Sa,u',w$. If Ra,u',w, then $\mathrm{N}v \;\&\; Ra,u,v$, for some v, so Sa,u,v. Otherwise $u' = b' \;\&\; w = c'$. By (PA5) $u = b$. Hence Ra,u,c, so Sa,u,c.

Finally suppose $\mathrm{N}u \;\&\; \sigma u,u' \;\&\; Sa,u,v \;\&\; Sa,u',w$. There are four cases to consider.

If $Ra,u,v \;\&\; Ra,u',w$, then $\sigma v,w$ by the final condition on R.

Otherwise suppose $u = b' \;\&\; v = c' \;\&\; Ra,u',w$. Then $Ra,u,x \;\&\; \sigma x,w$, for some x. Then $Ra,b,y \;\&\; \sigma y,x$, for some y. So $++(a,b,y)$. By *Prop 3.9*, $c = y$. By (PA4) $x = c'$. But then $x = v$, so $\sigma v,w$.

Otherwise suppose $Ra,u,v \;\&\; u' = b' \;\&\; w = c'$. So $++(a,u,v)$. By (PA5), $u = b$. By *Prop 3.9*, $c = v$. Thus $\sigma v,w$.

Otherwise suppose $u = b' \;\&\; v = c' \;\&\; u' = b' \;\&\; w = c'$. By (PA5) $u = b$, so $b = b'$. .Hence $\sigma b,b$. By *Corollary 3.2*, $\forall n\,(\mathrm{N}n \Rightarrow n = 0)$. So $\sigma 0,0$ and $v = 0 = w$, hence $\sigma v,w$. □

(**FPA**) *Prop 3.13*. Let $\mathrm{N}a' \;\&\; \mathrm{N}c' \;\&\; \sigma a,a' \;\&\; \sigma c,c' \;\&\; ++(a,b,c)$. Then $++(a',b,c')$.

Pf:

By induction, with ϕ as

$$\forall a\forall a'\forall c\forall c'\,(\,\mathrm{N}a' \;\&\; \mathrm{N}c' \;\&\; \sigma a,a' \;\&\; \sigma c,c' \;\&\; ++(a,n,c) \Rightarrow ++(a',n,c')\,)$$

Assume $\mathrm{N}a' \;\&\; \mathrm{N}c' \;\&\; \sigma a,a' \;\&\; \sigma c,c' \;\&\; ++(a,0,c)$. Then $a = c$, by *Prop 3.5*. By (PA4) $a' = c'$. By *Prop 3.8* $+(a',0,c')$.

Now assume $\mathrm{N}n \;\&\; \sigma n,m \;\&\; \phi$. Suppose $\mathrm{N}a' \;\&\; \mathrm{N}c' \;\&\; \sigma a,a' \;\&\; \sigma c,c' \;\&\; ++(a,m,c)$. Note by the definition of ++, $\mathrm{N}c \;\&\; \mathrm{N}m$. By *Prop 3.4*, $\sigma v,c \;\&\; ++(a,n,v)$, for some v. By the induction hypothesis $++(a',n,c)$. By *Prop 3.12*, $++(a',m,c')$. □

(**FPA**) *Prop 3.14*. *(Commutative Law of Addition)* $\forall n\forall a\forall b\,(++(a,n,b) \Rightarrow ++(n,a,b))$.

Pf:

By induction, with ϕ as

$$\forall a\forall b\,(++(a,n,b) \Rightarrow ++(n,a,b)).$$

Suppose $++(a,0,b)$. Then $a = b$ by *Prop 3.5*, so $++(0,a,b)$ by *Prop 3.7*.

Now assume $\mathrm{N}n \;\&\; \sigma n,m \;\&\; \phi$. And suppose $++(a,m,b)$. Then by *Prop 3.4* $++(a,n,c) \;\&\; \sigma c,b$, for some c. By the induction hypothesis, $++(n,a,c)$. By *Prop 3.13* $++(m,a,b)$. □

(**FPA**) *Prop 3.15.* $\forall a \forall b\ (++(a,b,a) \Rightarrow b = 0)$

Pf:

By induction, with ϕ as

$$\forall b\ (++(n,b,n) \Rightarrow b = 0)$$

Suppose $++(0,b,0)$. Then by *Prop 3.6*, $b = 0$.

Now assume Nn & $\sigma n,m$ & ϕ. Suppose $++(m,b,m)$. Then by *Prop 3.14,* $++(b,m,m)$. By *Prop 3.4,* $++(b,n,n)$. By *Prop 3.14* again, $++(n,b,n)$. By the induction hypothesis $b = 0$. □

Def 3.16. $n \ll m$ if and only if $\exists k\ (\neg\, k = 0\ \&\ ++(n,k,m))$. □

Remark that, if $n \ll m$, then Nn & Nm.

(**FPA**) *Prop 3.17.* $\forall n$ (Nn & $\neg\, n = 0 \Rightarrow 0 \ll n$)

Pf:

Assume Nn & $\neg\, n = 0$. Then $++(0,n,n)$ by *Prop 3.7*. So $0 \ll n$. □

(**FPA**) *Prop 3.18.* $\forall n\ \neg\, n \ll n$

Pf:

Suppose $n \ll n$. Then $++(n,k,n)$ for some k where $\neg\, k = 0$. But *Prop 3.15* implies that $k = 0$, a contradiction. □

The first appeal to (PA6) appears in the proof of the next proposition.

(**FPA**) *Prop 3.19.* $\forall n\ \neg\, n \ll 0$

Pf:

Suppose $n \ll 0$. Then $\neg\, k = 0$ & $++(n,k,0)$, for some k. By *Prop 1.2*, Nu & $\sigma u,k$, for some u. By *Prop 3.4*, $++(n,u,v)$ & $\sigma v,0$. But this contradicts (PA6). □

(**FPA**) *Prop 3.20.* $\forall a \forall b$ (Na & Nb & $\sigma a,b \Rightarrow a \ll b$)

Pf:

Assume Na & Nb & $\sigma a,b$. Then by *Prop 1.6*, Nu & $\sigma 0,u$, for some u. By *Prop 3.8*, $++(a,0,a)$. So by *Prop 3.12*, $++(a,u,b)$. By (PA6) $\neg\, u = 0$. Hence $a \ll b$. □

(**FPA**) *Lemma 3.21.* $\forall a\forall b\forall c\ (++(a,b,c)\ \&\ \neg\ a = 0 \Rightarrow \exists b'(\mathrm{N}b'\ \&\ \sigma b,b'))$

Pf:

By induction, with ϕ as

$$\forall b\forall c\ (++(n,b,c)\ \&\ \neg\ n = 0 \Rightarrow \exists b'(\mathrm{N}b'\ \&\ \sigma b,b'))$$

The assertion is trivially true when $n = 0$.

Now assume $\mathrm{N}n\ \&\ \sigma n,m\ \&\ \phi$. Suppose $++(m,b,c)\ \&\ \neg\ m = 0$. By *Prop 3.14*, $++(b,m,c)$. By *Prop 3.4*, $\sigma v,c\ \&\ ++(b,n,v)$ for some v. By *Prop 3.14* again, $++(n,b,v)$. If $n = 0$, then $b = v$ by *Prop 3.6*; hence set $b' = c$. Otherwise, $\neg\ n = 0$, so by the induction hypothesis $\exists b'(\mathrm{N}b'\ \&\ \sigma b,b')$. □

(**FPA**) *Prop 3.22.* $\forall n\forall m\ (\mathrm{N}n\ \&\ \mathrm{N}m\ \&\ \sigma n,m \Rightarrow \forall z((z << n \vee z = n) \Leftrightarrow z << m))$

Pf:

Assume $\mathrm{N}n\ \&\ \mathrm{N}m\ \&\ \sigma n,m$.

Suppose $z << n \vee z = n$. If $z = n$, then $\sigma z,m$, so by *Prop 3.20*, $z << m$. If $z = 0$, then $z = 0 << m$ by *Prop 3.17* since $\neg\ m = 0$ by (PA6). .Otherwise, suppose $z << n\ \&\ \neg\ z = 0$. Then $++(z,k,n)$ for some k. By the lemma, $\mathrm{N}k'\ \&\ \sigma k,k'$ for some k'. But then $++(z,k',m)$ by *Prop 3.12*. By (PA6) $\neg\ k' = 0$, so $z << m$.

Now assume $z << m$. Then $\neg\ k = 0\ \&\ ++(z,k,m)$, for some k. By *Prop 1.2*, $\mathrm{N}j\ \&\ \sigma j,k$ for some j. By *Prop 3.4*, $++(z,j,n)$. If $j = 0$, then $z = n$ by *Prop 3.5*. And if $\neg\ j = 0$, then $z << n$. □

(**FPA**) *Corollary 3.23.* $\forall n(\mathrm{N}n \Rightarrow \exists P\forall z(Pz \Leftrightarrow z << n))$.

Pf:

By induction (F4*), with ϕ as

$$\exists P\forall z(Pz \Leftrightarrow z << n).$$

For $n = 0$, let P be ϕ. Then, by *Prop 3.19*, $\forall z(Pz \Leftrightarrow z << 0)$.

Now assume $\mathrm{N}n\ \&\ \mathrm{N}m\ \&\ \sigma n,m\ \&\ \exists P\forall z(Pz \Leftrightarrow z << n)$. Set P' to $\{z : Pz \vee z = n\}$. Then by *Prop 3.22*, $\forall z(P'z \Leftrightarrow z << m)$. □

(**FPA**) *Def 3.24.* Let $\mathrm{N}n$. Let *[0 _ n)* be that P (unique up to equivalence) guaranteed by *Corollary 3.23*, so $\forall z([0\ \_\ n)z \Leftrightarrow z << n))$. □

Remark:

(**FPA**) *Prop 3.25.* $\forall n\ (\ \mathrm{N}n \Rightarrow ([0\ \_\ n) \equiv \phi \Leftrightarrow n = 0)\ )$

Pf:

By *Props 3.17* and *3.19*. □

(**FPA**) *Prop 3.26.* $\forall n \forall m$ (Nn & Nm & $\sigma n{,}m \Rightarrow ([0 \_ n) \cup \{n\} \equiv [0 \_ m)$ & $\neg\, [0 \_ n)n$))
Pf:

Assume Nn & Nm & $\sigma n{,}m$. Then $[0 \_ n) \cup \{n\} \equiv [0 \_ m)$ by *Prop 3.22*.
Suppose $[0 \_ n)n$. Then $n << n$, contrary to *Prop 3.18*. □

(**FPA**) *Prop.* $\forall n \forall k$ (Nn & Nk & $[0 \_ n) \sim [0 \_ k) \Rightarrow n = k$).
Pf:

By induction, with ϕ as

$$\forall k\ (\mathrm{N}n\ \&\ \mathrm{N}k\ \&\ [0 \_ n) \sim [0 \_ k) \Rightarrow n = k)$$

Suppose N0 & Nk & $[0 \_ 0) \sim [0 \_ k)$. By *Prop 3.25*, $[0 \_ 0) \equiv \phi$. But this forces $[0 \_ k) \equiv \phi$. By *Prop 3.25*, $k = 0$.

Now assume Nn & $\sigma n{,}m$ & ϕ. Suppose Nm & Nk & $[0 \_ m) \sim [0 \_ k)$. If $k = 0$, then it has already been shown that $m = 0$ as well. So suppose $\neg\, k = 0$. Then by *Prop 1.2*, Nj & $\sigma j{,}k$ for some j. By *Prop 3.26*,

$$[0 \_ n) \cup \{n\} \sim [0 \_ j) \cup \{j\},$$

where $[0 \_ n)$ and $\{n\}$ are pairwise disjoint, as are $[0 \_\ j)$ and $\{j\}$. By logic, $[0 \_ n) \sim [0 \_ j)$. By the induction hypothesis $n = j$. By (PA4) $m = k$. □

Def 3.27. M$n{,}P$ if and only if

$$(n = 0\ \&\ P \equiv \phi) \vee \exists k \exists a(\mathrm{N}k\ \&\ \sigma k{,}n\ \&\ Pa\ \&\ (P \setminus \{a\}) \sim [0 \_ k)). \quad □$$

Remark: It would perhaps seem more natural to define M$n{,}P$ as

$$\mathrm{P} \sim [0 \_ n).$$

However, $[0 \_ n) \equiv \phi$ whenever $\neg$ Nn. It would then be possible to have both M0,P and M$n{,}P$ for 0 and some $n \neq 0$, contrary to (F1).

It remains to prove (F1), (F2), (F3), and that (PA2) & (PA3) $\Rightarrow$ (F6).

(**FPA**) *Prop 3.28.* (F1) $\forall n \forall m \forall P$ (M$n{,}P$ & M$m{,}P$ $\Rightarrow n = m$)
Pf:

Assume M$n{,}P$ & M$m{,}P$. If $n = 0$, then $P \equiv \phi$. If $\neg\, m = 0$, then Nk & $\sigma k{,}m$ & Pa & $(P \setminus \{a\}) \sim [0 \_ k)$, for some $k{,}a$, contradicting $P \equiv \phi$. So $m = 0$. A similar argument shows that if $m = 0$, then $n = 0$.

Hence it may be assumed that both $\neg\, n = 0$ & $\neg\, m = 0$. Thus Nk & $\sigma k{,}n$ & Pa & $(P \setminus \{a\}) \sim [0 \_ k)$) and N$j$ & $\sigma j{,}m$ & Pb & $(P \setminus \{b\}) \sim [0 \_ j)$) for some $j{,}k{,}a{,}b$. But

$(P \setminus \{a\}) \sim (P \setminus \{b\})$, so $[0 \_ k) \sim [0 \_ j)$. By *Prop 3.27,* this forces $k = j$. By (PA4) $n = m$.□

(**FPA**) *Prop 3.29*. (F2) $\forall P\ (\ \mathrm{M}0,P \Leftrightarrow \neg\, \exists x\ Px\ )$

Pf:

If $P \equiv \phi$, then by definition $\mathrm{M}0,P$.

On the other hand, suppose $\mathrm{M}0,P$. By (PA6) not:

$$\exists k \exists a(\mathrm{N}k\ \&\ \sigma k,0\ \&\ Pa\ \&\ (P \setminus \{a\}) \sim [0 \_ k)).$$

This forces $P \equiv \phi$. □

(**FPA**) *Prop 3.30*. (F3) $\forall n \forall m \forall P \forall Q \forall a\ (\ \mathrm{N}n\ \&\ \sigma n,m\ \&\ \neg\, Pa\ \&\ Q \equiv (P \cup \{a\}) \Rightarrow (\mathrm{M}n,P \Leftrightarrow \mathrm{M}m,Q)\ )$

Pf:

Assume $\mathrm{N}n\ \&\ \sigma n,m\ \&\ \neg Pa\ \&\ Q \equiv (P \cup \{a\})$. Obviously, Qa.

Suppose $\mathrm{M}n,P$. If $n = 0$, then $P \equiv \phi$, so $Q \equiv \{a\}$, and $[0 \_ 0) \sim (Q \setminus \{a\}))$, so $\mathrm{M}m,Q$. Thus suppose $\neg\, n = 0$. Then $\mathrm{N}k\ \&\ \sigma k,n\ \&\ Pb\ \&\ (P \setminus \{b\}) \sim [0 \_ k)$, for some k,b. But by *Prop 3.26* $[0 \_ k) \cup \{k\} \equiv [0 \_ n)$, where $[0 \_ k)$ and $\{n\}$ are pairwise disjoint. Thus by logic $P \sim [0 \_ n)$. So:

$$\mathrm{N}n\ \&\ \sigma n,m\ \&\ Qa\ \&\ (Q \setminus \{a\}) \sim [0 \_ n).$$

Hence $\mathrm{M}m,Q$.

On the other hand, suppose $\mathrm{M}m,Q$. Then $\neg\, m = 0$ by *Prop 3.29*. Hence $\mathrm{N}k\ \&\ \sigma k,m\ \&\ Qb\ \&\ (Q \setminus \{b\}) \sim [0 \_ k)$, for some k,b. By (PA5) $n = k$. If $n = 0$, then $(Q \setminus \{b\}) \equiv \phi$ by *Prop 3.25* so $Q \equiv \{b\}$ and $P \equiv \phi$; but then $\mathrm{M}n,P$ by *Prop 3.29*. Otherwise $\neg\, n = 0$, i.e. $\neg\, k = 0$. So $\sigma j,k\ \&\ \mathrm{N}j$ for some j, by *Prop 1.2*. Now by logic, $P \sim (Q \setminus \{b\})$. So $P \sim [0 \_ k)$. By *Prop 3.26*, $[0 \_ k) \sim [0 \_ j) \cup \{j\}$, where $\neg\, [0 \_ j)j$. But then by logic, $(P \setminus \{c\}) \sim [0 \_ j)$, for some c where Pc. By definition $\mathrm{M}k,P$ and so $\mathrm{M}n,P$. □

(**FPA**) *Prop 3.31*. (PA2) & (PA3) $\Rightarrow$ (F6)

Pf:

Assume (PA2) & (PA3).

Suppose $\mathrm{N}n\ \&\ \mathrm{M}n,P\ \&\ \neg\, Pa$. By (PA3) $\sigma n,m$ for some m. By (PA2) $\mathrm{N}n$. By *Prop 3.30* $\mathrm{M}m,(P \cup \{a\})$. □

Thus it has been shown, given *Def* 3.28 of "M," that **FPA** proves the axioms of **F**, and **PA2** proves the axioms of **FF**.

4. Addition

From this point on, the axioms of **F** will be assumed. It will be shown, over the course of several chapters, that much of arithmetic can be derived from **F**. Given the equivalences demonstrated in the previous two chapters, this is the same thing as saying that the axioms of **FPA** can be used to derive much of arithmetic.

In the last chapter addition was defined (*Def 3.3*) in the context of the Peano Axioms **FPA**, and that course could be continued, most notably by making the analogous, recursive definition of multiplication. No direct recourse to “M” or the **F** axioms would be allowed or needed. However, the development chosen here will be to appeal to the axioms of **F** exclusively, with very occasional uses only of the Peano Axioms (PA4) and (PA6). In particular, the results of Chapter 3 will be ignored and not used henceforth..

4A. Prolegomenon to Addition

This section groups a somewhat hodgepodge collection of propositions, which will be used later.

Prop 4.1. $\forall n \forall P\ (\ \mathrm{M}n,P\ \&\ P \equiv \phi \Rightarrow n = 0\ )$
Pf:

By *Prop 2.1.* □

Prop 4.2. $\forall n \forall P \forall Q \forall R \forall S\ (\ \mathrm{N}n\ \&\ \mathrm{M}n,R\ \&\ P \sim Q\ \&\ R \sim S\ \&\ R \subseteq P\ \&\ S \subseteq Q$
$\Rightarrow (P \setminus R) \sim (Q \setminus S)\ )$
Pf:

By induction (F4*), with ϕ as

$$\forall P \forall Q \forall R \forall S (\mathrm{M}n,R\ \&\ P \sim Q\ \&\ R \sim S\ \&\ R \subseteq P\ \&\ S \subseteq Q\ \Rightarrow (P \setminus R) \sim (Q \setminus S))$$

□

Prop 4.3. $\forall n \forall P\ (\ \mathrm{N}n \Rightarrow \exists Q\ (\mathrm{M}n,Q\ \&\ (P \subseteq Q \vee Q \subseteq P))\ )$
Pf:

By induction (F4*), with ϕ as

$$\forall P \exists Q\ (\mathrm{M}n,Q\ \&\ (P \subseteq Q \vee Q \subseteq P)).$$

Obviously, by (F2), $\forall P\ (\mathrm{M}0,\phi\ \&\ \phi \subseteq P)$.

Now assume $\mathrm{N}n\ \&\ \mathrm{N}m\ \&\ \neg\ m = 0\ \&\ \sigma n,m\ \&\ \phi$. Consider any P. By the induction hypothesis, $\mathrm{M}n,Q\ \&\ (P \subseteq Q \vee Q \subseteq P)$, for some Q. By *POTINF* (*Theorem 2.24*), $\exists q \neg Qq$. By (F3), $\mathrm{M}m,(Q \cup \{q\})$.

If $P \subseteq Q$, then $P \subseteq Q \cup \{q\}$. Otherwise, $Q \subset P$, so $Q \cup \{q'\} \subseteq P$ for some q'. By (F3), $\mathrm{M}m,(Q \cup \{q'\})$. □

The following proposition ensures the “downwards” character of **F** and is thus important:

Prop 4.4. $\forall n\forall P\forall Q\,(\,\mathrm{N}n \,\&\, \mathrm{M}n,P \,\&\, Q \subseteq P \Rightarrow \exists k\,(\mathrm{N}k \,\&\, \mathrm{M}k,Q)\,)$

Pf.

By induction (F4*) on n, with ϕ as

$$\forall P\forall Q\,(\,\mathrm{M}n,P \,\&\, Q \subseteq P \Rightarrow \exists k\,(\mathrm{N}k \,\&\, \mathrm{M}k,Q)\,).$$

Suppose $\mathrm{N}0 \,\&\, \mathrm{M}0,P \,\&\, Q \subseteq P$. Then $P \equiv \phi$ by (F2). So $Q \equiv \phi$. By (F2) again, $\mathrm{M}0,Q$.

Now assume $\mathrm{N}n \,\&\, \mathrm{N}m \,\&\, \sigma n,m \,\&\, \neg\, m = 0 \,\&\, \phi$, and suppose $\mathrm{M}m,P \,\&\, Q \subseteq P$. If $Q \equiv P$, then set k to n. O.w. $Q \subseteq P \setminus \{a\}$ for some a with Pa. By (F3) $\mathrm{M}n,P \setminus \{a\}$. Done by the induction hypothesis. □

Prop 4.5.

a. Transitivity. If $a \le b$ and $b \le c$, then $a \le c$.

b. Dichotomy. $\forall a\forall b\,(\,\mathrm{N}a \,\&\, \mathrm{N}b \Rightarrow a \le b \vee b < a)$

Pf.

a. Assume $a \le b$ and $b \le c$. Then $\mathrm{N}a \,\&\, \mathrm{N}b \,\&\, \mathrm{N}c \,\&\, A \subseteq B \,\&\, \mathrm{M}a,A \,\&\, \mathrm{M}b,B \,\&\, B' \subseteq C \,\&\, \mathrm{M}b,B' \,\&\, \mathrm{M}c,C$, by *Def 1.7*. By *Prop 2.3* $B \sim B'$, so there exists one-to-one function R from B onto B'. Set A' to $\mathit{Im}(\mathrm{R} \lceil \mathrm{A})$. Evidently $A \sim A'$ and $A' \subseteq C$. So $\mathrm{M}a,A'$ by *Finite Hume’s Principle* (*Prop 2.3*), and thus $a \le c$.

b. Assume $\mathrm{N}a \,\&\, \mathrm{N}b$. By *POTINF* (*Theorem 2.24*), $\mathrm{M}a,P$ for some P. By *Prop 4.3*, $\mathrm{M}b,Q \,\&\, (P \subseteq Q \vee Q \subseteq P)$ for some Q.

If $P \subseteq Q$, then $a \le b$.

And if not $P \subseteq Q$, then $Q \subset P$. So $b \le a$. If $b = a$, then $P \equiv Q$ by *Prop 2.6*, a contradiction. So $\neg\, b = a$, hence $b < a$. □

Recall, by *Def 1.5*, that *one*(u) abbreviates ($\mathrm{N}u \,\&\, \sigma 0,u$). Of course, it cannot be shown that there exists u such that *one*(u). But if such a u exists, then it has all the “downward” properties of one.

In order to render assertions more perspicacious, introduce a new variable 1 (adding it to the usual alphabetic variables $x,y,z,\ldots$). In the future, this special variable will be used exclusively as the argument of the predicate one.

Prop 4.6. Let *one*(1). Then $\neg\, 0 = 1$ and indeed $0 < 1$.

Pf:

By definition of *one*, $\mathrm{N}1 \,\&\, \sigma 0,1$. Since $\mathrm{M}0,\phi$ by (F2), $\mathrm{M}1,\{0\}$ by (F3). By (F2) again, $\neg\, 1 = 0$.

Evidently $\phi \subseteq \{0\}$. Hence $0 \le 1$. □

Prop 4.7. Let *one*(1). Then M1,P if and only if $\exists$a $P \equiv \{a\}$.
Pf:

Suppose M1,P. By *Prop 4.6*, $\neg\, 1 = 0$. By *Prop 2.1 Pa* for some a. By (F3) M0,$(P \setminus \{a\})$. By (F2) $(\mathrm{P} \setminus \{a\}) \equiv \phi$. Hence $P \equiv \{a\}$.

On the other hand suppose $P \equiv \{a\}$ for some a. Since M0,ϕ by (F2), M1,P by (F3).

□

Prop 4.8. Let $P \equiv \{a\}$ for some a, and assume Nu. Then *one*(u) if and only if Mu,P.
Pf:

Half follows from *Prop 4.7*. Now suppose M1,P. Apply *Lemma 2.12*. □

Prop 4.9. Let Nn & $\neg\, n = 0$. Then $\exists 1$ *one*(1), and moreover $1 \leq \mathrm{n}$.
Pf:

By *POTINF* (*Theorem 2.24*), Mn,P for some P. By *Prop 2.1* Pa for some a. But $\{a\} \subseteq P$, so by *Prop 4.4*, N1 & M1,$\{a\}$ for some 1. By *Prop 4.8*, *one*(1). Evidently, $1 \leq n$.

□

Prop 4.10. Let $n \leq 1$, where *one*(1). Then $n = 0 \vee n = 1$.

Note: The proof would be more straight-foward if it could appeal to Anti-Symmetry (*Prop 4.18*), but the nature of the proposition places it here.

Pf:

By *Def 1.7*, Nx & Ny & $P \subseteq Q$ & Mn,P & M1,Q, for some P,Q. By *Prop 4.7*, $Q \equiv \{a\}$, for some a. By logic, $P \equiv \phi$ or $P \equiv \{a\}$. The former case and *Prop 4.1* imply $n = 0$. The latter case and *Prop 4.8* implies *one*(n). □

4B. Definition of Addition and Elementary Propositions.

Def 4.11. Use $+(x,y,z)$ to abbreviate:

Nx & Ny & Nz & $\exists P \exists Q$ ($(P \cap Q) \equiv \phi$ & Mx,P & My,Q & Mz,$(P \cup Q)$) □

Prop 4.12. (*Uniqueness*) $\forall$x$\forall$y$\forall$a$\forall$b ($+(x,y,a)$ & $+(x,y,b) \Rightarrow a = b$)
Pf:

Assume $+(x,y,a)$ & $+(x,y,b)$. Then by *Def 4.11*, for some P,Q,P',Q',

Nx & Ny & Na and $(P \cap Q) \equiv \phi$ & Mx,P & My,Q & Ma,$(P \cup Q)$

and

$$\mathrm{N}x \ \&\ \mathrm{N}y \ \&\ \mathrm{N}a \text{ and } (P' \cap Q') \equiv \phi \ \&\ \mathrm{M}x,P' \ \&\ \mathrm{M}y,Q' \ \ \&\ \mathrm{M}b,(P' \cup Q').$$

By logic, $(P \cup Q) \sim (P' \cup Q')$. By *Finite Hume's Principle* (*Prop 2.3*), $\mathrm{M}a,(P' \cup Q')$. By (F1), $a = b$. □

If $+(x,y,z)$, then $(x + y)$ will be used to refer to z, which is legitimate given the previous proposition. Note that the appearance of $(x + y)$ in an atomic formula ϕ is to be read as $\exists z\ (+(x,y,z)\ \&\ \phi^*)$ where ϕ^* is ϕ with z (assumed not to be appearing in ϕ) replacing $(x + y)$. So e.g. $(x + y) \leq a$ means

$$\exists z\ (+(x,y,z)\ \&\ z \leq a),$$

and $(x + y) = z'$ means

$$\exists z\ (+(x,y,z)\ \&\ z = z'), \text{ which is just } +(x,y,z').$$

Hence $(x + y) = z'$ and $+(x,y,z')$ are interchangeable.

Terms with additive sub-terms are permitted, and any reasonable unwinding is permitted, e.g. $((x + y) + u) \leq a$ may be read either as

$$\exists z\ (+(x,y,z)\ \&\ (z + u) \leq a)$$

and from there

$$\exists z\ (\ +(x,y,z)\ \&\ \exists z'(+(z,u,z')\ \&\ z' \leq a)\ ),$$

or as

$$\exists z'\ (+((x + y),u,z')\ \&\ z' \leq a)$$

and from there

$$\exists z'\ (\ \exists z(+(x,y,z)\ \&\ +(z,u,z'))\ \&\ z' \leq a\ ).$$

The two unwindings are, of course, logically equivalent.

Notice that by *Def 4.11*, if $(x + y)$ exists, then $\mathrm{N}(x + y)$.

Expressing addition as a term rather than as a predicate is more convenient, because terms involving multiple additions are easily built up, for instance as used in the *Associative Laws*. On the negative side, its use asserts uniqueness of the sum, which appeals to *Prop 4.12* and thus *Finite Hume's Principle*, which is not necessarily needed in the equivalent assertion involving addition as a 3-arity predicate. For instance, the proof of the *Commutative Law of Addition* in the predicate form

$$\forall \mathrm{x} \forall \mathrm{y} \forall z\ (\ +(x,y,z) \Rightarrow +(y,x,z)\ )$$

requires only logic and one appeal to *Corollary 2.4*. Because of the comments after that *Corollary*, this means that *Commutativity* in the predicate form can be proved with logic only, in an environment where extensionality is assumed.

Prop 4.13. (*Commutative Law*). $\forall x \forall y \forall \mathrm{z}\ (\ (x + \mathrm{y}) = z \Rightarrow (y + x) = z\ )$

Note: Henceforth commutative permutations will be assumed, so e.g. even though *Prop 4.15* only asserts $(0 + x) = x$, it will be supposed that the proposition $(x + 0) = x$ follows without explicit assertion.

Pf:

Assume $(x + y) = z$. By *Def 4.11*, Nx & Ny & Nz, and there are X,Y such that:

$$(X \cap Y) \equiv \phi\ \&\ \mathrm{M}x,X\ \&\ \mathrm{M}y,Y\ \&\ \mathrm{M}z,(X \cup Y).$$

By logic $(Y \cap X) \equiv \phi$ & $(Y \cap X) \equiv (X \cup Y)$. By *Corollary 2.4*, M$z$,$(Y \cup X)$. Thus $(y + x) = z$.

□

Prop 4.14. (*Zero*).

a. $\forall x\ (\ \mathrm{N}x \Rightarrow (0 + x) = x\ )$

b. $\forall x \forall y\ (\ (x + y) = x \Rightarrow y = 0\ )$

c. $\forall x \forall y\ (\ (x + y) = 0 \Rightarrow x = 0\ \&\ y = 0\ )$

Pf:

a. Suppose Nx. By *Prop 1.1*, N0. By *POTINF* (*Theorem 2.24*), Mx,P for some P. By (F2), M0,ϕ. By *Corollary 2.4* Mx,$(\phi \cup P)$. Thus

$$\mathrm{N}0\ \&\ \mathrm{N}x\ \&\ \mathrm{N}0\ \&\ (\phi \cap P) \equiv \phi\ \&\ \mathrm{M}0,\phi\ \&\ \mathrm{M}x,P\ \&\ \mathrm{M}x,(\phi \cup P).$$

b. Suppose $(x + y) = x$. Then by *Def 4.11*, Nx & Ny, and there are X,Y such that:

$$(X \cap Y) \equiv \phi\ \&\ \mathrm{M}x,X\ \&\ \mathrm{M}y,Y\ \&\ \mathrm{M}x,(X \cup Y).$$

Obviously, $X \subseteq (X \cup Y)$, so by the *Pigeon Hole Principle* (*Prop 2.6*), $(X \cup Y) \equiv X$. By logic $Y \equiv \phi$. By *Prop 4.1*, $y = 0$.

c. Assume $(x + y) = 0$. Then by *Def 4.11*, Nx & Ny, and there are X,Y such that:

$$(X \cap Y) \equiv \phi\ \&\ \mathrm{M}x,X\ \&\ \mathrm{M}y,Y\ \&\ \mathrm{M}0,(X \cup Y).$$

By (F2), $(X \cup Y) \equiv \phi$. Evidently, $X \equiv Y \equiv \phi$. By *Prop 4.1*, $\mathrm{x} = \mathrm{y} = 0$. □

Prop 4.15 (*Associative Laws*).

a. $\forall x \forall y \forall z \forall a\ (\ ((x + y) + z) = a \Rightarrow (x + (y + z)) = a\ )$

b. $\forall x \forall y \forall z \forall a\ (\ (x + (y + z)) = a \Rightarrow ((x + y) + z) = a\ )$

Pf:

a. Assume $((x + y) + z) = a$. Then by *Def 4.11*, Nz & Na, and there are c, C, Z such that:

$$(C \cap Z) \equiv \phi \ \&\ \mathrm{M}c,C \ \&\ \mathrm{M}z,Z \ \&\ \mathrm{M}a,(C \cup Z) \ \&\ (x + y) = c.$$

The latter conjunct implies that Nx & Ny & Nc and there are X,Y s.t.

$$(X \cap Y) \equiv \phi \ \&\ \mathrm{M}x,X \ \&\ \mathrm{M}y,Y \ \&\ \mathrm{M}c,(X \cup Y).$$

By *Finite Hume's Principle* (*Prop 2.3*), $(X \cup Y) \sim C$, so by logic there exist X',Y' such that

$$X' \sim X \ \&\ Y' \sim Y \ \&\ (X' \cap Y') \equiv \phi \ \&\ (X' \cup Y') \equiv C.$$

By *Finite Hume's Principle* in the other direction and *Corollary 2.4*, Mx,X' & My,Y' & M$c,(X' \cup Y')$.

By logic, $(Y' \cap Z) \equiv \phi$ and $(Y' \cup Z) \subseteq (C \cup Z)$. By *Prop 4.4*, M$d,(Y' \cup Z)$ for some d s.t. Nd. Note that $d = (y + z)$.

Also by logic, $(X' \cap (Y' \cup Z)) \equiv \phi$ and $(X' \cup (Y' \cup Z)) \equiv (C \cup Z)$. Thus by *Def 4.11*, $(x + d) = a$, and so $(x + (y + z)) = a$.

b. Assume $(x + (y + z)) = a$. By two applications of the *Commutative Law* (*Prop 4.13*), $((z + y) + x) = a$. By (*a*), $(z + (y + x)) = a$. By two more applications of the *Commutative Law*, $((x + y) + z) = a$. □

Prop 4.16 (Cancellation) $\forall x \forall y \forall z\ (\ (x + y) = (x + z) \Rightarrow y = z\ )$
Pf:

Assume $(x + y) = (x + z)$. Then by *Def 4.11*, Nx & Ny & Nz, and there are X,Y,X' and Z' such that:

$$(X \cap Y) \equiv \phi \ \&\ \mathrm{M}x,X \ \&\ \mathrm{M}y,Y \ \&\ \mathrm{M}(x + y),(X \cup Y)$$

and

$$(X' \cap Z') \equiv \phi \ \&\ \mathrm{M}x,X' \ \&\ \mathrm{M}z,Z' \ \&\ \mathrm{M}(x + z),(X' \cup Z').$$

By *Finite Hume's Principle* (*Prop 2.3*), $X \sim X'$ and, since $(x + y) = (x + z)$, $(X \cup Y) \sim (X' \cup Z')$. *Prop 4.2* implies that $Y \sim Z'$. So by *Finite Hume's Principle* in the other direction, My,Z'. By (F1), $y = z$. □

Prop 4.17. $\forall x \forall y\ (\ x \leq y \Leftrightarrow \exists z\ (x + z) = y\ )$
Pf:

Suppose $x \leq y$. Then by *Def 1.7*, Nx & Ny and $P \subseteq Q$ & Mx,P & My,Q for some P,Q. Consider P and $(Q \setminus P)$. Their union is equivalent to Q and their intersection is empty. By *Prop 4.4*, M$z,(Q \setminus P)$ for some z s.t. Nz. By *Def 4.11*, $(x + z) = y$.

Now suppose $(x + z) = y$. Then by *Def 4.11*, Nx & Ny & Nz and $(P \cap Q) \equiv \phi$ & Mx,P & Mz,Q & M$y,(P \cup Q)$ for some P,Q. Evidently, $P \subseteq (P \cup Q)$. But then, by *Def 1.7*, $x \leq y$. □

Prop 4.17 is very useful. For one thing, it facilitates the proof of Anti-Symmetry of inequality.

Prop 4.18. (*Anti-Symmetry*) $\forall x \forall y\ (x \leq y\ \&\ y \leq x \Rightarrow x = y)$
Pf:

Assume $x \leq y\ \&\ y \leq x$. By F.*Prop 4.17*, $(x + z) = y$ and $(y + z') = x$ for some z,z'. Then $((x + z) + z') = x$. By *Associativity* (*Prop 4.15a*), $(x + (z + z')) = x$. So $(z + z') = 0$ by *Prop 4.14b*. By *Prop 4.14c*, $z = 0$. By *Prop 4.14a*, $x = y$. □

Prop 4.19.

a. $\forall a \forall b \forall x \forall y \forall z\ (a \leq x\ \&\ b \leq y\ \&\ (x + y) = z \Rightarrow (a + b) \leq z)$

b. $\forall a \forall x \forall y \forall z\ (x \leq y\ \&\ (y + z) = a \Rightarrow (x + z) \leq (y + z))$

c. $\forall x \forall y \forall z\ ((x + z) \leq (y + z) \Rightarrow x \leq y)$

Pf:

a. Assume $a \leq x\ \&\ b \leq y\ \&\ (x + y) = z$. By *Prop 4.17*, $(a + a') = x$ and $(b + b') = y$ for some a',b'. So $z = ((a + a') + (b + b'))$. By various applications of the *Commutative* and *Associative Laws*, $z = ((a + b) + (a' + b'))$. Reapplying *Prop 4.17* in the other direction, $(a + b) \leq z$.

b. Assume $x \leq y\ \&\ (y + z) = a$. By *Prop 4.17* $(x + x') = y$. So $((x + x') + z) = a$. Applying the Commutative and Associative Laws, $((x + z) + x') = a$. Thus by *Prop 4.17* in the other direction, $(x + z) \leq a$, and so $(x + z) \leq (y + z)$.

c. Assume $(x + z) \leq (y + z)$. By *Prop 4.17* $((x + z) + c) = (y + z)$ for some c. By Associativity and Commutativity, $((x + c) + z) = (y + z)$. By Cancellation (*Prop 4.16*), $(x + c) = y$. By *Prop 4.17* in the other direction, $x \leq y$. □

Remark that *Prop 4.19a* could not be written as:

$$\forall a \forall b \forall x \forall y \forall z\ (a \leq x\ \&\ b \leq y \Rightarrow (a + b) \leq (x + y)).$$

This is because, given x and y, it cannot be inferred that $(x + y)$ exists. Its existence must be assumed, as is done in *Prop 4.19a* as actually stated.

Also notice that it is not necessary to assume the existence of $(a + b)$ as well. Its existence can be inferred from the existence of $(x + y)$, since it is a smaller number. (The proof of *Prop 4.19a* appeals to *Prop 4.17*, which in turn appeals to the crucial *Prop 4.4*.)

Prop 4.20.

a. $\forall x \forall y\ (\mathrm{N}x\ \&\ \mathrm{N}y\ \&\ \sigma x{,}y \Leftrightarrow \exists 1\ (\mathit{one}(1)\ \&\ (x + 1) = y))$

b. $\forall x \forall y \forall 1$ ($\mathrm{N}x$ & $\mathrm{N}y$ & $\mathit{one}(1)$ & $\sigma x,y \Rightarrow (x + 1) = y$)

c. $\forall x \forall y \forall 1$ ($\mathit{one}(1)$ & $(x + y) = 1$ & $\neg\, x = 0 \;\Rightarrow x = 1$ & $y = 0$)

Pf:

a. Suppose $\mathrm{N}x$ & $\mathrm{N}y$ & $\sigma x,y$. By *POTINF* (*Theorem 2.24*), $\mathrm{M}x,P$ & $\neg\, Pa$ for some P,a. By (F3), $\mathrm{M}y,(P \cup \{a\})$. By (F2), $\neg\, y = 0$. By *Prop 4.4*, $\mathrm{M}1,\{a\}$ for some 1 s.t. N1. By *Prop 4.8*, $\mathit{one}(1)$. By *Def 4.11*, $(x + \mathit{1}) = \mathrm{y}$.

Now suppose $\mathit{one}(1)$ & $(x + 1) = y$, for some 1. Then $\mathrm{N}x$ & $\mathrm{N}y$ & N1 and $(P \cap Q) \equiv \phi$ & $\mathrm{M}x,P$ & $\mathrm{M}1,Q$ & $\mathrm{M}y,(P \cup Q)$), for some P,Q. By *Prop 4.7*, $Q \equiv \{q\}$ for some q. Evidently, $(P \cup Q) \equiv (P \cup \{q\})$, so by *Corollary 2.4*, $\mathrm{My},(\mathrm{P} \cup \{\mathrm{q}\})$. So by *Lemma 2.12*, $\sigma x,y$.

b. Assume $\mathrm{N}x$ & $\mathrm{N}y$ & $\mathit{one}(1)$ & $\sigma x,y$. By *Def 1.5*, N1 & $\sigma 0,1$. By (*a*) $\mathrm{N}u$ & $\sigma 0,u$ & $(x + u) = y$ for some u. But $u = 1$ by (PA4).

c. Assume $\mathit{one}(1)$ & $(x + y) = 1$ & $\neg\, x = 0$. By *Def 4.11*, $\mathrm{N}x$ & $\mathrm{N}y$, and there are X,Y such that:

$$(X \cap Y) \equiv \phi \;\&\; \mathrm{M}x,X \;\&\; \mathrm{M}y,Y \;\&\; \mathrm{M}1,(X \cup Y).$$

By *Prop 4.7*, $(X \cup Y) \equiv \{a\}$ for some a. But $\neg\, X \equiv \phi$ by *Prop 2.1*, so evidently $X \equiv \{a\}$ and $Y \equiv \phi$. By *Prop 2.1* again, $y = 0$. By *Prop 4.7* and (F1), $x = 1$. □

Prop 4.21.

a. $\forall x \forall n \forall m$ ($\mathrm{N}n$ & $\mathrm{N}m$ & $\sigma n,m \Rightarrow (x \leq n \Leftrightarrow x < m))$

b. $\forall x \forall n \forall m$ ($\mathrm{N}n$ & $\mathrm{N}m$ & $\sigma n,m \Rightarrow (x \leq m \Leftrightarrow x \leq n \vee x = m))$

c. $\forall x \forall y \forall 1$ ($y < x$ & $\mathit{one}(1) \Rightarrow (y + 1) \leq x$)

Pf:

a. Assume $\mathrm{N}n$ & $\mathrm{N}m$ & $\sigma n,m$.

Suppose $x \leq n$. Then $(x + z) = n$ for some z, by *Prop 4.17*. Also, by *Prop 4.20a*, $\mathit{one}(1)$ & $(n + 1) = m$ for some 1. So $((x + z) + 1) = m$. By *Associativity (Prop 4.15a)*, $(x + (z + 1)) = m$. By the other direction of *Prop 4.17*, $x \leq m$. If $x = m$, then by *Props 4.14b* and *4.14c*, $1 = 0$; but this contradicts *Prop 4.6*.

On the other hand, suppose $x < m$. So $\neg\, x \;= m$. Further suppose that $\neg\, x \leq n$. By *Dichotomy* (*Prop 4.5b*), $n < x$. So $\neg\, x = n$. By *Prop 4.17*, $(n + z) = x$ and $(x + z') = m$, for some z,z'. Remark that, by *Prop 4.14a*, neither z nor z' equals 0. Also, using *Associativity* (*Prop 4.15a*), $(n + (z + z')) = m$. But by *Prop 4.20a*, $(n + 1) = \mathrm{m}$ where $\mathit{one}(1)$. Hence by *Cancellation* (*Prop 4.16*), $(z + z') = 1$. But *Prop 4.20c* then implies that either z or z' is 0, a contradiction.

b. Follows directly from (*a*).

c. Assume $y < x$ & $\mathit{one}(1)$. Then $\mathrm{N}x$ & $\mathrm{N}y$ by *Def 1.7*. By *Prop 1.2*, $\mathrm{N}k$ & $\sigma k,x$, for some k. By (*a*), $y \leq k$. By *Prop 4.20a*, $(k + 1) = x$. By *Prop 4.19b*, $(y + 1) \leq (k + 1)$. □

4C. Well-Ordering Principle and Maximality

Recall that $\phi[y\backslash x]$ is the formula resulting from replacing all free instances of x in ϕ with y.

Prop 4.22. Well-Ordering Principle. Let Nn and let φ be any formula with no appearance of m or y. Then:

a. Either:

$$\forall x\ (\ x \leq n \Rightarrow \neg\ \varphi\ )$$

or

$$\exists x\ (\ x \leq n\ \&\ \varphi\ \&\ \forall y\ (\ \mathrm{N}y\ \&\ \varphi\ [y\backslash x] \Rightarrow x \leq y\ )$$

b. Either:

$$\forall x\ (\ x \leq n \Rightarrow \neg\ \varphi\ )$$

or

$$\exists x\ (\ \mathrm{N}x\ \&\ \varphi\ \&\ \forall y\ (\ \mathrm{N}y\ \&\ \varphi\ [y\backslash x] \Rightarrow x \leq y\ )$$

c. Either:

$$\neg\ \exists x\ (\ \mathrm{N}x\ \&\ \varphi\ )$$

or

$$\exists x\ (\ \mathrm{N}x\ \&\ \varphi\ \&\ \forall y\ (\ y < x \Rightarrow \neg\ \varphi\ [y\backslash x]\ )$$

Pf:

a. Proceed by induction (F4*), with ϕ as

$$(\ \forall x\ (x \leq n \Rightarrow \neg\ \varphi\ )$$
$$\vee\ \exists x\ (\ x \leq n\ \&\ \varphi\ \&\ \forall y\ (\ \mathrm{N}y\ \&\ \varphi\ [y\backslash x] \Rightarrow x \leq y\ )\ )\ ).$$

Trivial when $n = 0$, since either $(\varphi\ [0\backslash n])[0\backslash x]$ or $\neg\ (\varphi\ [0\backslash n])[0\backslash x]$. If the former, then the first disjunct is true. If the latter, then the second disjunct is true by letting $x = 0$.

Now assume Nn & Nm & $\sigma n,m$ & $\neg\ m = 0$ & ϕ . By *Prop 4.21b*, one of these three cases obtains:

$$\forall x\ (\ x \leq m \Rightarrow \neg\ \varphi\ )$$
$$\forall x\ (\ x \leq n \Rightarrow \neg\ \varphi\ )\ \&\ \varphi\ [m\backslash x]$$

or

$$\exists x\ (\ x \leq n\ \&\ \varphi\ )$$

In the first case the conclusion follows immediately. In the second it is easy to show that

$$m \leq m\ \&\ \varphi\ [m\backslash x]\ \&\ \forall y\ (\ \mathrm{N}y\ \&\ \varphi\ [y\backslash x] \Rightarrow m \leq y\ ),$$

which implies

$$\exists x\ (\ x \leq m\ \&\ \varphi\ \&\ \forall y\ (\ \mathrm{N}y\ \&\ \varphi\ [y\backslash x] \Rightarrow x \leq y\ )\ ).$$

And the third case contradicts the first disjunct of the Induction Hypothesis ϕ, so it is the second disjunct

$$\exists x\,(\,x \leq n \;\&\; \varphi \;\&\; \forall y\,(\,\mathrm{N}y \;\&\; \varphi\,[y\backslash x] \Rightarrow x \leq y\,)\,)$$

which must obtain. But then obviously

$$\exists x\,(\,x \leq m \;\&\; \varphi \;\&\; \forall y\,(\,\mathrm{N}y \;\&\; \varphi\,[y\backslash x] \Rightarrow x \leq y\,)\,).$$

b. Follows from (*a*) since $x \leq n$ implies Nx, for all x,n.

c. Follows from (*b*) and *Dichotomy* (*Prop 4.5b*). □

The *Well-Ordering Principle* establishes the existence of the least number, the following proposition the existence of the greatest number.

Prop 4.23. Let Nn and let φ be any formula with no appearance of n, m or y. If

$$\forall x\,(\varphi \Rightarrow x \leq n) \;\&\; \exists x\,\varphi.$$

then

$$\exists x\,(\,\varphi \;\&\; x \leq n \;\&\; \forall y\,(\varphi\,[y\backslash x] \Rightarrow y \leq x)\,).$$

Pf:

Proceed by induction (F4*), with ϕ as

$$(\,\forall x\,(\varphi \Rightarrow x \leq n) \;\&\; \exists x\,\varphi \;\Rightarrow \exists x\,(\varphi \;\&\; \forall y\,(\varphi\,[y\backslash x] \Rightarrow y \leq x))\,).$$

Remark that $\varphi\,[0\backslash n]$ and $\varphi\,[\mathrm{m}\backslash n]$ are just φ, since n does not appear in φ.

Case n = 0. Suppose $\forall x\,(\varphi \Rightarrow x \leq 0)$ & $\exists x\,\varphi$. By the first conjunct, $\forall y\,(\varphi\,[y\backslash x] \Rightarrow y \leq 0)$. By the second conjunct, $\varphi\,[a\backslash x]$ for some a. Thus $a \leq 0$. By *Prop 2.14b*, $a = 0$. Hence $\varphi\,[0\backslash x]$, and thus

$$\varphi\,[0\backslash x] \;\&\; \forall y\,(\varphi\,[y\backslash x] \Rightarrow y \leq 0),$$

from which follows immediately

$$\exists x\,(\,\varphi \;\&\; \forall y\,(\varphi\,[y\backslash x] \Rightarrow y \leq x)\,)$$

Induction Step. Now assume Nn & Nm & $\sigma n{,}m$ & $\neg\, m = 0$ & ϕ. And suppose $\forall x\,(\varphi \Rightarrow x \leq m)$ & $\exists x\,\varphi$.

If $\neg\,\varphi\,[m\backslash x]$, then $\forall x\,(\varphi \Rightarrow x \leq n)$, by *Prop 4.21b*, and the result follows from the Induction Hypothesis.

On the other hand, suppose $\varphi\,[m\backslash x]$. But $\forall x\,(\varphi \Rightarrow x \leq m)$, so evidently if $\varphi\,[y\backslash x]$, then $y \leq m$. Thus

$$\varphi\,[m\backslash x] \;\&\; \forall y\,(\varphi\,[y\backslash x] \Rightarrow y \leq m),$$

from which follows immediately

$$\exists x\ (\ \varphi\ \&\ \forall y\ (\varphi\ [y\backslash x] \Rightarrow y \leq x)\ ). \qquad \square$$

5. Multiplication

Def 5.1. Use $*(x,y,z)$ to abbreviate:

$$\begin{aligned} &\mathrm{N}x \ \&\ \mathrm{N}y \ \&\ \mathrm{N}z\ \&\\ &\exists P\exists R\ (\mathit{Is1\text{-}1}(R)\ \&\ \mathrm{M}x,P\ \&\ \forall u(Pu \Rightarrow \mathrm{M}y,\{v : Ru,v\})\\ &\&\ \mathrm{M}z,\{v : \exists u\ (Pu\ \&\ Ru,v)\}\ ) \end{aligned}$$

□

Prop 5.2. (*Zero, Left*) $\forall x\ (\ \mathrm{N}x \Rightarrow *(0,x,0)\ )$
Pf:

Assume $\mathrm{N}x$. $\mathrm{M}0,\phi$ by (F2). Vacuously, $\forall u(\phi u \Rightarrow \mathrm{M}x,\{v : \phi u,v\})$. (Remark: the first instance of ϕ is one-place and the second is two-place.) Also vacuously, $\mathit{Is1\text{-}1}(\phi)$. Finally, $\{v :\ \exists u\ (\phi u\ \&\ \phi u,v)\} \equiv \phi$, so by (F2), $\mathrm{M}0,\{v :\ \exists u\ (\phi u\ \&\ \phi u,v)\}$. Hence by *Def 5.1*, $*(0,x,0)$.

□

Prop 5.3. $\forall n\forall y\forall m\forall a\forall b\ (\ *(n,y,a)\ \&\ (a + y) = b\ \&\ \mathrm{N}m\ \&\ \sigma n,m \Rightarrow *(m,y,b)\ )$
Pf:

Assume $*(n,y,a)\ \&\ (a + y) = b\ \&\ \mathrm{N}m\ \&\ \sigma n,m$. Then by *Defs 5.1 and 4.11,* $\mathrm{N}n\ \&\ \mathrm{N}y\ \&\ \mathrm{N}a\ \&\ \mathrm{N}b$ and for some P,R,A,B

$$\begin{aligned} &\mathit{Is1\text{-}1}(R)\ \&\ \mathrm{M}n,P\ \&\ \forall u(Pu \Rightarrow \mathrm{M}y,\{v : Ru,v\})\ \&\\ &\mathrm{M}a,\{v :\ \exists u\ (Pu\ \&\ Ru,v)\} \end{aligned}$$

and

$$(A \cap B) \equiv \phi\ \&\ \mathrm{M}a,A\ \&\ \mathrm{M}y,B\ \&\ \mathrm{M}b,(A \cup B).$$

By *POTINF* (*Theorem 2.24*), there exists p s.t. $\neg\ Pp$. Using predicative comprehension, set P' to $(P \cup \{p\})$. By (F3) $\mathrm{M}m,P'$. Now both $\{v :\ \exists u\ (Pu\ \&\ Ru,v)\}$ and A number a, so by *Finite Hume's Principle* (*Prop 2.3*), $\{v :\ \exists u\ (Pu\ \&\ Ru,v)\} \sim A$. Hence for some S, S is a one-to-one function onto A with domain $\{v :\ \exists u\ (Pu\ \&\ Ru,v)\}$. Evidently, $\{v : \exists u\ (Pu\ \&\ (R \circ S)u,v)\} \equiv A$. Using predicative comprehension, set R' to

$$\{u,v : (Pu\ \&\ (R \circ S)u,v) \vee (u = p\ \&\ Bv)\}.$$

Because R and S are one-to-one, so is $(R \circ S)$. But A and B are disjoint, and $\neg\ Pp$, so R' is also one-to-one.

Assume $P'u$. So either Pu or $u = p$. Suppose Pu. Then $\mathrm{M}y,\{v : Ru,v\}$. But S correlates $\{v : Ru,v\}$ with $\{v : (R \circ S)u,v\}$, so $\mathrm{M}y,\{v : (R \circ S)u,v\}$ by *Finite Hume's Principle*. $\neg\ p = u$ since Pu. So

$$\{v : (R \circ S)u,v\} \equiv \{v : (Pu\ \&\ (R \circ S)u,v) \vee (u = p\ \&\ Bv)\},$$

and thus $\{v : (R \circ S)u,v\} \equiv \{v : R'u,v\}$. So $\mathrm{M}y,\{v : R'u,v\}$. Similar reasoning shows that $\mathrm{M}y,\{v : R'u,v\}$ when $u = p$.

Finally, it is easy to see that $\{v : \exists u\ (Pu\ \&\ R'u,v)\} \equiv (A \cup B)$, so by *Corollary 2.4*,

$\mathrm{M}b,\{v : \exists u\,(Pu \mathbin{\&} R',v)\}$.

Putting all this together, it can be concluded that $*(m,y,b)$. □

Prop 5.4. $\forall n \forall y \forall z \forall m\,(\,*(m,y,z) \mathbin{\&} \mathrm{N}n \mathbin{\&} \sigma n,m \Rightarrow \exists b\,(*(n,y,b) \mathbin{\&} (b+y)=z\,)$

Pf:

Assume $*(m,y,z) \mathbin{\&} \mathrm{N}n \mathbin{\&} \sigma n,m$. Then by *Def 5.1*, $\mathrm{N}m \mathbin{\&} \mathrm{N}y \mathbin{\&} \mathrm{N}z$ and for some P,R

$$Is1\text{-}1(R) \mathbin{\&} \mathrm{M}m,P \mathbin{\&} \forall u(Pu \Rightarrow \mathrm{M}y,\{v : Ru,v\}) \mathbin{\&} \mathrm{M}z,\{v : \exists u\,(Pu \mathbin{\&} Ru,v)\}.$$

By (PA6) (*Corollary 2.25*), $\neg\, m = 0$. By *Prop 2.1*, Pp for some p. Set P' to $(P \setminus \{p\})$ and R' to $(R \lceil P')$. By (F3) $\mathrm{M}n,P'$. Evidently, $Is1\text{-}1(R')$ and $\forall u(P'u \Rightarrow \mathrm{M}y,\{v : R'u,v\})$. Also,

$$\{v : \exists u\,(P'u \mathbin{\&} R'u,v)\} \subseteq \{v : \exists u\,(Pu \mathbin{\&} Ru,v)\},$$

so by *Prop 4.4*, $\mathrm{M}b,\{v : \exists u\,(P'u \mathbin{\&} R'u,v)\}$ for some b s.t. $\mathrm{N}b$. Hence, $*(n,y,b)$.

But also

$$\{v : \exists u\,(Pu \mathbin{\&} Ru,v)\} \equiv \{v : \exists u\,(P'u \mathbin{\&} R'u,v)\} \cup \{v : Rp,v\}$$

and, because R is one-to-one,

$$\{v : \exists u\,(P'u \mathbin{\&} R'u,v)\} \cap \{v : Rp,v\} \equiv \phi.$$

Since $\mathrm{M}y,\{v : Rp,v\}$, one can conclude that $(b+y)=z$. □

Prop 5.5. (*Zero, Right*). $\forall x\,(\,\mathrm{N}x \Rightarrow *(x,0,0)\,)$

Pf:

Proceed by induction (F4*), with ϕ as $*(n,0,0)$.

If N0, then $*(0,0,0)$ by *Prop 5.2*.

Now assume $\mathrm{N}n \mathbin{\&} \mathrm{N}m \mathbin{\&} \sigma n,m \mathbin{\&} \neg\, m=0 \mathbin{\&} \phi$. Then N0 by *Prop 1.1*, so $(0+0)=0$ by *Prop 4.14a*. Hence $*(n,0,0) \mathbin{\&} (0+0)=0 \mathbin{\&} \mathrm{N}m \mathbin{\&} \sigma n,m$. By *Prop 5.3*, $*(m,0,0)$. □

Prop 5.6. (*Uniqueness*) $\forall x \forall y \forall a \forall b\,(\,*(x,y,a) \mathbin{\&} *(x,y,b) \Rightarrow a=b\,)$

Pf:

Proceed by induction (F4*), with ϕ as

$$\forall y \forall a \forall b\,(\,*(n,y,a) \mathbin{\&} *(n,y,b) \Rightarrow a=b\,).$$

Suppose $*(0,y,a) \mathbin{\&} *(0,y,b)$. The first conjunct implies, by *Def 5.1*, that for some P,R,

$$Is1\text{-}1(R) \mathbin{\&} \mathrm{M}0,P \mathbin{\&} \forall u(Pu \Rightarrow \mathrm{M}y,\{v : Ru,v\}) \mathbin{\&} \mathrm{M}a,\{v : \exists u\,(Pu \mathbin{\&} Ru,v)\}.$$

But then $P \equiv \phi$ by (F2), so evidently $\{v : \exists u\,(Pu \mathbin{\&} Ru,v)\} \equiv \phi$. By *Prop 2.1*, $a=0$. Similar reasoning shows that $b=0$. Thus $a=b$.

Now assume $\mathrm{N}n \mathbin{\&} \mathrm{N}m \mathbin{\&} \sigma n,m \mathbin{\&} \neg\, m=0 \mathbin{\&} \phi$. And suppose $*(m,y,a) \mathbin{\&} *(m,y,b)$. By *Prop 5.4*, $*(n,y,c) \mathbin{\&} (c+y)=a$ and $*(n,y,d) \mathbin{\&} (d+y)=b$, for some c,d. By the inductive hypothesis, $c=d$. By *Uniqueness for Addition* (*Prop 4.12*), $a=b$. □

From now on, as happened with addition, use $(x * y)$ to refer to that z (if it exists) such that $*(x,y,z)$, guaranteed to be unique by the previous proposition. Versions of *Props 5.2* to *5.5*, where a multiplication term rather than predicate is used, will be assumed.

Notice that if $(x * y)$ exists, then $\mathrm{N}(x * y)$.

Prop 5.7. $\forall x\ ((x * y) = 0 \Rightarrow x = 0 \vee y = 0)$
Pf:
Assume $(x * y) = 0$. Then by *Def 5.1*, Ny & Nz, and for some P,R

$$Is1\text{-}1(R)\ \&\ \mathrm{M}m,P\ \&\ \forall u(Pu \Rightarrow \mathrm{M}y,\{v : Ru,v\})\ \&\ \mathrm{M}0,\{v : \exists u\ (Pu\ \&\ Ru,v)\}.$$

By (F2) $\{v :\ \exists u\ (Pu\ \&\ Ru,v)\} \equiv \phi$. Suppose neither x nor y is zero. Then $\neg\ P \equiv \phi$ and $\neg\ R \equiv \phi$, by *Prop 2.1*. But then $\neg\ \{v : \exists u\ (Pu\ \&\ Ru,v)\} \equiv \phi$, a contradiction. □

Prop 5.8.

a. $\forall n \forall 1\ (\ \mathrm{N}n\ \&\ one(1) \Rightarrow (1 * n) = n\ )$

b. $\forall x \forall y \forall 1\ (\ one(1)\ \&\ (x * y) = 1 \Rightarrow x = 1\ \&\ y = 1\ )$

Pf:

a. Assume Nn & $one(1)$. By *POTINF* (*Theorem 2.24*), there exists P,Q s.t. M1,P and Mn,Q. By *Prop 4.7*, $P \equiv \{a\}$. Using predicative comprehension, set R to $\{x,y : x = a\ \&\ Qy\}$. Clearly $Is1\text{-}1(R)$ and $\forall u(Pu \Rightarrow \{v : Ru,v\} \equiv Q)$. Also, $\{v : \exists u\ (Pu\ \&\ Ru,v)\} \equiv Q$. So by *Corollary 2.4*, $\forall u(Pu \Rightarrow \mathrm{M}n,\{v : Ru,v\})$ and $\mathrm{M}n,\{v : \exists u\ (Pu\ \&\ Ru,v)\}$. Hence $(1 * n) = n$.

b. Assume $one(1)\ \&\ (x * y) = 1$. By *Prop 4.6*, $\neg\ (x * y) = 0$. By *Props 5.2* and *5.5*, $\neg\ x = 0$ and $\neg\ y = 0$. By *Def 5.1*, Nx & Ny and for some P,R

$$Is1\text{-}1(R)\ \&\ \mathrm{M}x,P\ \&\ \forall u(Pu \Rightarrow \mathrm{M}y,\{v : Ru,v\})\ \&\ \mathrm{M}1,\{v : \exists u\ (Pu\ \&\ Ru,v)\}.$$

By *Prop 4.7*,

$$(*)\ \{v : \exists u\ (Pu\ \&\ Ru,v)\} \equiv \{b\} \text{ for some } b.$$

Then, $Pa\ \&\ Ra,b$ for some a. Suppose Pc for some c where $\neg\ c = a$. Then $\mathrm{M}y,\{v : Rc,v\}$, so $\neg\ \{v : Rc,v\} \equiv \phi$ by *Prop 2.1*. But then Rc,d for some d, and $\neg\ d = b$ since $Is1\text{-}1(R)$. This contradicts (*). So $P \equiv \{a\}$, and by *Prop 4.7* and (F1), $x = 1$.

If $\neg\ y = 1$, then $\{v : Ra,v\}$ contains at least one other thing other than b, by *Prop 4.7* and (F1), say e. But this again contradicts (*). So $y = 1$ as well. □

Prop 5.9. (*Distributive Laws*)

a. $\forall n\forall x\forall y\forall a\ (\ ((x + y) * n) = a \Rightarrow ((x * n) + (y * n)) = a\ )$

b. $\forall n\forall x\forall y\forall a\ (\ (n * (x + y)) = a \Rightarrow ((n * x) + (n * y)) = a\ )$

c. $\forall n\forall x\forall y\forall a\ (\ ((n * x) + (n * y)) = a\ \&\ \neg\, n = 0 \Rightarrow (n * (x + y)) = a\ )$

Note: In (*c*) "$\neg\, n = 0$" is needed, since one may have $((0 * x) + (0 * y)) = 0$ without $(x + y)$ existing.

Pf:

a. Assume $((x + y) * n) = a$. Then by *Def 5.1*, $\mathrm{N}(x + y)\ \&\ \mathrm{N}n\ \&\ \mathrm{N}a$ and for some C,R

$$\begin{aligned}&Is1\text{-}1(R)\ \&\ \mathrm{M}(x + y),P\ \&\ \forall u(Pu \Rightarrow \mathrm{M}n,\{v : Ru,v\})\\ &\&\ \mathrm{M}a,\{v :\ \exists u\ (Pu\ \&\ Ru,v)\}.\end{aligned}$$

So by *Def 4.11*, $\mathrm{N}x\ \&\ \mathrm{N}y$ and for some X,Y

$$(X \cap Y) \equiv \phi\ \&\ \mathrm{M}x,X\ \&\ \mathrm{M}y,Y\ \&\ \mathrm{M}(x + y),(\mathrm{X} \cup Y).$$

By *Finite Hume's Principle* (*Prop 2.3*), $P \sim (X \cup Y)$. By logic, there are X' and Y' s.t. $X' \sim X$, $Y' \sim Y$, $(X' \cap Y') \equiv \phi$, and $(X' \cup Y') \equiv P$. By *Finite Hume's Principle* again, $\mathrm{M}x,X'$. $\forall u(X'u \Rightarrow \mathrm{M}n,\{v : Ru,v\})$ since $X' \subseteq P$. Evidently,

$$\{v : \exists u\ (X'u\ \&\ Ru,v)\} \subseteq \{v : \exists u\ (Pu\ \&\ Ru,v)\},$$

so by *Prop 4.4*, $\mathrm{M}b,\{v :\ \exists u\ (X'u\ \&\ Ru,v)\}$ for some b where $\mathrm{N}b$. By *Def 5.1*, $(x * n) = b$. Similarly, $(y * n) = c$ for some c s.t. $\mathrm{N}c\ \&\ \mathrm{M}c,\{v : \exists u\ (Y'u\ \&\ Ru,v)\}$. Evidently,

$$\{v :\ \exists u\ (X'u\ \&\ Ru,v)\}\ \cap \{v : \exists u\ (Y'u\ \&\ Ru,v)\}) \equiv \phi$$

and

$$\{v :\ \exists u\ (X'u\ \&\ Ru,v)\}\ \cup \{v : \exists u\ (Y'u\ \&\ Ru,v)\}) \equiv \{v : \exists u\ (Pu\ \&\ Ru,v)\}.$$

By *Def 4.11*, $(b + c) = a$. Thus $((x * n) + (y * n)) = (b + c) = a = ((x + y) * n)$.

b. Proceed by induction (F4*), with ϕ as

$$\forall x\forall y\forall a\ (\ (n * (x + y)) = a \Rightarrow ((n * x) + (n * y)) = a\ ).$$

Case n = 0. Assume $(0 * (x + y)) = a$. By *Prop 5.2*, $a = 0$ and $(0 * x) = (0 * y) = 0$. By *Def 5.1*, N0. By *Prop 4.14a*, $(0 + 0) = 0$. Hence $((0 * x) + (0 * y)) = a$.

Induction step. Assume $\mathrm{N}n\ \&\ \mathrm{N}m\ \&\ \sigma n,m\ \&\ \neg\, m = 0\ \&\ \phi$. And suppose $(m * (x + y)) = a$. By *Prop 5.4*, $(n * (x + y)) = b\ \&\ (b + (x + y)) = a$ for some b. So

$$\begin{aligned}a &= (b + (x + y))\\ &= ((n * (x + y)) + (x + y))\\ &= (((n * x) + (n * y)) + (x + y) && \text{by the induction hypothesis}\\ &= (((n * x) + x) + ((n * y) + y)) && \text{by } \textit{Additive Commutativity}\\ & && \text{and } \textit{Associativity}\\ &= ((m{*}x) + (m{*}y)) && \text{by } \textit{Prop 5.3}.\end{aligned}$$

c. Proceed by induction (F4*), with ϕ as

$$\forall x \forall y \forall a\ (\ ((n * x) + (n * y)) = a\ \&\ \neg\ n = 0 \Rightarrow (n * (x + y)) = a\ )$$

Case n = 0. Trivial.

Induction step. Assume $\mathrm{N}n\ \&\ \mathrm{N}m\ \&\ \sigma n{,}m\ \&\ \neg\ m = 0\ \&\ \phi$. And suppose $((m * x) + (m * y)) = a\ \&\ \neg\ m = 0$. By *Prop 5.4*, $(m * x) = ((n * x) + x)$ and $(m * y) = ((n * y) + y)$.

Suppose $n = 0$. Then $one(m)$ by *Def 1.5*. By *Prop 5.8a*, $(m * x) = x$ and $(m * y) = y$. So $(x + y) = a$, and $(m * (x + y)) = (m * a) = a$, again by *Prop 5.8a*.

Otherwise, $\neg\ n = 0$. Then

$$\begin{aligned}
&((m * x) + (m * y)) \\
&\quad = (\ ((n * x) + x) + ((n * y) + y)\ ) \\
&\quad = (\ ((n * x) + (n * y)) + (x + y)\ ) && \text{by } \textit{Additive Associativity} \\
& && \text{and } \textit{Commutativity} \\
&\quad = (\ (n * (x + y)) + (x + y)\ ) && \text{by the induction hypothesis} \\
&\quad = (m * (x + y)) && \text{by } \textit{Prop 5.3}.
\end{aligned}$$

□

Prop 5.10. $\forall x \forall y \forall z \forall a\ (\ ((y * x) + y) = a\ \&\ \sigma x{,}z \Rightarrow (y * z) = a\ )$

Pf:

Proceed by induction (F4*), with ϕ as

$$\forall x \forall z \forall a\ (\ ((n * x) + n) = a\ \&\ \sigma x{,}z \Rightarrow (n * z) = a\ ).$$

Assume $((0 * x) + 0) = a$. By *Prop 5.2* and *Prop 4.14a*, $a = 0$. But $(0 * z) = 0$ by *Prop 5.2* again.

Now assume $\mathrm{N}n\ \&\ \mathrm{N}m\ \&\ \sigma n{,}m\ \&\ \neg\ m = 0\ \&\ \phi$. And suppose $((m * x) + m) = a\ \&\ \sigma x{,}z$. By *Prop 5.4*, $(m * x) = ((n * x) + x)$, hence $(((n * x) + x) + m) = a$. By *Prop 4.9*, $one(1)$ for some 1. By *Prop 4.20b*, $(x + 1) = z$ and $(n + 1) = m$. So $(((n * x) + x) + (n + u)) = a$. By *Additive Associativity* and *Commutativity*, $(((n * x) + n) + (x + u)) = a$, hence $(((n * x) + n) + z) = a$. By the induction hypothesis, $((n * x) + n) = (n * z)$, so $((n * z) + z) = a$. By *Prop 5.3*, $(m * z) = a$. □

Prop 5.11. (*Commutative Law*). $\forall x \forall y \forall z\ (\ (x * y) = z \Rightarrow (y * x) = z\ )$

Note: From now on, as with addition, propositions will only state one form of commutative permutations, and assume the rest as granted.

Pf:

Proceed by induction (F4*), with ϕ as

$$\forall y \forall z\ (\ (n * y) = z \Rightarrow (y * n) = z\ ).$$

Assume $(0 * y) = z$. Then $(y * 0) = 0 = z$ by *Props 5.2* and *5.5*.

Now assume $\mathrm{N}n\ \&\ \mathrm{N}m\ \&\ \sigma n{,}m\ \&\ \neg\ m = 0\ \&\ \phi$. And suppose $(m * y) = z$. Then by *Prop 5.4*, $((n * y) + y) = z$. By the induction hypothesis, $(n * y) = (y * n)$, so $z = ((y * n) + y)$. By *Prop 5.10*, $(y * m) = z$. □

Prop 5.12 (*Associative Laws*).

a. $\forall x \forall y \forall z \forall a$ ($((x * y) * z) = a$ & $\neg$ x = 0 $\Rightarrow (x * (y * z)) = a$)

b. $\forall x \forall y \forall z \forall a$ ($((0 * y) * z) = a$ & $(y * z) = x \Rightarrow (0 * (y * z)) = a$)

c. $\forall x \forall y \forall z \forall a$ ($(x * (y * z)) = a$ & $\neg\, z = 0 \Rightarrow ((x * y) * z) = a$)

d. $\forall x \forall y \forall z \forall a$ ($(x * (y * 0)) = a$ & $(x * y) = z \Rightarrow$ ((x*y)*0 = a)

Note: It would obviously have been preferable to combine the first two assertions (*a* and *b*) into one, as

$$\forall x \forall y \forall z \forall a \text{ (} ((x * y) * z) = a \Rightarrow (x * (y * z)) = a \text{)}$$

Unfortunately, this assertion does not hold since the assumption that $((0 * y) * z) = a$ does not ensure that $(y * z)$ exists, because $(y * z)$ is usually a bigger number than any number appearing in $((0 * y) * z) = a$. So the assertion must be broken up into two parts, *a*, where *x* is non-zero so that the existence of $(y * z)$ in fact follows from the assumption of the existence of $((x * y) * z)$, and *b*, where *x* is 0 and the assumption of the existence of $(y * z)$ is made explicitly.

Pf:

a. Proceed by induction (F4*), with ϕ as

$$\forall y \forall z \forall a \text{ (} ((n * y) * z) = a \text{ \& } \neg\, n = 0 \Rightarrow (n * (y * z)) = a \text{).}$$

Case n = 0. Trivial.

Induction step. Assume Nn & Nm & σn,m & ¬ m = 0 & ϕ. And suppose $((m * y) * z) = a$ & $\neg\, m = 0$.

Suppose $n = 0$. Then *one*(*m*) by *Def 1.5* and so by *Prop 5.8a*, $(m * y) = y$. So $a = ((m * y) * z) = (y * z)$. But then by *Prop 5.8a* again, $(m * (y * z)) = (y * z) = a$.

Now suppose $\neg\, n = 0$. By *Prop 5.4*, $(m * y) = ((n * y) + y)$. By *Prop 5.9a*,

$$(((n * y) + y) * z) = (((n * y) * z) + (y * z)).$$

By the induction hypothesis,

$$((n * y) * z) = (n * (y * z)).$$

So

$$\begin{aligned}(m * (y * z)) &= ((n * (y * z)) + (y * z)) \\ &= (m * (y * z)) \qquad \text{by } \textit{Prop 5.3}.\end{aligned}$$

b. Assume $((0 * y) * z) = a$ & $(y * z) = x$. By two applications of *Prop 5.2*, $a = 0$. By another, $(0 * (y * z)) = 0$.

c. Assume $(x * (y * z)) = a$ & $\neg\, z = 0$. Then

$$\begin{aligned} a &= ((y * z) * x) && \text{by the } \textit{Commutative Law } (\textit{Prop 5.11}) \\ &= ((z * y) * x) && \text{by the } \textit{Commutative Law} \\ &= (z * (y * x)) && \text{by } (a) \\ &= ((y * x) * z) && \text{by the } \textit{Commutative Law} \\ &= ((x * y) * z) && \text{by the } \textit{Commutative Law} \end{aligned}$$

d. Analogous to the proof of (*c*). □

Prop 5.13. (*Cancellation*). $\forall x \forall y \forall z\ (\ (y * x) = (z * x)\ \&\ \neg\, x = 0 \Rightarrow y = z\ )$
Pf:

Proceed by induction (F4*), with ϕ

$$\forall x \forall z\ (\ (n * x) = (z * x)\ \&\ \neg\, x = 0 \Rightarrow n = z\ ).$$

Case $n = 0$. Assume $(0 * x) = (z * x)\ \&\ \neg\, x = 0$. Then $(0 * x) = 0$ by *Prop 5.2*. So by *Prop 5.7*, $z = 0$.

Induction step. Assume $\mathrm{N}n\ \&\ \mathrm{N}m\ \&\ \sigma n{,}m\ \&\ \neg\, m = 0\ \&\ \phi$. And suppose $(m * x) = (z * x)\ \&\ \neg\, x = 0$. By *Prop 5.4*, $(m * x) = ((n * x) + x)$. If $z = 0$, then $(z * x) = 0$ and so $(m * x) = 0$ using *Prop 5.2*, contradicting *Prop 5.7*. Hence $\neg\, z = 0$. By *Prop 1.2*, $\sigma z'{,}z$ for some z' s.t. $\mathrm{N}z'$. By *Prop 5.4*, $(z * x) = ((z' * x) + x)$. Thus

$$((n * x) + x) = ((z' * x) + x).$$

By *Cancellation for Addition* (*Prop 4.16*)

$$(n * x) = (z' * x).$$

By the induction hypothesis, $n = z'$. By (PA4), $m = z$. □

Corollary 5.14. $\forall x \forall u\ (\ (x * u) = x\ \&\ \neg\, x = 0 \Rightarrow \mathit{one}(u)\ )$
Pf:

Suppose $(x * u) = x\ \&\ \neg\, x = 0$. Then $\mathrm{N}x$, by *Def 5.1*. So by *Prop 4.9*, *one*(1) for some 1. By *Prop 5.8a*, $(x * 1) = x$. By *Prop 5.13, $z = 1$*. □

Prop 5.15.

a. $\forall x \forall y \forall z \forall a\ (\ x \leq y\ \&\ (y * z) = a \Rightarrow (x * z) \leq (y * z)\ ).$

b. $\forall x \forall y \forall z \forall a\ (\ \mathrm{N}z\ \&\ \neg\, z = 0\ \&\ x \leq y\ \&\ (y * z) = a \Rightarrow x \leq (y * z)\ ).$

c. $\forall x \forall x' \forall y \forall z \forall a\ (\ x \leq y\ \&\ x' \leq z\ \&\ (y * z) = a \Rightarrow (x * x') \leq (y * z)\ ).$

Pf:

a. Assume $x \leq y\ \&\ (y * z) = a$. So

$$(y * z) = ((x + x') * z) \qquad \text{for some } x' \text{ by } \textit{Prop 4.17}$$

$$= ((x * z) + (x' * z)) \qquad\qquad \text{by } \textit{Prop 5.9a}$$

Hence by *Prop 4.17* again, $(y * z) \geq (x * z)$.

b. Assume $\mathrm{N}z\ \&\ \neg\, z = 0\ \&\ x \leq y\ \&\ (y * z) = a$. $1 \leq z$, by *Prop 4.9*. $(x * 1) \leq (y * z)$ by (*a*). $x \leq (y * z)$, by *Prop 5.8a*.

c. Apply (*a*), *Commutativity of Multiplication* and *Transitivity of* ≤ (*Prop 4.5a*). □

Prop 5.16.

a. $\forall x \forall y \forall z\ (\ (x * z) \leq (y * z)\ \&\ \neg\, z = 0 \Rightarrow x \leq y\ )$

b. $\forall x \forall y \forall z \forall 1\ (\ \neg\, x = 0\ \&\ \textit{one}(1)\ \&\ 1 < y\ \&\ (x * y) = z\ \Rightarrow x < (x * y)\ )$

Pf:

a. Assume $(x * z) \leq (y * z)\ \&\ \neg\, z = 0$. Then by *Def 5.1*, $\mathrm{N}x\ \&\ \mathrm{N}y$, so by *Dichotomy* (*Prop 4.5b*), $x \leq y \vee y < x$.
Suppose $y < x$. By *Prop 5.15a*, $(y * z) \leq (x * z)$. By *Anti-Symmetry of* ≤ (*Prop 4.18*), $(x * z) = (y * z)$. By *Cancellation* (*Prop 5.13*), $x = y$, a contradiction.

b. Assume $\neg\, x = 0\ \&\ \textit{one}(1)\ \&\ 1 < y\ \&\ (x * y) = z$. Suppose $\neg\, x < (x * y)$. Then by *Dichotomy* (*Prop 4.5b*), $(x * y) \leq x$. By *Prop 5.8a*, $(x * y) \leq (x * 1)$. By (*a*), $y \leq 1$, contradicting *Anti-Symmetry* (*Prop 4.18*). □

Prop 5.17. (*Division Algorithm*)

a. (*Existence*). $\forall a \forall b\ (\ \mathrm{N}a\ \&\ \mathrm{N}b\ \&\ \neg\, b = 0 \Rightarrow \exists q \exists r\ (a = ((q * b) + r)\ \&\ r < b)\ )$

b. (*Uniqueness*). $\forall a \forall b \forall q \forall r \forall q' \forall r'\ (\ a = ((q * b) + r)\ \&\ r < b\ \&\ a = ((q' * b) + r')\ \&\ r' < b$
$\Rightarrow q = q'\ \&\ r = r')$

Pf:

a. Assume $\mathrm{N}a\ \&\ \mathrm{N}b\ \&\ \neg\, b = 0$. Let φ be the formula

$$\exists q\ a = ((q * b) + x).$$

Note first that $\exists x\ (\ \mathrm{N}x\ \&\ \varphi\ )$, since $a = ((\ 0 * b) + a)$ by *Props 5.2* and *4.14a*. By the *Well-Ordering Principle* (*Prop 4.22c*),

$$\mathrm{N}x\ \&\ \varphi\ \&\ \forall y\ (\ y < x \Rightarrow \neg\ \varphi\ [y\backslash x]\ )$$

for some x. Hence

$$a = ((q * b) + x)$$

for some q.
Suppose $\neg\, x < b$. By *Dichotomy* (*Prop 4.5b*), $b \leq x$. By *Prop 4.17*,

$(b + c) = x$ for some c. By *Prop 4.17* again, $c \leq x$. Because $\neg\, b = 0$, then $c < x$, by *Prop 4.14b*. Note that $one(1)$ for some 1 by *Prop 4.9*.

So

$$\begin{aligned} a &= ((q * b) + (b + c)) \\ &= (((q * b) + b) + c) && \text{by \textit{Associativity of Addition}} \\ &= (((q * b) + (1*b)) + \mathrm{c}) && \text{by \textit{Prop 5.8a}} \\ &= (((q + 1) * b) + c) && \text{by \textit{Prop 5.9c}.} \end{aligned}$$

But this contradicts $\forall y\ (\ y < x \Rightarrow \neg\ \varphi\,[y\backslash x]\ )$. Therefore $x < b$.

b. Assume $\neg\, b = 0$ & $a = ((q * b) + r)$ & $r < b$ & $y = ((q' * b) + r')$ & $r' < b$.

Suppose $\neg\, q = q'$. WLOG by *Dichotomy*, suppose $q < q'$. Then $(q + x) = q'$ by *Prop 4.17*, for some x where $\neg\, x = 0$ by *Prop 4.14a*. Then

$$\begin{aligned} a &= (((q + x) * b) + r') \\ &= (((q * b) + (x * b)) + r') && \text{by the \textit{Distributive Law}} \\ &= ((q * b) + ((x * b) + r')) && \text{by \textit{Associativity of Addition}} \end{aligned}$$

By *Cancellation* (*Prop 4.16*), $r = ((x * b) + r')$. But $one(1)$ for some 1 by *Prop 4.9*. Also, note $0 \leq r'$, by *Props 4.14a* and *4.17*. So

$$\begin{aligned} b &\leq (x * b) && \text{by \textit{Prop 5.15b}} \\ &\leq ((x * b) + r') && \text{by \textit{Props 4.14a}, \textit{4.19}, and} \\ & && \text{\textit{Transitivity of} } \leq \\ &\leq r. \end{aligned}$$

But recall $r < b$, so this contradicts *Anti-Symmetry of* $\leq$ (*Prop 4.18*). Thus $q = q'$. By *Cancellation* (*Prop 4.16*), $r = r'$. □

6. Division and Prime Numbers

6A. Definition of Division and Elementary Propositions

Def 6.1. $x \mid y$ abbreviates $\exists z\ (x * z) = y$. □

Prop 6.2.

a. $\forall x\ (\ \mathrm{N}x \Rightarrow x \mid 0\ )$

b. $\forall x\ (\ \mathrm{N}x \Rightarrow x \mid x\ )$

c. $\forall \mathrm{x} \forall 1\ (\ \mathrm{N}x\ \&\ one(1) \Rightarrow 1 \mid x\ )$

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

Pf:

a. Let Nx. $(x * 0) = 0$, by *Prop 5.5*.

b. Let Nx. If $x = 0$, then use (*a*). Otherwise, suppose $\neg\ x = 0$. By *Prop 4.9*, there exists 1 such that *one*(1). By *Prop 5.8*, $(x * 1) = x$.

c. Nx & *one*(1). By *Prop 5.8*, $(1 * x) = x$.

d. Suppose $0 \mid x$. By *Def 6.1*, $(0 * z) = x$, for some z. By *Prop 5.2*, $x = 0$. □

Prop 6.3. $\forall x \forall y\ (\ x \mid y\ \&\ \neg\ y = 0 \Rightarrow x \leq y\ )$
Pf:
Let $x \mid y\ \&\ \neg\ y = 0$. By *Def 6.1* $(x * z) = y$, for some z. $\neg\ z = 0$, by *Prop 5.5*. By *Prop 5.15b*, $x \leq (x * z)$. □

Prop 6.4.

a. (*Anti-Symmetry*) $\forall x \forall y\ (\ x \mid y\ \&\ y \mid x \Rightarrow x = y\ )$

b. (*Transitivity*) $\forall x \forall y \forall z\ (\ x \mid y\ \&\ y \mid z \Rightarrow x \mid z\ )$

Pf:

a. Let $x \mid y\ \&\ y \mid x$. Then by *Def 6.1*, $(x * z) = y$ and $(y * z') = x$, for some z, z'. Then $x = ((x * z) * z')$. If $x = 0$, then $y = 0$, by *Prop 5.2*, so $x = y$. Otherwise, suppose $\neg\ x = 0$. Then by the *Associative Law for Multiplication* (*Prop 5.12a*), $x = (x * (z * z'))$. By *Cancellation*, *one*$(z * z')$. By *Prop 5.8b*, $z = 1$. By *Prop 5.8a*, $x = y$.

b. Let $x \mid y$ & $y \mid z$. Then by *Def 6.1*, $(x * a) = y$ and $(y * b) = z$, for some a, b. Then $z = ((x * a) * b)$. If $x = 0$, then $y = 0$, so $z = 0$ by *Prop 5.2*; in which case $x \mid z$ by *Prop 6.2*. Otherwise, suppose $\neg\, x = 0$. Then by the *Associative Law for Multiplication* (*Prop 5.12a*), $z = (x * (a * b))$. Thus $x \mid z$. □

Prop 6.5.

a. $\forall x \forall y \forall z \forall a \forall b \forall c\ (\, x \mid y\ \&\ x \mid z\ \&\ ((a * y) + (b * z)) = c \Rightarrow x \mid c\,)$

b. $\forall x \forall y \forall z \forall a \forall b \forall c\ (\, x \mid y\ \&\ x \mid z\ \&\ ((b * z) + c) = (a * y) \Rightarrow x \mid c\,)$

Pf:

a. Assume $x \mid y$ & $x \mid z$ & $((a * y) + (b * z)) = c$.

If $x = 0$, then $y = 0$ and $z = 0$, by *Prop 6.2d*; by *Props 5.5* and *4.14a*, $c = 0$; and so by *Prop 6.2a*, $x \mid c$.

Otherwise, $\neg\, x = 0$. By *Def 6.1*, $(x * u) = y$ and $(x * v) = z$, for some u,v. So

$$\begin{aligned} c &= ((a * (x * u)) + (b * (x * v))) \\ &= (\, ((x * u) * a) + ((x * v) * b)\,) && \text{by } \textit{Commutativity of } * \\ &= (\, (x * (u * a)) + (x * (v * b))\,) && \text{by } \textit{Associativity of } * \text{ (since } \neg\, x = 0) \\ &= (\, (\, x * ((u * a) + (v * b))\,)\,) && \text{by } \textit{Distributive Law} \end{aligned}$$

Hence $x \mid c$.

b. Assume $x \mid y$ & $x \mid z$ & $((b * z) + c) = (a * y)$.

If $x = 0$, then $y = 0$ and $z = 0$, by *Prop 6.2d*; $c = 0$ by *Prop 4.14c*; and so $x \mid c$ by *Prop 6.2a*.

Otherwise, $\neg\, x = 0$. Now $(x * u) = y$ and $(x * v) = z$ for some u,v, by *Def 6.1*. Substituting,

$$((b * (x * v)) + c) = (a * (x * u)).$$

Applying *Commutativity* and (since $\neg\, x = 0$) *Associativity of Multiplication*,

$$((x * (b * v)) + c) = (x * (a * u)).$$

By *Prop 4.17*, $(x * (b * v)) \leq (x * (a * u))$. Since $\neg\, x = 0$, by *Prop 5.16a*, $(b * v) \leq (a * u)$, so by *Prop 4.17* in the other direction, $((b * v) + w) = (a * u)$. Substitute, distribute, cancel, to get

$$c = (x * w).$$

Thus $x \mid c$. □

6B. The Greatest Common Divisor.

Prop 6.6. (*Existence and Uniqueness of a Greatest Common Divisor*). Let Na & Nb & $(\neg\, a = 0 \vee \neg\, b = 0)$. Then, there exists some z such that,

$$z \mid a \;\&\; z \mid b \;\&\; \forall c\,(\, c \mid a \;\&\; c \mid b \Rightarrow c \leq z\,).$$

If $z' \mid a \;\&\; z' \mid b \;\&\; \forall c\,(\, c \mid a \;\&\; c \mid b \Rightarrow c \leq z'\,)$, then $z' = z$.
Pf:

Suppose $a = 0$. Then $\neg\, b = 0$. Then $b \mid a$ by *Prop 6.2a*, and $b \mid b$ by *Prop 6.2b*. If $c \mid a \;\&\; c \mid b$, then $c \leq b$ by *Prop 6.3*. So set z to b. By symmetry, similar reasoning succeeds in the case $b = 0$.

Now suppose $\neg\, a = 0 \;\&\; \neg\, b = 0$. Set φ to

$$(x \mid a \;\&\; x \mid b),$$

and set n to a. Then by *Prop 6.3*, $\forall x\,(\varphi \Rightarrow x \leq n)$. By *Prop 4.9*, *one*(1) for some 1. By *Prop 6.2c*, $1 \mid a \;\&\; 1 \mid b$. So $\exists x\, \varphi$. By *Prop 4.23* (and a change of variables), there exists z s.t. $z \mid a \;\&\; z \mid b \;\&\; \forall c\,(\, c \mid a \;\&\; c \mid b \Rightarrow c \leq z\,)$.

Finally, suppose $z' \mid a \;\&\; z' \mid b \;\&\; \forall c\,(\, c \mid a \;\&\; c \mid b \Rightarrow c \leq z'\,)$. Then both $z \leq z'$ and $z' \leq z$. By *Anti-Symmetry of* $\leq$ (*Prop 6.4a*), $z' = z$. □

Def 6.7. Suppose Na & Nb & $(\neg\, a = 0 \vee \neg\, b = 0)$. Use $(a \,\Delta\, b)$ to refer to that unique z guaranteed to exist by the previous proposition. □

Prop 6.8.

a. (*Commutativity*) $\forall x \forall y\,(\mathrm{N}x \;\&\; \mathrm{N}y \;\&\; (\neg\, x = 0 \vee \neg\, \mathrm{y} = 0) \Rightarrow (x \,\Delta\, y) = (y \,\Delta\, x))$

Note: As usual, from now on, only one form of commutative permutations will be asserted, and the rest will be assumed.

b. $\forall x \forall y\, \neg\,(x \,\Delta\, y) = 0$

c. $\forall x \forall y\,(\, \mathrm{N}x \;\&\; \mathrm{N}y \;\&\; (\neg\, x = 0 \vee \neg\, y = 0) \Rightarrow (x \,\Delta\, y) \mid x\,)$

d. $\forall x \forall y\,(\, \mathrm{N}x \;\&\; \mathrm{N}y \;\&\; (\neg\, x = 0 \vee \neg\, y = 0) \Rightarrow (x \,\Delta\, y) \leq x\,)$

e. $\forall x \forall y\,(\, \neg\, x = 0 \;\&\; x \mid y \Rightarrow (x \,\Delta\, y) = x\,)$

f. $\forall x \forall y \forall z \forall a \forall b\,(\, (\neg\, x = 0 \vee \neg\, y = 0) \;\&\; ((a * x) + (b * y)) = z \Rightarrow (x \,\Delta\, y) \mid z\,)$

g. $\forall x \forall y \forall z \forall a \forall b\,(\, (\neg\, x = 0 \vee \neg\, y = 0) \;\&\; ((a * x) + z) = (b * y) \Rightarrow (x \,\Delta\, y) \mid z\,)$

h. $\forall q \forall r \forall a \forall b\,(\, \neg\, b = 0 \;\&\; a = ((q * b) + r) \Rightarrow (a \,\Delta\, b) = (b \,\Delta\, r)\,)$

i. $\forall x\,(\, \mathrm{N}x \Rightarrow (x \,\Delta\, 0) = x\,)$

j. $\forall x \forall 1\,(\, \mathrm{N}x \;\&\; one(1) \Rightarrow (x \,\Delta\, 1) = 1\,)$

k. $\forall x \forall y \forall z\,(\, z \mid x \;\&\; z \mid y \;\&\; (\neg\, x = 0 \vee \neg\, y = 0) \Rightarrow z \mid (x \,\Delta\, y)\,)$

l. $\forall x \forall y \forall a \forall b \forall 1(\, (a * (x \,\Delta\, y)) = x \;\&\; (b * (x \,\Delta\, y)) = y \;\&\; one(1) \Rightarrow (a \,\Delta\, b) = 1\,)$

Pf:

b. Suppose $(x \Delta y) = 0$. By *Def 6.7*, $\neg x = 0 \vee \neg \mathrm{y} = 0$. By *Prop 4.9*, *one*(1) for some 1. By *Prop 6.2c*, $1 \mid x$ and $1 \mid y$. By *Def 6.7*, $1 \leq (x \Delta y)$, hence $1 \leq 0$, contradicting *Prop 4.6* and *Anti-Symmetry of* ≤ (*Prop 4.18*).

f. Assume $(\neg x = 0 \vee \neg y = 0)$ & $((a * x) + (b * y)) = z$. Then $(x \Delta y) \mid x$ and $(x \Delta y) \mid y$ by (*c*). The result follows from *Prop 6.5a*.

h. Assume $\neg b = 0$ & $a = ((q * b) + r)$. Then by *Prop 4.9*, *one*(1) for some 1. So $a = ((q * b) + (1 * r))$ by *Prop 5.8a*.. Then $(b \Delta r) \mid a$ by (*f*). By (*c*), $(b \Delta r) \mid b$. Now suppose $y \mid a$ & $y \mid b$. Again, $(1 * a) = ((q * b) + r)$. By *Prop 6.5b*, $y \mid r$. Thus, $y \leq (b \Delta r)$. Hence $(b \Delta r) = (a \Delta b)$.

k. Suppose not, that is suppose for some *x*,*z*

$$\neg\forall x\ (\ z \mid x\ \&\ z \mid y\ \&\ (\neg x = 0 \vee \neg y = 0) \Rightarrow z \mid (x \Delta y)\ )$$

By *Prop 4.22c* suppose *x* is the smallest number s.t.

$$z \mid x\ \&\ z \mid y\ \&\ (\neg x = 0 \vee \neg y = 0)\ \&\ \neg z \mid (x \Delta y).$$

If $x = 0$, then $\neg y = 0$, and $(x \Delta y) = y$ by (*c*); hence from $z \mid y$, conclude $z \mid (x \Delta y)$, a contradiction.

So suppose $\neg x = 0$. Then $y = ((q * x) + r)$ & $r < x$ for some *q*,*r*, by the *Division Algorithm* (*Prop 5.17a*). By *Prop 4.9*, *one*(1) for some 1, and $(1 * y) = y$ by *Prop 5.8a*. By *Prop 6.5b*, $z \mid r$. If $r = 0$, then $y = (q * x)$ by *Prop 4.14a*. Then by *Def 6.1*, $x \mid y$, and so by (*e*), $(x \Delta y) = x$, contradicting $\neg z \mid (x \Delta y)$ Hence $\neg r = 0$. By assumption of the leastness of *x*, $z \mid (\ x \Delta r)$. By (*h*), $z \mid (x \Delta y)$.

l. Assume $(a * (x \Delta y)) = x$ & $(b * (x \Delta y)) = y$. Then $(x \Delta y)$ exists, so one of *x* or *y* is non-zero. Hence one of *a* or b is non-zero, so $(a \Delta b)$ exists. The result follows now in the standard way. □

6C. A Few Other Numbers

As with the introduction of a special variable *1* to serve as argument of the predicate *one*, other special variables, *2*, *3*, and *4*, will be introduced to be arguments of the predicates *two*, *three*, and *four*, defined below.

Defs 6.9.

a. *two*(*u*) abbreviates: ∃1 (*one*(1) & N*u* & σ1,*u*).

b. *three*(*u*) abbreviates: ∃2 (*two*(2) & N*u* & σ2,*u*).

c. *four*(*u*) abbreviates: $\exists 3\ (\mathit{three}(3)\ \&\ \mathrm{N}u\ \&\ \sigma 3,u)$. □

It is not possible to prove (in **F**) that there are things 2, 3, and 4 s.t. *two*(2), *three*(3), or *four*(4). On the other hand, if there exists 2 s.t. *two*(2), then it has all the "downward" properties of two, including that it is preceded by a unique number one, which is the successor of 0. Similar remarks hold for *three* and *four*.

Prop 6.10. Suppose *two*(2). Then M2,*P* if and only if

$$\exists a \exists b\ (\neg\, a = b\ \&\ P \equiv \{a,b\}). \qquad \square$$

Prop 6.11. Suppose $P \equiv \{a,b\}$ for some *a*,*b* with $\neg\, a = b$, and suppose N*u*. Then *two*(*u*) if and only if M*u*,*P*. □

Prop 6.12. Let *one*(1) & *two*(2). Then $\neg\, 2 = 0\ \&\ \neg\, 2 = 1$. Indeed, $1 < 2$. □

Remark that, since the existence of some 1 where *one*(1) follows from the existence of there being a 2 such that *two*(2), the previous proposition could have been asserted in the following way:

> "Let *two*(2). Then there exists 1 such that *one*(1) and such that $\neg\, 2 = 0\ \&\ \neg\, 2 = 1\ \&\ 1 < 2$."

Prop 6.13. Suppose *two*(2) & $x < 2$. Then $x = 0 \vee$ *one*(x). □

Prop 6.14. Suppose N*n* & $\neg\, n = 0$ & $\neg$ *one*(*n*). Then ∃2 *two*(2) and indeed $2 \leq n$. □

Prop 6.15. Suppose *one*(1) & *two*(2). Then $(1 + 1) = 2$.
Pf:

By *Prop 4.6*, $\neg\, 0 = 1$. By *Prop 6.11*, M2,{0,1}. By *Prop 4.7*, M1,{0} and M1,{1}. By *Def 4.11*, $(1 + 1) = 2$. □

Similar propositions can be stated for *three* and *four* and indeed predicates for larger numbers. For instance (a proposition which actually will never be used):

Prop 6.16.

a. Supppose $\mathit{two}(2)$ & $\mathit{four}(4)$. Then $(2 + 2) = 4$.

b. Supppose $\mathit{four}(4)$. Then there exists 2 s.t. $\mathit{two}(2)$ and $(2 + 2) = 4$. □

6D. Prime Numbers

Def 6.17. $\pi(x)$ abbreviates:

$$\mathrm{N}x \;\&\; \neg\, x = 0 \;\&\; \neg\, \mathit{one}(x) \;\&\; \forall y\; (\, y \mid x \Rightarrow \mathit{one}(y) \vee y = x\,).$$

x is said to be *prime*. □

Note that in the previous definition, "$\neg\, x = 0$" is added among the conditions for primeness, which is not habitual. This is done because otherwise 0 would be prime in the special cases where only zero or only zero and one existed.

Prop 6.18. $\forall x \forall n\; (\, \pi(x) \;\&\; n \mid x \Rightarrow \mathit{one}(n) \vee n = x\,)$

Pf:

Assume $\pi(x)$ & $n \mid x$. Then $\mathrm{N}x \;\&\; \neg\, \mathit{one}(x) \;\&\; \neg\, x = 0$. Then by *Prop 4.9*, $\mathit{one}(1)$ for some 1. By *Def 6.17*, $n = 1 \vee n = x$. □

Prop 6.19.

a. $\forall 2\; (\, \mathit{two}(2) \Rightarrow \pi(2)\,)$

b. $\forall x \forall 2\; (\pi(x) \;\&\; \mathit{two}(2) \Rightarrow 2 \leq x\,)$

Pf:

a. Assume $\mathit{two}(2)$. By *Prop 6.12*, $\neg\, 2 = 0$ and $\neg\, \mathit{one}(2)$. Suppose $y \mid 2$. Then by *Prop 6.3*, $y \leq 2$. By *Prop 6.13*, $y = 0 \vee \mathit{one}(y) \vee y = 2$. But $y = 0$ contradicts *Prop 6.2d.*

b. Assume $\pi(x)$ & $\mathit{two}(2)$. By *Def 6.17*, $\neg\, x = 0 \;\&\; \neg\, \mathit{one}(x)$. By *Prop 6.14*, $2 \leq x$. □

Prop 6.20.

a. $\forall x\; (\, \mathrm{N}x \;\&\; \neg\, x = 0 \;\&\; \neg\, \mathit{one}(x) \Rightarrow \exists p\; (\pi(p) \;\&\; p \mid x)\,)$

b. $\forall x \forall y\ (\ \pi(x)\ \&\ \mathrm{N}y \Rightarrow \mathit{one}(x \Delta y) \vee (x \Delta y) = x\ )$

c. $\forall x \forall y\ (\ \pi(x)\ \&\ x \mid (x \Delta y) \Rightarrow x \mid y\ )$

d. $\forall x \forall y\ (\ \mathrm{N}x\ \&\ \mathrm{N}y\ \&\ (\neg\, x = 0 \vee \neg\, y = 0)\ \&\ \forall p(\pi(p)\ \&\ p \mid x \Rightarrow \neg\, p \mid y) \Rightarrow \mathit{one}(x \Delta y)\ )$

Pf:

a. WLOG by *Prop 4.22c*, suppose x is the least number s.t. $\mathrm{N}x\ \&\ \neg\, x = 0\ \&\ \neg\, \mathit{one}(x)$ but $\neg\, \exists y\ (\ \pi(y)\ \&\ y \mid x\ )$. $x \mid x$ by *Prop 6.2b*, so $\neg\, \pi(x)$. Then there exists z s.t. $z \mid x$ & but $\neg\, \mathit{one}(z)$ and $\neg\, z = x$. By *Prop 6.2d*, $\neg\, z = 0$. By *Prop 6.3*, $z \leq x$, so $z < x$. By assumption of the leastness of x, $\pi(p)\ \&\ p \mid z$, for some p. But by *Transitivity of* | (*Prop 6.4b*), $p \mid x$, a contradiction.

b. Assume $\pi(x)\ \&\ \mathrm{N}y\ \&\ \mathit{one}(1)$. By *Def 6.17*, $\neg\, x = 0$. So by *Prop 6.8c*, $(x \Delta y) \mid x$. Hence $\mathit{one}(x \Delta y)$ or $(x \Delta y) = x$.

c. Assume $\pi(x)\ \&\ x \mid (x \Delta y)$. By *Def 6.17*, $\neg\, x = 0$, and so by *Prop 6.3*, $x \leq (x \Delta y)$. By (*b*), $\mathit{one}(x \Delta y) \vee (x \Delta y) = x$. The former produces a contradiction to $\pi(x)$, since it forces $x = 0$ or $\mathit{one}(x)$, by *Prop 4.10*. The latter implies that $x = (x \Delta y) \mid y$.

d. Assume $\mathrm{N}x\ \&\ \mathrm{N}y\ \&\ (\neg\, x = 0 \vee \neg\, y = 0)\ \&\ \forall p(\pi(p)\ \&\ p \mid x \Rightarrow \neg\, p \mid y)$. By *Prop 6.6* and *Def 6.7*, $(x \Delta y)$ exists. $\neg\, (x \Delta y) = 0$, by *Prop 6.8b*. Assume $\neg\, \mathit{one}(x \Delta y)$. Then, by *Def 6.7*, $z \mid x\ \&\ z \mid y\ \&\ \neg\, z = 0\ \&\ \neg\, \mathit{one}(z)$, for some z. By (*a*), there exists p such that $\pi(p)\ \&\ p \mid z$. By *Transitivity of* | (*Prop 6.4b*), $p \mid x\ \&\ p \mid y$, contrary to assumption. □

7. The Euclidean Algorithm and Unique Prime Factorization

Proofs will now become shorter or eliminated when possible, with appeals to previous propositions less minutely detailed

7A. Sequences

Second-order logic, with its second-order entities, provides a ready-made manner of representing sequences of first-order things, which first-order logic does not have.

Recall from *Def 2.19* that $\{0\ \_\ n\}$ represents a predicate satisfied by those numbers between 0 and n (inclusive), where n is a natural number.

Defs 7.1. Let Nn. R is a *sequence to n*, written *Seq*(R,n), if and only if *IsFunction*(R) & *Dom*(R) $\equiv$ $\{0\ \_\ n\}$. If n is not important, *Seq*(R) may be written.

In the trivial case when 0 is not a natural number, R will also be said to be a *sequence to 0* if and only *IsFunction*(R) & *Dom*(R) $\equiv \{0\}$.

When *Seq*(R,n) and Rx,y, then $R'x$ or R_x will be used to denote y. □

Prop 7.2. $\forall x \exists R\ (\ Seq(R,0)\ \&\ (R'0) = x\ \&\ \forall T(Seq(T,0)\ \&\ (T'0) = x \Rightarrow T \equiv R)\ )$.

Pf:

By *Predicative Comprehension*, for any x, $\{(0,x)\}$ exists. Clearly $\{(0,x)\}$ is unique up to equivalence. □

Prop 7.3. Let *Seq*(R,n) & *Seq*(S,m) & $k = ((n + m) + 1)$. Then there exists T, unique up to equivalence, such that:

1) *Seq*(T,k)
2) $\forall \mathrm{i}\ (\ i \le n \Rightarrow T'i = R'i\ )$
3) $\forall \mathrm{i}\ (\ i \le m \Rightarrow T'(n + i + 1) = S'i\ )$

Pf:

Set T to $R \cup \{(x,y) : S(n + x + 1),y\}$.

Suppose $i \le k$. Now $i \le n$ or $n < i$, by *Dichotomy* (*Prop 4.5b*), and these possibilities are disjoint, by *Anti-Symmetry* (*Prop 4.18*). In the first case $Ti,(R'y)$. In the second case, $Ti,(S'x)$, where $i = (n + x + 1))$. The result follows. □

Def 7.4. Let *Seq*(R,n) & *Seq*(S,m) & $k = ((n + m) + 1)$. Then let R^S refer to that T, unique up to equivalence, guaranteed by the previous proposition. □

Prop 7.5 (*Associativity of* ^) Let $Seq(R,n)$ & $Seq(S,m)$ & $Seq(T,k)$. And suppose $two(2)$ and that $(((n + m) + k) + 2)$ exists. Then $(R\hat{}S)\hat{}T \equiv R\hat{}(S\hat{}T)$.
Pf:

Standard proof. □

Given *Props 7.2* and *7.4*, sequences to natural numbers n may be constructed given some list of things. For instance, if $three(3)$, and given some a,b,c,d, then there exists a sequence R to 3 such that $R'0 = a$, $R'1 = b$, $R'2 = c$, and $R'3 = d$.

7B. The Euclidean Algorithm.

Lemma 7.6. Suppose $0 < b$ & $b \leq a$ & $a \leq n$, and suppose $one(1)$ & $two(2)$. Then there exist Q,R,c such that:

$$\begin{aligned}&(c + 2) \leq a \;\&\; Seq(Q,c) \;\&\; Seq(R,(c + 2))\\ &\& \; R_0 = a \;\&\; R_1 = b \;\&\; R_{(c+1)} = (a \,\Delta\, b) \;\&\; R_{(c+2)} = 0\\ &\& \; \forall \mathrm{i} \; (\, i \leq c \Rightarrow R_i = Q_i * R_{(i+1)} + R_{(i+2)} \;\&\; R_{(i+2)} < R_{(i+1)} \,).\end{aligned}$$

Pf:

Proceed by induction (F4*) on n. Trivial for the base step, when $n = 0$, since this leads to a contradiction.

Suppose true for n, and assume $\mathrm{N}n$ & $\mathrm{N}m$ & $\sigma n,m$ & $\neg\, m = 0$. Suppose $0 < b$ & $b \leq a$ & $a \leq m$.

If $\mathrm{a} \leq n$, then use the Induction Hypothesis to conclude the result. Otherwise, $a = m$. By the *Division Algorithm* (*Prop 5.17*), $a = ((q * b) + r)$ & $r < b$ for some q,r.

If $r = 0$, then set $\mathrm{c} = 0$, $R'0 = a$, $R'1 = b$, $R'(c + 1) = (R'1) = b = (a \,\Delta\, b)$ (the last equality by *Prop 6.8e*), and $(R'2) = 0$.

Otherwise, suppose $\neg\, r = 0$.

If $b = m$, then by the uniqueness of the *Division Algorithm* (*Prop 5.17b*), $q = 1$ and $r = 0$, a contradiction. So $b < m$, and thus $b \leq n$.

Hence $0 < r$ & $r \leq b$ & $b \leq n$. So by the Induction Hypothesis, there exist Q,R,c such that

$$\begin{aligned}&(c + 2) \leq b \;\&\; Seq(Q,c) \;\&\; Seq(R,(c + 2))\\ &\& \; R_0 = b \;\&\; R_1 = r \;\&\; R_{(c+1)} = (b \,\Delta\, r) \;\&\; R_{(c+2)} = 0\\ &\& \; \forall \mathrm{i} \; (\, i \leq c \Rightarrow R_i = Q_i * R_{(i+1)} + R_{(i+2)} \;\&\; R_{(i+2)} < R_{(i+1)} \,).\end{aligned}$$

By *Prop 7.2*, there exists A and B such that $Seq(A,0)$ & $Seq(B,0)$ & $A_0 = a$ & $B_0 = b$. Since $(c + 2) \leq$ *b and* $b < m$, $((c + 2) + 1)$ exists. Hence by *Prop 7.3* $(A \hat{} R)$ and $(B \hat{} Q)$ exist. It is straightfoward to verify the result using $(B \hat{} Q)$, $(A \hat{} R)$, and $(c + 1)$. □

Prop 7.7. The Euclidean Algorithm (Existence). Suppose $0 < a$, $0 < b$, and $one(1)$ & $two(2)$. Then there exist Q,R,c such that:

$$Seq(Q,c) \;\&\; Seq(R,(c + 2))$$

$$\& \; R_0 = a \;\&\; R_1 = b \;\&\; R_{(c+1)} = (a \,\Delta\, b) \;\&\; R_{(c+2)} = 0$$
$$\& \; \forall \mathrm{i} \; (\; i \leq c \Rightarrow R_i = Q_i * R_{(i+1)} + R_{(i+2)} \;\&\; R_{(i+2)} < R_{(i+1)} \;).$$

Pf:

Suppose $b > a$. Then $a = (0 * b) + a$. Then $0 < a \;\&\; a \leq b \;\&\; a \leq a$. The result follows from *Lemma 7.6*, since $(a \,\Delta\, b) = (b \,\Delta\, a)$.

Otherwise, by *Dichotomy* (*Prop 4.5b*), $b \leq a$. Then $0 < b \;\&\; b \leq a \;\&\; b \leq b$. Apply *Lemma 7.6*. □

7C. Exponentiation

Prop 7.8. Let Nx & Nn & *one*(1). If

$$\mathrm{N}y \;\&\; \exists R \; (\; Seq(R,n) \;\&\; R_n = y \;\&\; R_0 = 1 \;\&\; \forall i \; (\; i < n \Rightarrow R_{(i+1)} = R_i * x) \;)$$

and

$$\mathrm{N}z \;\&\; \exists R \; (\; Seq(R,n) \;\&\; R_n = z \;\&\; R_0 = 1 \;\&\; \forall i \; (\; i < n \Rightarrow R_{(i+1)} = R_i * x) \;),$$

then $y = z$.

Pf:

An easy induction on n. □

Def 7.9. Let Nx & Nn & *one*(1). Use $(x \wedge n)$ to refer to that unique (by *Prop 7.8*) y (if it exists) such that:

$$\mathrm{N}y \;\&\; \exists R \; (\; Seq(R,n) \;\&\; R_n = y \;\&\; R_0 = 1 \;\&\; \forall i \; (\; i < n \Rightarrow R_{(i+1)} = R_i * x) \;).$$

□

Notice that ^ means concatenation when it operates on upper-case letters and exponentiation when it operates on lower-case. This should not create any confusion, since the meaning should be clear by context.

Prop 7.10.

a. $\forall x \forall 1 \; (\; \mathrm{N}x \;\&\; one(1) \Rightarrow (x \wedge 0) = 1 \;)$

b. $\forall x \forall 1 \; (\; \mathrm{N}x \;\&\; one(1) \Rightarrow (x \wedge 1) = x \;)$

c. $\forall n \forall 1 \; (\; \mathrm{N}n \;\&\; \neg \; n = 0 \;\&\; one(1) \Rightarrow (0 \wedge n) = 0 \;)$

Pf:

a. Assume Nx & *one*(1). Consider {(0,1)}, which is a sequence on {0 _ 0}.

b. Assume Nx & ¬ $x = 0$ & *one*(1). Set R to {(0,1)} ^ {(0,x)}. Then R is a sequence on {0 _ 1} by *Prop7.3*. Also by the same proposition, $R_0 = 1$ and $R_1 = x$. Hence (x ^ 1) = x.

c. By induction on n, with ϕ as

$$\forall 1\ (\ \mathrm{N}n\ \&\ \neg\, n = 0\ \&\ one(1) \Rightarrow (0 \wedge n) = 0\ ).$$

This is trivially true when $n = 0$.

Now assume Nn & Nm & $\sigma n,m$ & ¬ $m = 0$ & ϕ . If $n = 0$, then *one*(m), so by (*b*), (0 ^ m) = 1. Otherwise, assume ¬ $n = 0$. By the induction hypothesis, (0 ^ n) = 0. By *Def 7.9*,

$$Seq(R,n)\ \&\ R_n = 0\ \&\ R_0 = 1\ \&\ \forall i\ (\ i < n \Rightarrow R_{(i+1)} = R_i * x),$$

for some R. Set S to {(0,0)}. Evidently, *Seq*(S,0). Then since (n + 1) = m by *Prop 4.20a*, apply *Prop 7.3* to infer the existence of T such that

$$Seq(T,m)\ \&\ T_m = 0\ \&\ T_0 = 1\ \&\ \forall i\ (\ i < n \Rightarrow T_{(i+1)} = T_i * x),$$

Hence (0 ^ m) = 0. □

Prop 7.11. $\forall x \forall y \forall 1 \forall n\ (\ one(1)\ \&\ (x \wedge (n + 1)) = y \Rightarrow ((x \wedge n) * x) = y\ )$

Pf:

Let *one*(1) & (x ^ (n + 1)) = y. Set m to (n + 1) Then by *Def 7.9*, Ny and

$$Seq(R,m)\ \&\ R_m = y\ \&\ R_0 = 1\ \&\ \forall i\ (\ i < m \Rightarrow R_{(i+1)} = R_i * x),$$

for some R. Then $\sigma n,m$ by *Prop 4.20a*, and so $n < m$ by *Prop 4.21a*. Thus $R_{(n+1)} = R_n * x$. By *Corollary 2.20*, {0 _ m} ≡ {0 _ n} ∪ {m}, where ¬ m ∈ {0 _ n}. So, setting S to (R ⌈ {0 _ n}),

$$Seq(S,n)\ \&\ S_0 = 1\ \&\ \forall i\ (\ i < n \Rightarrow S_{(i+1)} = S_i * x)$$

But $y = R_{(n+1)} = R_n * x = S_n * x = ((x \wedge n) * x)$. □

Lemma 7.12.

a. $\forall x \forall n\ (\ \mathrm{N}x\ \&\ \mathrm{N}n\ \&\ \neg\, x = 0 \Rightarrow \neg\, (x \wedge n) = 0\ )$

b. $\forall x \forall y \forall n \forall 1\ (\ one(1)\ \&\ (x \wedge (n + 1)) = y\ \&\ x > 1 \Rightarrow (x \wedge (n + 1)) > (x \wedge n)\ )$

c. $\forall x \forall y \forall n \forall 1\ (\ one(1)\ \&\ (x \wedge n) = y\ \&\ x > 1 \Rightarrow (x \wedge n) \geq\ (n + 1)\ )$

Pf:

a. By induction on n, with ϕ as

$$\forall x\ (\ \mathrm{N}x\ \&\ \mathrm{N}n\ \&\ \neg\, x = 0 \Rightarrow \neg\,(x \hat{}\ n) = 0\ )$$

Case n = 0. Assume $\mathrm{N}x$ & N0 & $\neg\, x = 0$. By *Prop 4.9*, *one*(1) for some 1. By (*a*), $(x \hat{}\ 0) = 1$. By *Prop 4.6*, $\neg\,(x \hat{}\ 0) = 0$.

Induction Step. Now assume $\mathrm{N}n$ & $\sigma n,m$ & ϕ. Let $\mathrm{N}x$ & $\mathrm{N}m$ & $\neg\, x = 0$. And suppose $(x \hat{}\ m) = 0$. By *Prop 7.11*, $(x \hat{}\ m) = ((x \hat{}\ n) * x)$. By the induction hypothesis, $\neg\,(x \hat{}\ n) = 0$. By *Prop 5.7*, $x = 0$, a contradiction.

b. Assume *one*(1) & $(x \hat{}\ (n + 1)) = y$ & $x >1$. Then $(x \hat{}\ (n + 1)) = ((x \hat{}\ n) * x)$, by *Prop 7.11*. $\neg\,(x \hat{}\ n) = 0$, by (*a*). So $(x \hat{}\ (n + 1)) > (x \hat{}\ n)$ by *Prop 5.16b*.

c. By induction on n, with ϕ as

$$\forall x \forall y \forall n \forall 1\ (\ one(1)\ \&\ (x \hat{}\ n) = y\ \&\ x > 1 \Rightarrow (x \hat{}\ n) \geq (n + 1)\ ).$$

Case n = 0. Assume *one*(1) & $(x \hat{}\ 0) = y$ & $x > 1$. Then $(x \hat{}\ 0) = 1 \geq (0 + 1)$.

Induction Step. Now assume $\mathrm{N}n$ & $\sigma n,m$ & ϕ. Let *one*(1) & $(x \hat{}\ m) = y$ & $x > 1$. By (*b*), $(x \hat{}\ m) > (x \hat{}\ n)$. By the induction hypothesis, $(x \hat{}\ n) \geq (n + 1)$. So $(x \hat{}\ m) > m$. By *Prop 4.21c*, $(x \hat{}\ m) \geq (m + 1)$. □

Prop 7.13. $\forall x \forall y \forall z \forall n \forall 1$ (*one*(1) & $((x \hat{}\ n) * x) = y$ & $(x > 1 \vee (n + 1) = z)$
$\Rightarrow (x \hat{}\ (n + 1)) = ((x \hat{}\ n) * x)$)

Note: As usual it is not possible to assert, without conditions, that $(x \hat{}\ (n + 1)) = ((x \hat{}\ n) * x)$, since $(x \hat{}\ (n + 1))$ is almost always a bigger number than either x or n. *Prop 7.11* assumed that the left-hand side exists, the present proposition the right-hand side. However, simply assuming the existence of the right-hand side is not sufficient, because it might be the case that $x = 0$ or $x = 1$, n exists, but $(n + 1)$ does not exist. In this case, $((x \hat{}\ n) * x)$ exists (and in fact equals 0 or 1), but $(x \hat{}\ (n + 1))$ does not exist. So one needs to add in the condition that $(n + 1)$ exists, either explicitly or, since it can be seen that $x > 1$ implies the existence of $(n + 1)$, implicitly.

Pf:

Assume *one*(1) & $((x \hat{}\ n) * x) = y$ & $(\neg\, x = 1 \vee (n + 1) = z)$.
Suppose $x > 1$. By *Lemma 7.12c*, $(x \hat{}\ n) \geq (n + 1)$.
So $(x > 1 \vee (n + 1) = z)$ implies that $(n + 1)$ exists.
Since $(x \hat{}\ n)$ exists, there exists R such that

$$Seq(R,n)\ \&\ R_n = (x \hat{}\ n)\ \&\ R_0 = 1\ \&\ \forall i\ (\ i < n \Rightarrow R_{(i+1)} = R_i * x),$$

Set S to $\{(0,y)\}$ and k to $(n + 1)$. Then using *Prop 7.3*, there exists a sequence T, equivalent to $R \hat{}\ S$, such that

$$Seq(T,k)\ \&\ T_k = y\ \&\ T_0 = 1\ \&\ \forall i\ (\ i < k \Rightarrow T_{(i+1)} = T_i * x).$$

So $(x \hat{}\ m) = ((x \hat{}\ n) * x)$. □

Prop 7.14. $\forall x \forall y \forall n \forall 1$ (*one*(1) & $(x \hat{}\ n) = y$ & $z \leq x \Rightarrow (z \hat{}\ n) \leq (x \hat{}\ n)$)

Pf:

By induction on n, with ϕ as

$$\forall x \forall y \forall 1\ (\ one(1)\ \&\ (x \mathbin{\hat{}} n) = y\ \&\ z \le x \Rightarrow (z \mathbin{\hat{}} n) \le\ (x \mathbin{\hat{}} n)\ ).$$

Case n = 0. Assume $one(1)\ \&\ (x \mathbin{\hat{}} 0) = y\ \&\ z \le x$. Then $y = 1$ and $(z \mathbin{\hat{}} n) = 1$, by *Prop 7.10a*. Hence $(z \mathbin{\hat{}} n) \le\ (x \mathbin{\hat{}} n)$.

Induction Step. Now assume $\mathrm{N}n\ \&\ \sigma n{,}m\ \&\ \phi$. Let $one(1)\ \&\ (x \mathbin{\hat{}} m) = y\ \&\ z \le x$. By *Prop 7.11*, $((x \mathbin{\hat{}} n) * x) = y$. By the induction hypothesis, $(z \mathbin{\hat{}} n) \le\ (x \mathbin{\hat{}} n)$. By *Prop 5.15c*, $((z \mathbin{\hat{}} n) * z) \le ((x \mathbin{\hat{}} n) * x)$. By *Prop 7.13*, $((z \mathbin{\hat{}} n) * z) = (z \mathbin{\hat{}} m)$. □

Prop 7.15.

a. $\forall x \forall y \forall z \forall z' \forall n\ (\ z = (x * y) \mathbin{\hat{}} n\ \&\ (x = 0 \Rightarrow z' = y \mathbin{\hat{}} n)\ \&\ (y = 0 \Rightarrow z' = x \mathbin{\hat{}} n)$
$\Rightarrow (x \mathbin{\hat{}} n) * (y \mathbin{\hat{}} n) = z\ )$

b. $\forall x \forall y \forall z \forall z' \forall n\ (\ (x \mathbin{\hat{}} n) * (y \mathbin{\hat{}} n) = z\ \&\ (\neg\, n = 0 \vee x * y = z') \Rightarrow z = (x * y) \mathbin{\hat{}} n\ )$

Note: The point of this proposition is to assert $(x \mathbin{\hat{}} n) * (y \mathbin{\hat{}} n) = (x * y) \mathbin{\hat{}} n$. Again, certain conditions are required. In (*a*) one assumes that the right-hand side exists *and*, if x is 0, that $y \mathbin{\hat{}} n$ exists (and similarly if y is 0). In (*b*) one assumes that the left-hand side exists *and* the existence of $x * y$, either explicitly or implicitly with the assumption that $\neg\, n = 0$.

Pf:

a. First consider the case $x = 0$. Assume $z = (x * y) \mathbin{\hat{}} n\ \&\ (x = 0 \Rightarrow z' = y \mathbin{\hat{}} n)\ \&$ $(y = 0 \Rightarrow z' = x \mathbin{\hat{}} n)$. By *Def 7.9*, $one(1)$ for some 1. By *Prop 5.2*, $x * y = 0$. If $n = 0$, then $(x * y) \mathbin{\hat{}} n = x \mathbin{\hat{}} n = y \mathbin{\hat{}} n = 1$ by *Prop 7.10a* , so $(x \mathbin{\hat{}} n) * (y \mathbin{\hat{}} n) = 1 = z$, by *Prop 5.8a*. Otherwise, suppose $\neg\, n = 0$. By *Lemma 7.12b*, $x \mathbin{\hat{}} n = (x * y) \mathbin{\hat{}} n = 0$. But $(x = 0 \Rightarrow z' = y \mathbin{\hat{}} n)$, so $y \mathbin{\hat{}} n$ exists. Hence $(x \mathbin{\hat{}} n) * (y \mathbin{\hat{}} n) = 0$ by *Prop 5.2*.

The same type of argument applies when $y = 0$.

Finally, consider the case $\neg\, x = 0\ \&\ \neg\, y = 0$. Proceed by induction, with ϕ as

$$\forall z\ (\ z = (x * y) \mathbin{\hat{}} n \Rightarrow (x \mathbin{\hat{}} n) * (y \mathbin{\hat{}} n) = z\ ).$$

Case n = 0. Let $z = (x * y) \mathbin{\hat{}} 0$. By *Def 7.9*, $one(1)$ for some 1. $z = x \mathbin{\hat{}} 0 = y \mathbin{\hat{}} 0 = 1$, by *Prop 7.10a*. The result follows by *Prop 5.8a*.

Induction Step. Now assume $\mathrm{N}n\ \&\ \sigma n{,}m\ \&\ \phi$. Let $z = (x * y) \mathbin{\hat{}} m$. By *Prop 7.11*, $((x * y) \mathbin{\hat{}} n) * (x * y) = z$. By the induction hypothesis, $((x \mathbin{\hat{}} n) * (y \mathbin{\hat{}} n)) * (x * y) = z$. By *Associativity* and *Commutativity of Multiplication* (*Props 5.11* and *5.12*), $((x \mathbin{\hat{}} n) * x) * ((y \mathbin{\hat{}} n) * y) = z$. By *Prop 7.13*, $((x \mathbin{\hat{}} n) * x) = x \mathbin{\hat{}} m$ and $((y \mathbin{\hat{}} n) * y) = y \mathbin{\hat{}} m$.

b. First, let $(x \mathbin{\hat{}} n) * (y \mathbin{\hat{}} n) = z\ \&\ \neg\, n = 0$. By *Def 7.9*, $one(1)$ for some 1. Then $x = x \mathbin{\hat{}} 1 \le x \mathbin{\hat{}} n$, by *Props 7.10a*, *4.9*, and *7.14*. Similarly, $y \le y \mathbin{\hat{}} n$. By *Prop 5.15c*, $x * y \le (x \mathbin{\hat{}} n) * (y \mathbin{\hat{}} n)$, so $x * y$ exists. Hence it is sufficient to prove:

$$\forall x \forall y \forall z \forall z' \forall n\ (\ (x \mathbin{\hat{}} n) * (y \mathbin{\hat{}} n) = z\ \&\ x * y = z' \Rightarrow z = (x * y) \mathbin{\hat{}} n\ )$$

Proceed by induction, as in (*a*). □

Prop 7.16. $\forall x \forall y \forall n\ (\ (\neg\, x = 0 \vee \neg\, y = 0)\ \&\ x \le a\ \&\ y \le b\ \&\ (a \mathbin{\hat{}} b) = c \Rightarrow (x \mathbin{\hat{}} y) \le c\ )$

Note: The first condition is necessary since $0 \le 0\ \&\ 0 \le 1\ \&\ (0 \mathbin{\hat{}} 1) = 0$, but since $(0 \mathbin{\hat{}} 0) = 1$, not $(0 \wedge 0) \leq (0 \wedge 1)$.

Pf:

Assume $(\neg\, x = 0 \vee \neg\, y = 0)\ \&\ x \leq a\ \&\ y \leq b\ \&\ (a \wedge b) = c$. An induction and *Prop 5.15c* shows that $(x \wedge b) \leq c$. Another induction and *Lemma 7.12b* and *Prop 7.10c* shows that $(x \wedge a) \leq (x \wedge b)$. □

Prop 7.17. $\forall x \forall a \forall b \forall c \forall n \forall m \forall k\ (\ (x \wedge n) = a\ \&\ (x \wedge m) = b\ \&\ (a * b) = c\ \&\ (n + m) = k \Rightarrow (x \wedge k) = c\ )$

Pf:

By an induction on n. □

7D. Prime Factorization.

Theorem 7.18. (*Prime Factorization, Existence*) Let *one*(1). If $n > 1$, then $\exists v \exists R \exists S \exists T$ s.t.

$$
\begin{aligned}
& v < n \\
& \&\ Seq(R,v)\ \&\ Seq(S,v)\ \&\ Seq(T,v) \\
& \&\ T_0 = R_0 \wedge S_0 \\
& \&\ T_v = n \\
& \&\ \forall i\ (\ i \leq v \Rightarrow \pi(R_i)\ \&\ S_i > 0\ ) \\
& \&\ \forall i\ (\ i < v \Rightarrow R_{i+1} > R_i\ \&\ T_{i+1} = T_i * (R_{i+1} \wedge S_{i+1})).
\end{aligned}
$$

Note: For example, if $n = 700 = 2^2 * 5^2 * 7$, then

$v = 2$,
R is the sequence with $R_0 = 2\ \&\ R_1 = 5\ \&\ R_2 = 7$,
S is the sequence with $S_0 = 2\ \&\ S_1 = 2\ \&\ S_2 = 1$, and
T is the sequence with $T_0 = 4\ \&\ T_1 = 100\ \&\ T_2 = 700$.

Pf:

Suppose natural number n is a counter-example. By the *Well-Ordering Principle* (*Prop 4.22b*), we may suppose that n is the least counter-example. Since 0 and 1 satisfy the assertion trivially, $n > 1$.

By *Prop 6.20a* there exists a prime p s.t. $p \mid n$. WLOG by the *Well-Ordering Principle* again we may suppose p is the least such prime. By *Def 6.17*, $\neg\, p = 0$ and $\neg\, p = 1$. So if $(p \wedge i) \mid n$, then $i \leq (p \wedge i)$ by *Prop 7.12c* and so $i \leq n$ by *Prop 6.3* and *Transitivity of* $\leq$ (*Prop 4.5a*). By *Prop 4.23* there is a greatest number j s.t. $(p \wedge j) \mid n$. Obviously $j \leq n$. $j \geq 1$, since $p \mid n$. Now $((p \wedge j) * n') = n$ for some n', where $\neg\, n' = 0$ by *Prop 5.5*. If $n' = 1$, then set $v = 0$ and let R be $\{(0,p)\}$, S be $\{(0,j)\}$, and T be $\{(0,n)\}$. Otherwise, suppose $\neg\, n' = 1$. It can be seen that $n' < n$, so by the assumption of the leastness of n, it can be inferred that n' has a prime factorization. That is, $\exists u \exists A \exists B \exists C$ s.t.

$$
\begin{aligned}
& u < n' \\
& \&\ Seq(A,v)\ \&\ Seq(B,v)\ \&\ Seq(C,v) \\
& \&\ C_0 = A_0 \wedge B_0
\end{aligned}
$$

$\&\ C_v = n$
$\&\ \forall i\ (\ i \le v \Rightarrow \pi(A_i)\ \&\ B_i > 0\ )$
$\&\ \forall i\ (\ i < v \Rightarrow A_{i+1} > A_i\ \&\ C_{i+1} =\ C_i * (A_{i+1} \wedge B_{i+1}))$.

Let q be A_0. $q < p$ would contradict the leastness of p, since q is prime and $q \mid n'$ and $n' \mid n$ so $q \mid n$ by *Transitivity of* | (*Prop 6.4b*). If $q = p$, then since $(j + 1)$ exists by *Lemma 7.12* and since $p = p \wedge 1 = p$ by *Prop 7.10b*, then $(p \wedge (j + 1)) \mid n$ by *Prop 7.17*, contradicting the maximality of j. Hence $q > p$. Hence, set

v to $(u + 1)$
R to $\{(0,\mathrm{p})\} \wedge A$
S to $\{(0,j)\} \wedge B$, and
T to $\{(0,(p \wedge j))\} \wedge \{(i,y) : y = C_i\ * (p \wedge j)\}$.

Remark that every $C_i\ * (p \wedge j)$ exists since all are less than or equal to n. It is straight-foward to check that these v,R,S,T satisfy the desired conditions. □

Lemma 7.19 is stated here but proven later:

Lemma 7.19. If $\pi(p)\ \&\ p \mid (x * y)$, then $p \mid x$ or $p \mid y$. □

Theorem 7.20. (*Prime Factorization, Uniqueness*) Let *one*(1), $n > 1$. Suppose $\exists v \exists R \exists S \exists T$ and $\exists u \exists A \exists B \exists C$ s.t.

$v < n$
$\&\ Seq(R,v)\ \&\ Seq(S,v)\ \&\ Seq(T,v)$
$\&\ T_0 = R_0 \wedge S_0$
$\&\ T_v = n$
$\&\ \forall i\ (\ i \le v \Rightarrow \pi(R_i)\ \&\ S_i > 0\ )$
$\&\ \forall i\ (\ i < v \Rightarrow R_{i+1} > R_i\ \&\ T_{i+1} =\ T_i * (R_{i+1} \wedge S_{i+1}))$

and

$u < n$
$\&\ Seq(A,u)\ \&\ Seq(B,u)\ \&\ Seq(C,u)$
$\&\ C_0 = A_0 \wedge B_0$
$\&\ C_u = n$
$\&\ \forall i\ (\ i \le u \Rightarrow \pi(A_i)\ \&\ B_i > 0\ )$
$\&\ \forall i\ (\ i < u \Rightarrow A_{i+1} > A_i\ \&\ C_{i+1} =\ C_i * (A_{i+1} \wedge B_{i+1}))$.

Then $u = v$ and $R \equiv A\ \&\ S \equiv B\ \&\ T \equiv C$.
Pf:

Apply the standard proof using *Lemma 7.19*. □

It remains to prove *Lemma 7.19*. The proof of the *Lemma*, at least the one given here, is anything but standard, because the standard one does not work and cannot apparently be converted into one that does.

The usual proof of the *Lemma* proceeds as follows. First, it is shown that, given any two non-zero natural numbers x and y, there exist natural numbers a and b such that $a * x = b * \mathrm{y} + (x \Delta y)$.[1] Now let p be a prime dividing $u * v$. And suppose p does not divide u. Then $(p \Delta u) = 1$. So there exist a and b such that $a * p = b * u + 1$. Multiplying each term by v,

$$a * p * v = b * u * v + v$$

p divides the term on the left-hand side and the first term on the right, so p divides v.

This reasoning cannot be carried out in **F** because the product $a * x$ and $b * y$ cannot be proven to exist, given the existence of x and y, because they are usually larger numbers. There does not appear to be an easy way to correct the argument, so another method must be found.

In this section a proof using brute force will be presented. It is not pretty, but the degree of its ugliness is perhaps itself of interest. Subsequently, a more traditional proof appealing to congruences will be presented as well.

Lemma 7.21. Let $k \mid (x * y)$, $one(k \Delta y)$, and suppose $(k * x)$ exists. Then $k \mid x$.

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

Pf:

Suppose $(x * y) = 0$. If $x = 0$, then $k \mid x$ by *Prop 6.2a*. Otherwise, assume $\neg\, x = 0$. So $y = 0$, by *Prop 5.7*. By *Def 6.7*, $\neg\, k = 0$, and by *Prop 6.2a*, $k \mid y$. By *Prop 6.8e*, $one(k)$ since $one(k \Delta y)$. So by *Prop 6.2c*, $k \mid x$.

Otherwise, $\neg\, (x * y) = 0$. And suppose $one(x * y)$. Hence $(x * y) \mid x$, by *Prop 6.2c*. By *Transitivity of* $\mid$ (*Prop 6.4b*), $k \mid x$.

So one may suppose that $\neg\, one(x * y)$. By *Prop 6.14*, $two(2)$ for some 2. Let $one(1)$.

If $k = 0$, then $(x * y) = 0$ by *Prop 6.2d*, a contradiction. So $\neg\, k = 0$, hence $0 < k$. By *Prop 5.5*, $\neg\, y = 0$, hence $0 < y$. So, by the *Euclidean Algorithm*, there exist Q,R,c such that:

$$\begin{aligned}
&Seq(Q,c)\ \&\ Seq(R,(c + 2))\\
&\&\ R_0 = k\ \&\ R_1 = y\ \&\ R_{(c+1)} = (k \Delta y)\ \&\ R_{(c+2)} = 0\\
&\&\ \forall \mathrm{i}\ (\, i \le c \Rightarrow R_i = Q_i * R_{(i+1)} + R_{(i+2)}\ \&\ R_{(i+2)} < R_{(i+1)}\,).
\end{aligned}$$

In particular, $R_0 = Q_0 * R_1 + R_2$, that is

$$k = (q * y) + r,$$

where $q = Q_0$ and $r = R_2$. By assumption, $(x * k)$ exists, so by the *Distributive Law* (*Prop 5.9a*),

$$(x * k) = (x * (q * y)) + (x * r).$$

[1] If this assertion looks anything but standard, it is because the result is usually stated working in the integers (while the exposition here works in the natural numbers): given two non-zero integers x and y, then there are integers a and b such that $a * x + b * y = (x \Delta y)$.

Now $k \mid (x * k)$ by *Def 6.1*, and $k \mid (x * (q * y))$ by *Def 6.1* and *Transitivity of* $\mid$ (*Prop 6.4b*). So

$$k \mid (x * r),$$

by *Prop 6.5b*. An easy induction shows that $k \mid (x * R_i)$ for all $i \leq (c + 1)$. So in particular, $k \mid (x * R_{(c+1)})$. But $R_{(c+1)} = (k \Delta y) = 1$, so $k \mid x$, by *Prop 5.8a*. □

Prop 7.22. Assume $\pi(p)$ & $p \mid (x * y)$. And suppose that either $(p * x)$ or $(p * y)$ exists. Then $p \mid x$ or $p \mid y$.
Pf:

WLOG by symmetry, suppose $(p * x)$ exists. By *Prop 6.20b*, $(p \Delta y) = 1 \vee (p \Delta y) = p$, where $one(1)$. If $(p \Delta y) = p$, then by *Prop 6.20c*, $p \mid y$. Otherwise, suppose $one(p \Delta y)$. By *Lemma 7.21*, $p \mid x$. □

The previous proposition can be improved to *Lemma 7.19*, where the condition that either $(p * x)$ or $(p * y)$ exists, is dropped.

Proof of Lemma 7.19:

Let $\pi(p)$ & $p \mid (x * y)$.

If $x = 0$, then $p \mid x$ by *Prop 6.2a*.

Otherwise, assume $\neg\, x = 0$. So $one(1)$, for some 1, by *Prop 4.9*.

If $p \leq x$, then $(p * y) \leq (x * y)$ by *Prop 5.15a*, so $(p * y)$ exists. Then by *Prop 7.22*, the result follows.

So assume $p > x$. By the *Division Algorithm* (*Prop 5.17a*),

$$p = (q * x) + r \ \&\ r < x$$

for some q,r. By *Prop 6.8h*, $(p \Delta x) = (x \Delta r)$. If $\neg\, (p \Delta x) = 1$, then $(p \Delta x) = p$ by *Prop 6.20b*. So $p \mid x$, by *Def 6.7*.

So assume $(p \Delta x) = 1$. Hence $(x \Delta r) = 1$. Now $p \mid (x * y)$, so $(p * a) = (x * y)$ for some a. In particular $(p * a)$ and so $(((q * x) + r) * a)$ exists. Thus

$$(p * a) = ((q * x) * a) + (r * a),$$

by the *Distributive Law* (*Prop 5.9a*). Of course $x \mid (x * y) = (p * a)$ and $x \mid (q * x)$. By *Prop 6.5b*, $x \mid (r * a)$. Now $(p * a)$ exists and $x \leq p$, so $(x * a)$ exists, by *Prop 5.15a*. By *Lemma 7.21*, $x \mid a$. So $(x * v) = a$ for some v. So

$$(p * (x * v)) = (p * a) = (x * y).$$

If $v = 0$, then $a = 0$, and $(x * y) = 0$; so $x = 0$ or $y = 0$, so $p \mid x$ or $p \mid y$. Otherwise, $\neg\, v = 0$ and *Associativity of Multiplication* applies. By *Associativity* and *Cancellation*, $(p * v) = y$. Therefore, $p \mid y$. □

7E. Consequences of Unique Prime Factorization, including Least Common Multiples

Our development will now be speeded up in a couple of ways. First, proofs may be less detailed. Secondly, subtraction will be assumed. That is, when $x \geq y$, the term $(x - y)$ will be used to refer to that number k (which exists, by *Prop 4.17* and which is unique by *Prop 4.16*) such that $(y + k) = x$. So when $(x - y)$ exists, it may be inferred that $x \geq y$. All relevant fundamental propositions concerning subtraction will be assumed.

The next corollary can be considered a generalization of *Lemma 7.19* and indeed its standard proof simply follows the same reasoning as the standard proof of the *Lemma*. It is thus normally an antecedent to *Theorem 7.22*. Here it is presented as a consequence:

Corollary 7.23 (to *Theorems 7.18* and *7.20*)
Pf:

Let $k \mid (x * y)$ and $one(k \Delta y)$. Then $k \mid x$.

Pf:

$(k * a) = (x * y)$, for some a.

The cases $(x * y) = 0$ and $one(x * y)$ are easy to handle.

Otherwise, $\neg\, (x * y) = 0$ and $\neg\, one(x * y)$. So $\neg\, x = 0$ & $\neg\, y = 0$ & $\neg\, k = 0$. If $one(x)$, then $k \mid y$, which implies $(k \Delta y) = k$, so $one(k)$. And if $one(k)$ or $one(y)$, then $k \mid x$. So it may be supposed that $\neg\, one(k)$ & $\neg\, one(y)$ & $\neg\, one(x)$. Hence x, y, and k have unique prime factorizations (*Theorems 7.18* and *7.20*). No prime can appear in both the factorization of y and of k, since $one(k \Delta y)$. Thus whatever primes appear in k's factorization must also appear in x's, and the exponent of any prime in k's factorization must be less than the exponent of the same prime in x's prime factorization. Hence $k \mid x$. □

Corollary 7.24 (to *Theorems 7.18* and *7.20*). Let $\neg\, z = 0$, $x \mid z$, $y \mid z$, and $one(x \Delta y)$. Then $(x * y) \mid z$.

Pf:

If $one(z)$, then $one(x)$ and $one(y)$ by *Prop 5.8b*. So $one(x * y)$ and $(x * y) \mid z$.

Otherwise, $z > 1$, where $one(1)$. Consider the unique prime factorization of z, by *Theorems 7.18* and *7.20*. Part of the factorization must be equal to x, and since $one(x \Delta y)$, a different part must be equal to y. But then $(x * y) \mid z$. □

Corollary 7.25. Suppose $one(1)$ & $(x \Delta z) = 1$ & $(y \Delta z) = 1$ and that $(x * y)$ exists. Then $((x * y) \Delta z) = 1$.

Pf:

If $z = 0$, then $x = 1$ & $y = 1$, so $((x * y) \Delta z) = 1$.

Otherwise, let $\neg\, z = 0$. Then $((x * y) \Delta z)$ exists. Set $d = ((x * y) \Delta z)$. By *Prop 6.8b*, $d \geq 1$.

Suppose $d > 1$. By *Prop 6.20a*, $p \mid d$ for some prime p. Now $d \mid (x * y)$ & $d \mid z$, so by *Transitivity of* $\mid$ (*Prop 6.4b*), $p \mid (x * y)$ & $p \mid z$. By *Lemma 7.19*, $p \mid x$ or $p \mid y$. But this contradicts $(x \Delta z) = 1$ or $(y \Delta z) = 1$. □

Corollary 7.26. Suppose $one(x \Delta y)$, and suppose $d > 0$. Then there exist e,f s.t. $one(e \Delta x)$ &

$one(f \Delta y)$ & $one(e \Delta f)$ & $e * f = d$.
Pf:

$one(1)$ for some 1, since $d > 0$.

If $d = 1$, then set $e = 1$ and $f = 1$.

Otherwise, let $d > 1$,   Consider the unique prime factorization of d, by *Theorems 7.18* and *7.20*. Let e be equal to the product of all the terms whose primes do not divide x. Hence $one(e \Delta x)$. And let f be equal to the product of the remaining terms. Hence $one(e \Delta f)$. Since $one(x \Delta y)$, x and y have no common prime factors. So all the prime terms with primes dividing y are prime terms with primes not dividing x, and so do not appear in the factorization of f. Hence $one(f \Delta y)$. Obviusly, $e * f = d$. □

The next lemma and subsequent usage reverts to traditional notation, where sequences of numbers are smaller case letters. It should of course be remembered that such sequences are in fact second-order entities.

Lemma 7.27. Suppose $one(1)$ & $two(2)$ and

$$\begin{aligned}
&Seq(q,c) \;\&\; Seq(r,(c+2)) \\
&\&\; r_0 = a \;\&\; r_1 = b \;\&\; r_{(c+1)} = (a \Delta b) \;\&\; r_{(c+2)} = 0 \\
&\&\; \forall \mathrm{i}\ (\ i \le c \Rightarrow r_i = q_i * r_{(i+1)} + r_{(i+2)} \;\&\; r_{(i+2)} < r_{(i+1)}\ ),
\end{aligned}$$

i.e. the conditions of the Euclidean Algorithm apply. Let $1 \le i \le c$ and suppose $r_{(i\text{-}1)} * r_i$ exists. Then $\exists u,v$ s.t. $u \le r_{(i\text{-}1)}$ & $v \le r_i$ and either

$$(a \Delta b) = u * r_i - v * r_{(i-1)}$$

or

$$(a \Delta b) = v * r_{(i-1)} - u * r_i.$$

Pf:

Proceed by induction, downward on i, i.e. the base step is $i = c$, and in the induction step, we decrease i by 1.

Now

$$r_{(c-1)} = q_{(c-1)} * r_c + r_{(c+1)}.$$

$r_{(c+1)} < r_c$, so $1 \le r_c$. Also $q_{(c-1)} \le r_{(c-1)}$. But

$$(a \Delta b) = r_{(c+1)} = 1 * r_{(c-1)} - q_{(c-1)} * r_c.$$

So the assertion is true for $i = c$.

Now assume the assertion is true for $i = k$ with $c \ge k > 1$. It will be shown that it is true for $(k\text{-}1)$.

So suppose $r_{(k\text{-}2)} * r_{(k\text{-}1)}$ exists. Because r is a monotonically decreasing sequence, $r_{(k\text{-}1)} * r_k$ exists. By the inductive assumption,

$$(a \Delta b) = u * r_k - v * r_{(k-1)}$$

or

$$(a \Delta b) = v * r_{(k-1)} - u * r_k$$

for some u,v, where $u \le r(k\text{-}1)$ and $v \le r_k$. Assume the first (the proof of the second case is similar). Use

$$r(k\text{-}2) = q(k\text{-}2) * r(k\text{-}1) + r_k$$

to get

$$(a \Delta b) = u * (r(k\text{-}2) - q(k\text{-}2) * r(k\text{-}1)) - v * r(k\text{-}1).$$

$u \le r(k\text{-}1)$, so $u * r(k\text{-}2) \le r(k\text{-}1) * r(k\text{-}2)$, the latter existing by assumption. All other relevant products are evidently less as well, so distributivity applies, and the equation can be manipulated into

$$(a \Delta b) = u * r(k\text{-}2) - (u * q(k\text{-}2) + v) * r(k\text{-}1)$$

Finally, note that

$$u * q(k\text{-}2) + v \le r_k\text{-}1 * q(k\text{-}2)k + r_k = r(k\text{-}2).$$ □

Prop 7.28. Suppose $a * b$ exists, with either a or b non-zero. Then $\exists u,v$ s.t.

$$(a \Delta b) = u * a - v * b$$

or

$$(a \Delta b) = v * b - u * a.$$

Remark: the assumption that $a * b$ exists will be improved on in a subsequent proposition.

Pf:

Since either a or b is non-zero, *one*(1) for some 1.

The assertion is trivial if $a,b \le 1$.

Otherwise, it may be supposed that either a or $b > 1$, and so that *two*(2) for some 2.

The *Euclidean Algorithm* (*Prop 7.7*) therefore holds. Hence, by the previous lemma *7.27*, taking $i = 1$ and noting that $r(i\text{-}1) * r_i = a * b$ exists by assumption,

$$(a \Delta b) = u * a - v * b$$

or

$$(a \Delta b) = v * b - u * a,$$

for some u,v. □

Def 7.29. Let $x > 0$ & $y > 0$. z is called the *least common multiple* of x and y if:

i) $\neg\, z = 0$
ii) $x \mid z$ and $y \mid z$
iii) if $x \mid k$ and $y \mid k$, then $z \le k$

If such a z exists, then it is evidently unique, so write it as $(x \lozenge y)$. □

Unlike the greatest common divisor, it is not assured, given two numbers, that their least common multiple exists, since this would usually be a bigger number. However, since $(x * y)$ is evidently a common multiple of x and y and is non-zero since x and y are, if $(x * \mathrm{y})$ exists, then the least common multiple does as well, by the *Well Ordering Principle*.

Prop 7.30.

a. $\forall x \forall y \forall z\ (\ (x * y) = z\ \&\ x > 0\ \&\ y > 0 \Rightarrow \exists m\ (x \Diamond y) = m\ )$

b. $\forall x \forall y \forall z\ (\ (x \Diamond y) = z \Rightarrow (y \Diamond x) = z\ )$

c. $\forall x \forall y \forall z\ (\ (x \Diamond y) = z \Rightarrow x \mid z\ )$

d. $\forall x \forall y \forall z\ (\ (x \Diamond y) = z \Rightarrow x \leq z\ )$

e. $\forall x \forall y \forall z\ (\ (x \Diamond y) = z\ \&\ x \mid y \Rightarrow z = y\ )$

f. $\forall x \forall 1\ (\ \mathrm{N}x\ \&\ one(1) \Rightarrow (\mathrm{x} \Diamond 1) = x\ )$ □

Prop 7.31.

a. Suppose $(x \Diamond y)$ exists. Then $(x \Diamond y) = (x\ \Delta\ y) * x' * y'$, for some x',y' s.t. $x = (x\ \Delta\ y) * x'$ and $y = (x\ \Delta\ y) * y'$ and $one(x'\ \Delta\ y')$.

b. Suppose $(x * y)$ exists, and neither x nor y is zero. Then $(x\ \Delta\ y) * (x \Diamond y) = x * y$.

Pf:

a. Let $d = (x\ \Delta\ y)$, which exists since neither x nor y is zero. $one(1)$ for some 1, since x is non-zero.

Set $c = (x \Diamond y)$. $x \mid c\ \&\ y \mid c$ by *Prop 7.30c*, so $c = x * a$ and $c = y * b$, for some a,b. By *Prop 6.8c*, $x = d * x'$ and $y = d * y'$ for some natural numbers x',y', neither of which are zero since neither of x,y are zero. By *Prop 6.8l*, $one(x'\ \Delta\ y')$. By *Corollary 7.26* there exist e,f s.t. $one(e\ \Delta\ x')\ \&\ one(f\ \Delta\ y')\ \&\ one(e\ \Delta f)\ \&\ e * f = d$. $\neg\ d = 0$, so $\neg\ e = 0\ \&\ \neg f = 0$. By *Corollary 7.25*, $one((x' * f)\ \Delta\ y')$ and $one((x' * f)\ \Delta\ e)$, so $one((x' * f)\ \Delta\ (y' * e))$.

$$\begin{aligned} c &= x * a \\ &= ((e * f) * x') * a \\ &= (e * (f * x')) * a && \text{by } \textit{Associativity of Multiplication} \text{ since } \neg\ e = 0 \\ &= (e * a) * (f * x') && \text{by } \textit{Associativity of Multiplication} \text{ since } \neg\ (f * x') = 0 \end{aligned}$$

Hence $(x' * f) \mid c$ and similarly $(y' * e) \mid c$. By *Corollary 7.24*, $((x' * f) * (y' * e)) \mid c$. Rearranging by *Associativity* (again, no factor is 0), $(x * y') \mid c$. Since c is non-zero, $x * y' \leq c$. On the other hand, $x * y'$ is a common multiple of x and y, so $c \leq x * y'$. Thus $c = x * y' = (\ d * x'\ ) * y'$. Since all terms are non-zero, one can apply *Associativity* to group the product as one desires, so one can forget the order of the grouping and write $c = d * x' * y'$.

b. $(x \Diamond y)$ exists since $(x * y)$ does and neither x nor y is zero. Now apply (*a*). □

Lemma 7.32. Assume $(a \Diamond b)$ exists. Then $\exists s,t$ such that $(a \Diamond b) = s * a = t * b$ and either

$$1)\ \exists u \leq s \exists v \leq t \text{ such that } (a \Delta b) = u * a - v * b$$

or

$$2)\ \exists u \leq s \exists v \leq t \text{ such that } (a \Delta b) = v * b - u * a.$$

Proof:

Since $(a \Diamond b)$ exists, both a and b are non-zero. So $(a \Delta b)$ exists. Let $d = (a \Delta b)$. By *Prop 7.31*, $(a \Diamond b) = d * a' * b'$, for some a',b' s.t. $a = d * a'$ and $b = d * b'$ and $one(a' \Delta b')$. Evidently both a' and b' are non-zero and $(a' * b')$ exists, so by *Prop 7.28*, $\exists u,v$ s.t. $u \leq b'$ & $v \leq a'$ and

$$1 = (a' \Delta b') = u * a' - v * b'$$

or

$$1 = (a' \Delta b') = v * b' - u * a',$$

where $one(1)$.

Consider the first case (the proof of the second is similar). Then:

$$d = d * (u * a' - v * b').$$

Sincce $u \leq b'$ and $d * a' * b'$ evidently exists, so does $d * u * a'$. Similarly, $d * v * b'$ exists, so distribution applies, and

$$d = d * u * a' - d * v * b'.$$

Rearranging

$$d = u * (d * a') - v * (d * b'), \text{ i.e.}$$
$$d = u * a - v * b.$$

Set $s = b'$ and $t = a'$. □

Prop 7.33. Assume $(a \Diamond b)$ exists. Then $\exists s,t$ such that $(a \Diamond b) = s * a = t * b$ and both

$$1)\ \exists u \leq s, v \leq t \text{ such that } (a \Delta b) = u * a - v * b$$

and

$$2)\ \exists u \leq s, v \leq t \text{ such that } (a \Delta b) = v * b - u * a.$$

Proof:

By *Lemma 7.32* either 1) or 2) holds. WLOG it suffices to show that if 1) holds, then 2) does as well. So suppose

$$(a \Delta b) = u * a - v * b$$

for some $u \leq s$ and $v \leq t$, where $s * a = t * b = (a \Diamond b)$. Then

$$\begin{aligned}(a \Delta b) &= (u * a - v * b) + (t * b - s * a)\\ &= (t - v) * b - (s - u) * a.\end{aligned}$$

Evidently $t - v \leq t$ and $s - u \leq s$. □

8. Congruences and Fermat’s Little Theorem

In this chapter and the next, a theory of congruences will be developed, culminating in a proof of quadratic reciprocity. The development here, while broadly following the normal path, has still some notable differences. Typically the theory begins with the definition of a congruence relationship, and then investigates how normal addition, multiplication, and exponentiation behave under the relationship. This does not optimize the theory in the context studied here, because while normal addition, multiplication, and exponentiation of course are not necessarily total functions in **F**, in the theory of congruences they *should* be. So the normal operations need to be replaced with new ones, which ensure totality.

That is, consider addition, and let $n > 0$ be the modulus, and let a and b be two numbers less than n. Then the existence of the sum $(a + b)$ cannot be assured in **F**, because it may be a larger number than both a and b. Nonetheless, in some sense, the sum modulo n should exist, because there *does* exist a number $c < n$ which is congruent to whatever the sum equals, if only it did exist. For instance, set $n = 10$, $a = 7$, and $b = 8$. Given these numbers, it can be inferred in **F** that only those numbers less than or equal to 10, exist. In particular, it cannot be inferred that 7 + 8 exists, because of course 15 is larger than 10. Nonetheless the sum of 7 and 8 *modulo 10* does in some sense exist, because it equals 5, and 5, being less than 10, can be inferred to exist. The answer exists, only the manner of arriving at it must change. So a definition of addition modulo 10, or in general addition modulo n, needs to be provided which does not depend on the existence of the normal sum, but which points to the congruence sum directly. Similarly, definitions of multiplication modulo n and exponentiation modulo n need to be given, which point to the result without referencing the normal operations.

Since operations are now modulo a number, it is possible to combine, in the same equation, operations for different moduli. For instance, *Prop 9.22* sets conditions on when this equation is true:

$$(a \otimes_n b) + (k \otimes_b n) = b.$$

It is also possible to talk about congruence operations and normal operations. For instance, *Prop 8.6f* asserts that if $a + b = c$ & $c < n$, then $a \oplus_n b = c$. So in the premise one finds normal addition and in the conclusion congruence addition.

In this chapter and the next, David Burton’s *Elementary Number Theory* and Hardy & Wright’s *An Introduction to the Theory of Numbers* has been followed, when possible closely.

8A. Definition.

Def 8.1. Let $n > 0$, Na. Use $rm(a,n)$ to denote the unique number which is the remainder term guaranteed by the *Divison Algorithm* (*Prop 5.17*) , i.e. $rm(a,n) = r$ where

$a = n * q + r$ and $0 \le r < n$ for some q. □

Def 8.2. Let $n > 0$. Write

$$a \equiv_n b$$

or

$$a \equiv b \text{ (mod } n\text{)}$$

when $rm(a,n) = rm(b,n)$. a is said to be *congruent to b mod n*. When n (called the *modulus*) can be understood, it may be omitted, leaving $a \equiv b$ or the like. □

Remark that the symbol "≡" has already been used to express predicate equivalence. Since both sides are big letters in that case, and small letters here, there should be no confusion.

Also remark that, by the usual convention, if $a \equiv b$ (mod n), then it can be inferred that Na, Nb, Nn, and $n > 0$.

Prop 8.3. ≡ is an equivalence relation. I.e. let $n > 0$. Then:

a. $\forall a$ (N$a \Rightarrow a \equiv a$ (mod n))

b. $\forall a \forall b$ ($a \equiv b$ (mod n) $\Rightarrow b \equiv a$ (mod n))

c. $\forall a \forall b$ ($a \equiv b$ (mod n) & $b \equiv c$ (mod n) $\Rightarrow a \equiv c$ (mod n)) □

Prop 8.4. Let $n > 0$.

a. If $(k * n)$ exists, then $(k * n) \equiv 0$ (mod n)

b. If $a \equiv 0$ (mod n), then $a = (k * n)$ for some k.

c. $a \equiv 0$ (mod n) if and only if $n \mid a$

d. If $a \equiv b$ (mod n) and $a < n$ and $b < n$, then $a = b$

e. If $a \equiv b$ (mod n), then $n \mid (b - a)$ or $n \mid (\mathrm{a} - b)$. (Indeed which disjunct holds depends on whether $b \leq a$ or $a \leq b$, respectively.) □

8B. Congruence Addition

Suppose a' , b', and n are natural numbers, with $n > 0$ and $a' < n$ and $b' < n$. Then $(n - a')$ is defined, since $a' \leq n$. And so $b' - (n - a')$ is defined if and only if $(n - a') \leq b'$. And this holds if and only if $\neg\, (a' + b') < n$.

For if $(a' + b') < n$, then $(a' + b' + k) = n$, for some $k > 0$. So $(n - a') = (b' + k) > b'$. On the other hand, if $(n - a') > b'$, then $(a' + b') < n$.

Remark that it is possible that $(a' + b')$ does not exist, because it is too big. In this case both $(n - a') \leq b'$ and $\neg\, (a' + b') < n$.

Def 8.5. Let $n > 0$, Na, Nb, and set $a' = rm(a,n)$, $b' = rm(b,n)$. Then use $(a \oplus_n b)$ to denote:

$$\begin{cases} a' + b' & \text{if } a'+b' < n \\ b' - (n - a') & \text{otherwise} \end{cases}$$

The subscripted n (called the *modulus*) may be omitted if capable of being understood. □

In this and subsequent examples, the normal meaning of number constants will be assumed, in order to expedite matters.

Example. Let $a = 7$, $b = 8$, and $n = 10$. Then $rm(a,n) = 7$ and $rm(b,n) = 8$. Since $\neg\, (7 + 8) < 10$, the second choice of the definition is used, and

$$(7 \oplus_n 8) = (8 - (10 - 7)) = (8 - 3) = 5.$$

Remark that there are two ways that it could happen that $\neg\, (7 + 8) < 10$. First, $(7 + 8)$ could exist, in which case it would equal 15, and of course $\neg\, 15 < 10$. Or $(7 + 8)$ might not exist, in which case an atomic wff containing it cannot be true, hence the negation is true, so $\neg\, (7 + 8) < 10$. □

It is important to note that $(a \oplus_n b)$ always exists, provided $n > 0$ & Na & Nb. This is of course unlike the behaviour of normal addition in **F**.

Prop 8.6. Let $n > 0$ be the modulus.

a. $\forall a \forall b$ (Na & N$b \Rightarrow 0 \leq a \oplus b < n$)

b. $\forall a \forall b$ $(a < n \;\&\; b < n \Rightarrow (\, a \oplus b = 0 \Leftrightarrow (a = 0 \;\&\; b = 0) \vee (a + b = n)\,)$

c. $\forall a \forall b \forall c \forall d$ $(a \oplus b \equiv c \oplus d \Rightarrow a \oplus b = c \oplus d)$

d. $\forall a \forall b \forall c \forall d$ $(a \equiv c \;\&\; b \equiv d \Rightarrow a \oplus b = c \oplus d)$

e. $\forall a \forall b \forall c$ $(a + b = c \Rightarrow a \oplus b \equiv c)$

f. $\forall a \forall b$ $(a + b = c \;\&\; c < n \Rightarrow a \oplus b = c)$

g. $\forall a \forall b$ (Na & N$b \Rightarrow a \oplus b = b \oplus a$)

h. $\forall a \forall b \forall c$ (Na & Nb & N$c \Rightarrow a \oplus (b \oplus c) = (a \oplus b) \oplus c$)

i. $\forall a$ (N$a \Rightarrow a \oplus 0 \equiv a$)

j. $\forall a \forall b \forall c \; (a \oplus b \equiv a \oplus c \Rightarrow b \equiv c)$

k. $\forall a \forall b \; (a < n \;\&\; \mathrm{N}b \;\&\; \neg\, (a + b) < n \Rightarrow a \oplus b < b)$

Pf:

e. Assume $a + b = c$. Let $a = q_a * n + r_a$, $b = q_b * n + r_b$, for some q_a, q_b, r_a, r_b, where $0 \le r_a, r_b < n$.

If $(r_a + r_b) < n$, then $a \oplus b = r_a + r_b = rm(r_a + r_b, n) = rm(c, n)$.
On the other hand, if $(r_a + r_b) \ge n$, then $rm(c, n) = (r_a + r_b) - n = r_b - (n - r_a) = a \oplus b$.
So in both cases, $rm(c, n) = a \oplus b = rm(a \oplus b, n)$.

f. Follows from (*a*), (*e*) and *Prop 8.4d*.

h. By cases.

j. By cases.

k. Suppose $a < n \;\&\; \mathrm{N}b \;\&\; \neg\, (a + b) < n$. Then $a = rm(a, n)$. Set $b' = rm(b, n)$. Then $a \oplus b = b' - (n - a) < b' \le b$. □

Prop 8.7. Suppose $d \mid n$, and that

$a \equiv 0 \pmod{d}$ and
$b \equiv 0 \pmod{d}$.

Then

$$a \oplus_n b \equiv 0 \pmod{d}.$$

Pf:

By *Prop 8.4c*, $d \mid a$ and $d \mid b$. By the *Division Algorithm*, there exist q_a, q_b, a', b' such that

$a = n * q_a + a'$ with $0 \le a' < n$ and
$b = n * q_b + b'$ with $0 \le b' < n$.

By *Prop 6.5b*, $d \mid a'$ and $d \mid b'$. So $d \mid (a' + b')$ if $(a' + b')$ exists, and $d \mid (b' - (n - a'))$ if $(b' - (n - a'))$ exists. But then $d \mid (a \oplus_n b)$. □

Prop 8.8. Let $n > 0$ be the modulus.

a. If $\mathrm{N}a$, then $\exists c \; (a \oplus c) = 0$. Moreover, there is only one such $c < n$.

b. If $\mathrm{N}a$ and $b < n$, then $\exists c \; (a \oplus c) = b$. Moreover, there is only one such $c < n$.

c. If $a \oplus c = 0$ and $0 < c \le n$, then $c = n - rm(a, n)$.

Pf:

a. Let Na. If $a \equiv 0$, then set $c = 0$. Otherwise, set $c = n - rm(a,n)$. □

Prop 8.9. Let $n > 0$, $h \leq k \leq m$, $Seq(r,m)$, and $Im(r) \subseteq$ N. Then there exists a unique y s.t.

$$\exists s\ (Seq(s,(k - h))\ \&\ s_0 = r_h\ \&\ s_{(k-h)} = y$$
$$\&\ \forall j\ (\ j < (k - h) \Rightarrow s_{(j+1)} = s_j \oplus_n r_{(h+j+1)}\ )\ ).$$

Pf:

Since $a \oplus_n b$ always exists and is unique should a and b be natural numbers, a simple induction proves the result. □

Def 8.10. Let $n > 0$, $h \leq k \leq m$, $Seq(r,m)$, and $Im(r) \subseteq$ N. Use $(\ n\sum_{h}^{k} r_i)$ to refer to the y guaranteed by the previous proposition. □

The notation will be abused as needed. In particular, when the modulus n can be understood, it will be dropped.

The following proposition follows immmediately from the definition:

Prop 8.11. Let $n > 0$, $h \leq k \leq m$, $Seq(r,m)$, and $Im(r) \subseteq$ N.

a. $n\sum_{h}^{h} r_i = r_h$

b. If $one(1)$ and $(k + 1) \leq m$, then $n \sum_{h}^{k+1} r_i = n\sum_{h}^{k} r_i \oplus_n r_{(k+1)}$.

c. If $k \leq m'$ & $Seq(s,m')$ & $\forall i\ (h \leq i \leq k \Rightarrow r_i = s_i)$, then $n\sum_{h}^{k} r_i = n\sum_{h}^{k} s_i$ □

8C. Congruence Multiplication.

Def 8.12. Let $n > 0, a \le m$, Nb. Set $(a \otimes_n b)$ to

$$ {}_n\sum_{0}^{a} r_i $$

where $Seq(r,m)$ & $r_0 = 0$ & $\forall i(0 < i \le a \;\Rightarrow r_i = b)$. By *Prop 8.11c*, the symbol is well-defined.

Note: As usual, n is called the *modulus*. It may be omitted if it can be understood. □

Prop 8.13. Let $n \ge 1$, Na, Nb. Then $(a \otimes_n b)$ exists. Also, if $(a{+}1)$ exists, then

$$(a{+}1) \otimes_n b = (a \otimes_n b) \oplus_n b$$

and indeed

$$(a+1) \otimes_n b = \begin{cases} (a \otimes_n b) + b & \text{if } (a \otimes_n b) + b < n \\ b - (n - (a \otimes_n b)) & \text{if } \neg\ (a \otimes_n b) + b < n \end{cases}$$

Pf:

For the first equation, use *Props 8.9* and *8.11*. For the second use the first and *Def 8.5*. □

Example. Let $n = 10$, $a = 7$, and $b = 8$. Then

$0 \otimes_n 8 = 0$
$1 \otimes_n 8 = 0 \oplus_n 8 = 8$, since $0 + 8 < 10$
$2 \otimes_n 8 = 8 \oplus_n 8 = 8 - (10 - 8) = 6$, since $\neg\ 8 + 8 < 10$
$3 \otimes_n 8 = 6 \oplus_n 8 = 6 - (10 - 8) = 4$, since $\neg\ 6 + 8 < 10$
$4 \otimes_n 8 = 4 \oplus_n 8 = 4 - (10 - 8) = 2$, since $\neg\ 4 + 8 < 10$
$5 \otimes_n 8 = 2 \oplus_n 8 = 2 - (10 - 8) = 0$, since $\neg\ 2 + 8 < 10$
$6 \otimes_n 8 = 0 \oplus_n 8 = 8$
$7 \otimes_n 8 = 8 \oplus_n 8 = 6$

In other words, on successive terms, either add 8 if this doesn't put the result 10 or over, or otherwise subtract 2. □

Prop 8.14. Let $n \ge 1$ be the modulus.

a. $\forall a \forall b$ (Na & N$b \Rightarrow 0 \le a \otimes b < n$)

b. $\forall a \forall b \forall c \forall d$ $(a \otimes b \equiv c \otimes d \Rightarrow a \otimes b = c \otimes d)$

c. $\forall a\,(\mathrm{N}a \Rightarrow 0 \otimes a = 0)$

d. $\forall a \forall b\,(\mathrm{N}b \;\&\; a \equiv 0 \Rightarrow b \otimes a = 0)$

e. $\forall a \forall 1\,(\mathrm{N}a \;\&\; one(1) \Rightarrow 1 \otimes a \equiv a)$

f. $\forall a \forall b \forall b'\,(\mathrm{N}a \;\&\; b \equiv b' \Rightarrow a \otimes b = a \otimes b')$

g. $\forall a \forall b \forall 1\,(\mathrm{N}a \;\&\; \mathrm{N}b \;\&\; one(1) \Rightarrow a \otimes (b \oplus 1) = (a \otimes b) \oplus a)$

h. $\forall a \forall b\,(\mathrm{N}b \;\&\; a \equiv 0 \Rightarrow a \otimes b = 0)$

i. $\forall a \forall b\,(\mathrm{N}a \;\&\; \mathrm{N}b \Rightarrow a \otimes b = b \otimes a)$

j. $\forall a \forall b \forall c\,(\mathrm{N}a \;\&\; \mathrm{N}b \;\&\; \mathrm{N}c \Rightarrow a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c))$

k. $\forall a \forall b \forall c \forall d\,(\ \mathrm{N}a \;\&\; d = (b + c) \Rightarrow a \otimes d = (a \otimes b) \oplus (a \otimes c)\ )$

l. $\forall a \forall b \forall c\,(\mathrm{N}a \;\&\; \mathrm{N}b \;\&\; \mathrm{N}c \Rightarrow a \otimes (b \otimes c) = (a \otimes b) \otimes c)$

m. $\forall a \forall b \forall c\,(a * b = c \Rightarrow a \otimes b \equiv c)$

n. $\forall x \forall y\,(x \leq n \;\&\; y \leq n \Rightarrow (n - x) \otimes (n - y) = x \otimes y)$

o. $\forall x \forall y\,(\ x \otimes y > 0 \Rightarrow (n - x) \otimes y = n - (x \otimes y)\ )$

p. $\forall x \forall y\,(\ (x \otimes y) = 0 \Rightarrow (n - x) \otimes y = 0\ )$

Pf:

c. Let Na. Set r to $\{(0,0)\}$. Then $Seq(r,0)$. N0 by *Prop 1.1*, so $Im(r) \subseteq \mathrm{N}$. So $(0 \otimes a) =$ $n\sum_{0}^{0} r_i = r_0 = 0$.

d. By induction on b.
If $a \equiv 0$, then Na by *Defs 8.1* and *8.2*, so $(0 \otimes a) = 0$ by (*c*).
Now suppose $a \equiv 0$ and $(b \otimes a) = 0$ and that $(b + 1)$ exists, where $one(1)$. By *Prop 8.13*,

$$(b + 1) \otimes a = (b \otimes a) \oplus a = 0 \oplus a \equiv a \equiv 0.$$

By (*a*) and *Prop 8.4d*, $(b + 1) \otimes a = 0$.

e. Assume Na & $one(1)$.

$$\begin{aligned} 1 \otimes a &= (0 \otimes a) \oplus a && \text{by } \textit{Prop 8.13}\text{, so E.2} \\ &= 0 \oplus a && \text{by } (c) \\ &= a && \text{by } \textit{Prop 8.6i} \end{aligned}$$

f. By induction on a. If $b \equiv b'$, then Nb & Nb' by *Defs 8.1* and *8.2*, so

$$0 \otimes b = 0 = 0 \otimes b' \text{ by } (c),$$

so the assertion is true when $a = 0$.

Now suppose Na & $b \equiv b'$ & $a \otimes b = a \otimes b'$, and assume that $(a + 1)$ exists, where *one*(1). By *Prop 8.13*,

$$\begin{aligned}
&(a + 1) \otimes b \equiv (a \otimes b) \oplus b \qquad \text{and}\\
&(a + 1) \otimes b' \equiv (a \otimes b') \oplus b'.
\end{aligned}$$

The result follows from the induction hypothesis and *Prop 8.6d*.

g. Assume *one*(1). Proceed by induction on a.

$$0 \otimes (b \oplus 1) = 0 = 0 \oplus 0 = (0 \otimes b) \oplus 0,$$

so the assertion is true when a = 0.

Now suppose Na & Nb & $a \otimes (b \oplus 1) = (a \otimes b) \oplus a$, and assume that $(a + 1)$ exists. Then

$$\begin{aligned}
(a + 1) \otimes (b \oplus 1) &= a \otimes (b \oplus 1) \oplus (b \oplus 1) && \text{by \textit{Prop 8.13}}\\
&= ((\mathrm{a} \otimes \mathrm{b}) \oplus \mathrm{a}) \oplus (\mathrm{b} \oplus 1) && \text{by the induction hypothesis}\\
&= ((\mathrm{a} \otimes \mathrm{b}) \oplus \mathrm{b}) \oplus (\mathrm{a} \oplus 1) && \text{by \textit{Commutativity} and \textit{Associativity}}\\
&= ((a + 1) \otimes b) \oplus (a \oplus 1) && \text{by \textit{Prop 8.13}}\\
&= ((a + 1) \otimes b) \oplus (a +1) && \text{by \textit{Props 8.6d} and \textit{8.6e}}
\end{aligned}$$

h. By induction on b. Na & $b \equiv 0 \Rightarrow a \otimes b = 0$ by (c). For the induction step, suppose $a \equiv 0$ and $a \otimes b = 0$ and $(b + 1)$ exists, where *one*(1). Then

$$\begin{aligned}
a \otimes (b + 1) &= a \otimes (b \oplus 1) && \text{by \textit{Prop 8.6e} and (\textit{f})}\\
&= (a \otimes b) \oplus a && \text{by (\textit{g})}\\
&= 0 \oplus 0 && \text{by the induction hypothesis and \textit{Prop 8.6d}}\\
&= 0 && \text{by \textit{Prop 8.6b}.}
\end{aligned}$$

i. By induction on a. N$b \Rightarrow 0 \otimes \mathrm{b} = 0 = \mathrm{b} \otimes 0$ by (c) and (d).

For the induction step, suppose Na & Nb & $a \otimes b = b \otimes a$, and that $(a + 1)$ exists. Then

$$\begin{aligned}
(a + 1) \otimes b &= (a \otimes b) \oplus b && \text{by \textit{Prop 8.13}}\\
&= (b \otimes a) \oplus b && \text{by the induction hypothesis}\\
&= b \otimes (a \oplus 1) && \text{by (\textit{g})}\\
&= b \otimes (a + 1) && \text{by \textit{Props 8.6e} and \textit{8.6d}}
\end{aligned}$$

j. By induction on a.

k. Assume Na & $d = (b + c)$. Then $d \equiv (b \oplus c)$, by *Prop 8.6e*. So

$$\begin{aligned}
a \otimes d &\equiv a \otimes (b \oplus c) && \text{by (\textit{f})}\\
&\equiv (a \otimes b) \oplus (a \otimes c) && \text{by (\textit{j})}
\end{aligned}$$

Equality follows by (a) and *Prop 8.4d*.

l. By induction on a.

m. By induction on a, using *Prop 8.6e*.

n. Let $x \leq n$ & $y \leq n$. By (*j*), $(x \otimes y) \oplus (x \otimes (n - y))$ and $((n - x) \otimes (n - y)) \oplus (x \otimes (n - y))$ both equal 0. By *Prop 8.6j*, $(x \otimes y) \equiv ((n - x) \otimes (n - y))$. By (*a*), $(x \otimes y) < n$ and $((n - x) \otimes (n - y)) < n$. By *Prop 8.4d*, $(x \otimes y) = ((n - x) \otimes (n - y))$. □

Prop 8.15. Let Na & Nx & $n > 0$. Then $(a \Delta n) \mid (a \otimes_n x)$.
Pf:

By induction on x. If $x = 0$, then $a \otimes_n x = 0$, and the result follows. Now set $d = (a \Delta n)$ and suppose $d \mid (a \otimes_n x)$ and that $(x + 1)$ exists. By *Prop 8.14g*,

$$a \otimes_n (x + 1) = (a \otimes_n x) \oplus_n a.$$

By the induction hypothesis $d \mid (a \otimes_n x)$. Obviously $d \mid a$ and $d \mid n$. By *Prop 8.7*, $d \mid (a \otimes_n x) \oplus_n a$. □

Prop 8.16. $\forall a \forall c \forall n\ (one(c \Delta n)\ \&\ c \otimes_n a = 0 \Rightarrow a \equiv 0 \pmod{n})$.
Pf:

Let *one*(1), and suppose c is the smallest number such that

$$(c \Delta n) = 1\ \&\ c \otimes_n a = 0\ \&\ \neg\, a \equiv 0 \pmod{n}.$$

If $c = 0$, then $n = 1$ since $(c \Delta n) = 1$. But $a \equiv 0 \pmod{1}$ for all a, contradicting the last conjunct.

So $c > 0$. Hence there are q, r such that

$$n = q * c + r, \text{ where } 0 \leq r < c.$$

By *Props 8.6e* and *8.14m*,

$$n \equiv (q \otimes c) \oplus r,$$

where these and all subsequent congruences and operations are modulo n. So

$$\begin{array}{ll}
0 \equiv (q \otimes c) \oplus r & \\
0 \otimes a \equiv ((q \otimes c) \oplus r) \otimes a & \text{by } \textit{Prop 8.14f} \\
0 \equiv ((q \otimes c) \oplus r) \otimes a & \text{by } \textit{Prop 8.14c} \\
0 \equiv (q \otimes c \otimes a) \oplus (r \otimes a) & \text{by } \textit{Prop 8.14j} \\
0 \equiv (q \otimes 0) \oplus (r \otimes a) & \text{by assumption} \\
0 \equiv 0 \oplus (r \otimes a) & \text{by } \textit{Prop 8.14d} \\
0 \equiv (r \otimes a) & \text{by } \textit{Prop 8.6i}
\end{array}$$

But

$$(r \Delta n) = (c \Delta n) = 1$$

by *Prop 6.8h*. Since $r < c$, this is a contradiction. □

Note that the previous proposition is simply the congruence version of *Corollary 7.23*, from which one could then deduce *Lemma 7.19*.

Corollary 8.17. Suppose $one(c \,\Delta\, n)$ & $c \otimes_n a = c \otimes_n b$. Then $a \equiv b$ (mod n). □

Prop 8.18. Suppose $one(1)$ and $(c \,\Delta\, n) = 1$. Then

$$0 \otimes_n c, 1 \otimes_n c, \ldots , (n - 1) \otimes_n c$$

are the numbers $0,1,\ldots,(n - 1)$, perhaps in a different order.
Pf:

It suffices to establish that the list has no repetitions. For, if they are distinct, then there are n entries. By *Prop 8.14a* they are all between 0 and $(n -1)$, and there are of course n of these. By *Prop 2.6*, the two lists would then contain the same numbers.

So, suppose $i \otimes_n c = j \otimes_n c$. By *Corollary 8.17*, $j \equiv i$. By *Prop 8.4d*, $j = i$ since both are less than n. □

Corollary 8.19. Suppose $one(1)$ and $(c \,\Delta\, n) = 1$. Then

$$1 \otimes_n c, \ldots , (n - 1) \otimes_n c$$

are the numbers $1,\ldots,(n - 1)$, perhaps in a different order. □

Corollary 8.20. Suppose $one(c \,\Delta\, n)$ and $b < n$. Then

$$c \otimes_n x = b$$

has a solution for x with $x < n$. Any other solution is congruent to this solution. □

Prop 8.21. $c \otimes_n x = b$ has a solution if and only if $b < n$ and $(c \,\Delta\, n) \mid b$.
Pf:

($\Rightarrow$) Suppose $(c \otimes_n x) = b$. By *Prop 8.15*, $(c \,\Delta\, n) \mid (c \otimes_n x) = b$.

($\Leftarrow$) Suppose $b < n$ and $(c \,\Delta\, n) \mid b$. Set $d = (c \,\Delta\, n)$. Then there exist b',c' such that $b = (b' * d)$ and $c = (c' * d)$. So $one(c' \,\Delta\, n)$ by *Prop 6.8l* and hence by *Corollary 8.20*, $(c' \otimes_n x) = b'$ for some x. Thus $d \otimes_n c' \otimes_n x = d \otimes_n b' = b$, hence by *Props 8.14m* and *8.14f*, $(c \otimes_n x) = b$. □

Prop 8.22. Let $n > 0$, $\mathsf{N}a$, $\mathsf{N}b$. Suppose $\neg\, one(b \,\Delta\, n)$. Then $\neg\, one((a \otimes_n b) \,\Delta\, n)$. Indeed, $(b \,\Delta\, n) \mid ((a \otimes_n b) \,\Delta\, n)$.

Pf:

By *Prop 8.15*, $(b \,\Delta\, n) \mid (a \otimes_n b)$. Since $(b \,\Delta\, n) \mid n$ as well, by *Prop 6.8k*, $(b \,\Delta\, n) \mid ((a \otimes_n b) \,\Delta\, n)$. □

Prop 8.22. Let $n > 0$, $one(1)$. Suppose $(a \,\Delta\, n) = (b \,\Delta\, n) = 1$. Then $((a \otimes_n b) \,\Delta\, n) = 1$.

Pf:

If $n = 1$, then $(a \otimes_n b) = 0$, so $((a \otimes_n b) \,\Delta\, n) = 1$.

Otherwise, assume $1 < n$. Since $(a \,\Delta\, n) \mid b$, by *Prop 8.21* there exists c such that $(c \otimes_n a) = 1$.

Suppose $\neg\ ((a \otimes_n b) \,\Delta\, n) = 1$.. By *Prop 8.21*, $\neg\ (\ (c \otimes_n (a \otimes_n b)) \,\Delta\, n\ ) = 1$. Now $c \otimes_n (a \otimes_n b) = (c \otimes_n a) \otimes_n b = 1 \otimes_n b = rm(b,n)$, so $\neg\ (rm(b,n) \,\Delta\, n) = 1$. But $(rm(b,n) \,\Delta\, n) = (b \,\Delta\, n)$ by *Prop 6.8h*, a contradiction. □

Prop 8.23. Let $n > 0$, $h \leq k \leq m$, $Seq(r,m)$, and $Im(r) \subseteq \mathrm{N}$. Then there exists a unique y s.t.

$$\begin{aligned} &\exists s\ (Seq(s,(k - h))\ \&\ s_0 = r_h\ \&\ s_{(k-h)} = y \\ &\quad \&\ \forall j\ (\ j < (k - h) \Rightarrow s_{(j+1)} = s_j \otimes_n r_{(h+j+1)}\ )\ ). \end{aligned}$$

Pf:

Since $a \otimes_n b$ always exists and is unique should a and b be natural numbers, a simple induction proves the result. □

Def 8.24. Let $n > 0$, $h \leq k \leq m$, $Seq(r,m)$, and $Im(r) \subseteq \mathrm{N}$. Use $(\, n\prod_{h}^{k} r_i)$ to refer to the y guaranteed by the previous proposition. □

Again, the notation will be abused as needed and the modulus n will be dropped when possible. The following proposition follows immmediately from the definition:

Prop 8.25. Let $n > 0$, $h \leq k \leq m$, $Seq(r,m)$, and $Im(r) \subseteq \mathrm{N}$.

a. $n\prod_{0}^{0} r_i = r_0$

b. If *one*(1) and $(k + 1) \leq m$, then $n\prod_{h}^{k+1} r_i = n\prod_{h}^{k} r_i \otimes_n r_{(k+1)}$

c. If $k \leq m'$ & $Seq(s,m')$ & $\forall i\ (h \leq i \leq k \Rightarrow r_i = s_i)$, then $n\prod_{h}^{k} r_i = n\prod_{h}^{k} s_i$ □

8D. Congruence Exponentiation.

Def 8.26. Let $n > 0$, $a \leq m$, Nb. Set $(b\ \Theta_n\ a)$ to

$$n\prod_{0}^{a} r_i\,,$$

where $Seq(r,m)$ & $one(r_0)$ & $\forall i(0 < i\ \&\ i \leq a\ \Rightarrow\ r_i = b)$. By *Prop 8.25c*, the symbol is well-defined.

As usual the *n* subscript may be dropped if it can be understood. □

Prop 8.27. Let *one*(1), $n > 0$, Na, Nb. Then:

a. $b\ \Theta_n\ a$ exists.

b. If $n > 1$, then $b\ \Theta_n\ 0 = 1$.
Note: this includes $b = 0$, so $0\ \Theta_n\ 0 = 1$.

c. If $n > b$, then $b\ \Theta_n\ 1 = b$.

d. If $(a + 1)$ exists, then $b\ \Theta_n\ (a + 1) = (b\ \Theta_n\ a) \otimes_n b$. □

Prop 8.28. Let *one*(1), $n > 1$, $(b\ \Delta\ n) = 1$, Nr. Then $\neg\ (b\ \Theta_n\ r) = 0$.
Pf:

If $b = 0$, then $(b\ \Delta\ n) = n > 1$, a contradiction. So $\neg\ b = 0$.

Then proceed by induction, using the fact that $(b\ \Theta_n\ r) \otimes_n b = 0$ implies $b\ \Theta_n\ r = 0$ by *Prop 8.16*. □

Prop 8.29. Let *one*(1), $i \geq j$, and suppose $x\ \Theta_n\ i = x\ \Theta_n\ j$. Then $x\ \Theta_n\ (i - j) = 1$. □

8E. Euler's Phi Function

Recall that Mk,P says that P has size k.

Lemma 8.30. Let $n > 0$. Then Nk & Mk,$\{x : 0 < x$ & $x \le n$ & *one*$(x \Delta n)\}$, for some (unique) k.
Pf:
$\{x : 0 < x$ & $x \le n$ & *one*$(x \Delta$ n$)\} \subseteq \{z$: $0 < z$ & $z \le n\}$. But Mn,$\{z$: $0 < z$ & $z \le n\}$, so the result follows by *Prop 4.4*. □

Def 8.31. For $n > 0$, let $\phi(n)$ refer to the k assured by the previous proposition. ϕ is called *Euler's Phi Function*. □

So, M$\phi(n)$,$\{x : 0 < x$ & $x \le n$ & *one*$(x \Delta n)\}$ for all n with $n > 0$.

Evidently, if 1 exists, then $\phi(1) = 1$.

For the next propositions, recall that $\pi(p)$ is used to abbreviate that "p is prime".

Prop 8.32. $\pi(p) \Leftrightarrow \sigma p,\phi(p)$. That is, let *one*(1). Then $\pi(p) \Leftrightarrow \phi(p) = p - 1$.

Prop 8.33. *(Euler)* Let *one*(1), $n > 0$, $a > 0$, and $(a \Delta n) = 1$. Then $a\ \Theta_n\ \phi(n) \equiv_n 1$. So if $n > 1$, then $a\ \Theta_n\ \phi(n) = 1$.
Pf:
If $n = 1$, $x \equiv_n 1$ for all natural numbers x, so the result follows trivially.

Otherwise let $n > 1$. Then $x \le n$ & *one*$(x \Delta$ n$)$ if and only if $x < n$ & *one*$(x \Delta n)$. Set A to $\{x : 0 < x$ & $x < n$ & *one*$(x \Delta$ n$)\}$, and B to $\{(x \otimes_n a) : 0 < x$ & $x < n$ & *one*$(x \Delta n)\}$. Remark that M$\phi(n)$,A.

By an induction, it can be shown that there exists a one-to-one function r from $\{x : 0 < x$ & $x \le \phi(n)\}$ onto A. Extend it by defining $r_0 = 0$ so that r is now a sequence, where indeed *Seq*$(r,\phi(n))$. Define a sequence s where *Seq*$(r,\phi(n))$ by setting $s_i = (r_i \otimes_n a)$ for $i \le \phi(n)$. It will be shown that the values of s are simply the values of r, perhaps in a different order. In order to show this, it suffices to prove that $A \equiv B$.

Suppose $(x \otimes_n a) \equiv_n (y \otimes_n a)$ & $x < n$ & $y < n$. Then by *Corollary 8.17*, $x \equiv_n y$, and by *Prop 8.4d*, $x = y$. So M$\phi(n)$,B.

Suppose $0 < x$ & $x < n$ & *one*$(x \Delta n)$. Then $(x \otimes_n a) > 0$ by *Prop 8.16*. $(x \otimes_n a) < n$, by *Prop 8.14a*. And *one*$((x \otimes_n a) \Delta n)$ by *Prop 8.22*. Thus $B \subseteq A$, so by the *Pigeon Hole Principle* (*Prop 2.6*), $A \equiv B$.

So the values of r and s are the same. Indeed, since $r_i = 0 = s_i$, the values of r and s are the same from 1 through $\phi(n)$, inclusive. So their products are equal:

$$n\prod_{1}^{\phi(n)} r_i = n\prod_{1}^{\phi(n)} s_i = n\prod_{1}^{\phi(n)} (r_i \otimes_n a)$$

By an induction again, it can be seen that

$$n\prod_{1}^{\phi(n)} r_i = (n\prod_{1}^{\phi(n)} r_i) \otimes_n (a \,\Theta_n\, \phi(n)).$$

By *Prop 8.22* and an induction, $(n\prod_{1}^{\phi(n)} r_i \,\Delta\, n) = 1$. By *Corollary 8.17*, $a \,\Theta_n\, \phi(n) \equiv_n 1$. □

Corollary 8.34. (Fermat) Let $\pi(p)$, $one(1)$, and $(a \,\Delta\, p) = 1$. Then $a \,\Theta_p\, (p - 1) = 1$. □

Corollary 8.35. Let $\pi(p)$, Na. Then $a \,\Theta_p\, p \equiv_p a$. So if $a < p$, then $a \,\Theta_p\, p = a$. □

9. QUADRATIC RECIPROCITY

9A. Quadratic Residues

Def 9.1. $\pi^*(p)$ if and only if $\pi(p)$ & $\neg$ *two*(p). □

I.e. $\pi^*(p)$ if and only if p is an odd prime. Remark that the supposition that p is an odd prime implies that 3 exists, where *three*(3).

Def 9.2. *Res*(a,p) if and only if $\pi^*(p)$ & *one*$(a \,\Delta\, p)$ & $\exists x\ (x \otimes_p x) = a$. *Res*$(a,p)$ may be read, "*a is a quadratic residue of p*." □

Note: Res(a,p) implies that a is non-zero. So any x such that $(x \otimes_p x) = a$ must be non-zero as well. Note that if such an x exists, then one exists which is less than p.

Prop 9.3. Let *Res*(a,p). Then there are precisely two x, with $0 < x < p$, such that $(x \otimes_p x) = a$. Indeed, if x is one, then $(p - x)$ is the other, and

$$x \otimes_p (p - x) = p - a.$$

Pf:

$z \otimes z = a$ for some z, with $0 < z < p$, since *Res*(a,p). By *Prop 8.14n*, $(p - z)$ is another solution. Since $a > 0$, by *Prop 8.14o*, $z \otimes_p (p - z) = p - a$.

Now suppose $y \otimes y = a$, with $0 < y < p$. WLOG $y \leq z$. By standard manipuation,

$$(z \oplus (p - y)) \otimes (z \oplus y) = 0.$$

Since p is prime and both $(z \oplus (p - y))$ and $(z \oplus y)$ are less then p, *one*$((z \oplus (p - y)) \,\Delta\, p)$ and *one*$((z \oplus y) \,\Delta\, p)$. By *Prop 8.16*, either $(z \oplus (p - y)) = 0$ or $(z \oplus y) = 0$, i.e. $z = y$ or $z = p - y$. □

Def 9.4. Suppose Nk, $n > 0$. Define $(k\,!)_n = n\prod_{0}^{k} r_i$, where *Seq*(r,k) & *one*(r_0) & $\forall i(0 < i \;\&\; i \leq k \;\Rightarrow\; r_i = i)$. □

Let $n > 0$. Then $(0\,!)_n = (1\,!)_n = 1$, where *one*(1).

Example. $(3\ !)_{10} = 6$, while $(3\ !)_4 = 2$. □

Prop 9.5. Let $\pi^*(p)$, *one*(1), and $(a\ \Delta\ p) = 1$. Set p' such that $(p' + p') = p - 1$. Then:

a. If $Res(a,p)$, then $((p - 1)\ !)_p = p - (a\ \Theta_p\ p')$

b. If $\neg\ Res(a,p)$, then $((p - 1)\ !)_p = a\ \Theta_p\ p'$

Pf:

Since $\pi^*(p)$, there exists 2 and 3 such that *two*(2) and *three*(3).

By *Corollary 8.19*, for each i with $1 \leq i \leq (p - 1)$, there exists i', also with $1 \leq i' \leq (p - 1)$, such that

$$i \otimes_p i' = a.$$

a. By *Prop* 9.3, there are precisely two x, with $1 \leq x \leq (p - 1)$, such that $x \otimes_p x = a$. Call these y and z. By *Prop 9.3* again, $y \otimes_p z = p - a$.

Thus the numbers between 1 and $(p\ \text{-}1)$ are either: y, or z, or one of $(p' - 1)$ pairs (i,i') such that $(i \otimes_p i') = a$. But then,

$$\begin{aligned} ((p\ \text{-}1)\ !)_p &= (p - a) \otimes_p (a\ \Theta_p\ (p' - 1)) \\ &= p - (a \otimes_p (a\ \Theta_p\ (p' - 1))) && \text{by } \textit{Prop 8.14o} \\ &= p - (a\ \Theta_p\ p') && \text{by } \textit{Prop 8.27d} \end{aligned}$$

b. Then the numbers between 1 and $(p\ \text{-}1)$ are just one of p' pairs (i,i') such that $i \otimes_p i' = a$. But then,

$$((p\ \text{-}1)\ !)_p = a\ \Theta_p\ p'$$ □

Corollary 9.6 (*Wilson's Theorem*). Let $\pi(p)$, *one*(1). Then $((p - 1)\ !)_p = p - 1$.

Pf:

If $\pi^*(p)$, set $a = 1$ in the previous proposition. □

Prop 9.7. Let $\pi^*(p)$, *one*(1), $(a\ \Delta\ p) = 1$, $(p' + p') = (p\ \text{-}1)$.

a. If $Res(a,p)$, then $a\ \Theta_p\ p' = 1$.

b. If $\neg\ Res(a,p)$, then $a\ \Theta_p\ p' = p - 1$.

Pf:

Apply *Corollary 9.6* to *Prop 9.5*. □

Lemma 9.8. Let $\pi^*(p)$, *one*(1), $(a\ \Delta\ p) = 1$, $(p' + p') = (p\ \text{-}1)$. Consider

$$X = \{x : \exists i\ (0 < i \leq p' \ \&\ x = (i \otimes_p a)\ \&\ x > p')\},$$
$$Y = \{y : \exists i\ (0 < i \leq p' \ \&\ y = (i \otimes_p a)\ \&\ y \leq p')\}$$
$$Z = \{z : \exists x\ (Xx \ \&\ z = p - x)\}$$

Then $(Y \cup Z) \equiv \{x : 1 \leq x \leq p'\}$.

Pf:

$(Y \cup Z) \subseteq \{x : 1 \leq x \leq p'\}$, using *Prop 8.16*.

Let Zz, say $z = p - (k \otimes_p a)$, where $0 < k \leq p'$. It is claimed that, for all i with $0 < i \leq p'$, $\neg\ i \otimes_p a = z$. For suppose to the contrary that $i \otimes_p a = z$, with $0 < i \leq p'$. Then

$$(i \otimes_p a) \oplus_p (k \otimes_p a) = 0$$
$$(\mathrm{i} \oplus_p k) \otimes_p a = 0 \qquad \text{by } \textit{Prop 8.14m}$$
$$i \oplus_p k = 0 \qquad \text{by } \textit{Prop 8.16}$$

But this is impossible since $0 < i,k \leq p'$. Thus Y and Z are disjoint.

Clearly X and Y are disjoint. Also Z has the same size as X.

Moreover, by the usual argument, the $(i \otimes_p a)$ of X and Y are all distinct, i.e. $(X \cup Y)$ has size p'. Putting all this together, $(Y \cup Z)$ has size p', and by the *Pigeon Hole Principle* (*Prop 2.6*), $(Y \cup Z) \equiv \{x : 1 \leq x \leq p'\}$. □

Lemma 9.9. (*Gauss*) Let $\pi^*(p)$, *one*(1), *two*(2), $(a\ \Delta\ p) = 1$, $(p' + p') = (p - 1)$. Consider

$$X = \{x : \exists i\ (0 < i \leq p' \ \&\ x = (i \otimes_p a)\ \&\ x > p')\},$$

and suppose Mn,X. Then:

Res(a,p) if and only if $2 | n$.

Pf:

As in the previous lemma, consider

$$Y = \{y : \exists i\ (0 < i \leq p' \ \&\ y = (i \otimes_p a)\ \&\ y \leq p')\}$$
$$Z = \{z : \exists x\ (Xx \ \&\ z = p - x)\}.$$

By *Lemma 9.8*, $(Y \cup Z) \equiv \{x : 1 \leq x \leq p'\}$. Evidently, $\mathrm{M}n,Z$.

If $2 | n$, then it is possible to pair off the elements of Z, and so by *Prop 8.14n*, the product (modulo p) of all the elements of Z equals the product (modulo p) of all the elements of X,

$$\prod_{Zz} z = \prod_{Xx} x.$$

And if $\neg\ 2 | n$, then all but one element of Z can be paired off, so by *Prop 8.14n and 8.14o*,

$$\prod_{Zz} z = p - \prod_{Xx} x.$$

.

Hence, if $2 | n$,

$$\begin{aligned}(p'\,!)_p \otimes_p (a\ \Theta_p\ p') &= (1 \otimes_p a) \otimes_p (2 \otimes_{\mathrm{p}} a)\ \otimes_p \ldots \otimes_p (p' \otimes_p a)\\ &= (p'\,!)_p \qquad\qquad \text{by } \textit{Corollary 8.19}\end{aligned}$$

Thus $a\ \Theta_p\ p' = 1$, so by *Prop 9.5*, *Res*(a,p).

On the other hand, if $\neg\ 2|\ n$,

$$\begin{aligned}(p'\,!)_p \otimes_p (a\ \Theta_p\ p') &= p - (1 \otimes_p a) \otimes_p (2 \otimes_p a)\ \otimes_p \ldots \otimes_p (p' \otimes_p a)\\ &= p - (p'\,!)_p, \qquad\qquad \text{again by } \textit{Corollary 8.19}.\end{aligned}$$

Thus $a\ \Theta_p\ p' = p - 1$, so by *Prop 9.5*, $\neg$ *Res*(a,p). □

9B. The Product Quotient

Recall, by the *Division Algorithm*, that given any $n > 0$ and any number c, there exist q,r such that

$$c = q * n + r, \text{ where } r < n.$$

Congruences modulo n refer to the remainder, and one consequence of the results hitherto is that it is possible to determine what the remainder of $(a + b)$, $(a * b)$, and $(a \wedge b)$, upon division by n, would be even if these numbers do not in fact exist.

Now it is time to turn to the quotient q. If either a or b is less than or equal to n, then the quotient of $(a * b)$ divided by n is less than or equal to n and so exists. It is determined by a, b, and n. Since it cannot be assured that $(a * b)$ exists, another way of referring to this quotient must be found, and is the motivation for the following definition.

Def 9.10. Let $n > 0$ & *one*(1) & Na & $b \leq n$. Use $[a,b\ /\ n]$ to refer to the (evidently unique) y, if it exists, such that

$$\begin{aligned}&\exists r \exists k\ (Seq\ (r,k)\ \&\ r_0 = 0\ \&\ r_k = y\ \&\\ &\qquad \forall j\ (j < k\ \ \&\ ((j \otimes_n b) + b) < n \Rightarrow r_{(j+1)} = r_j)\ \&\\ &\qquad \forall j\ (j < k\ \ \&\ \neg\ ((j \otimes_n b) + b) < n \Rightarrow r_{(j+1)} = r_j + 1\ )\ )\end{aligned}$$

□

Example. Let $a = 7$, $b = 8$, and $n = 10$.

$$\begin{aligned}&[0,8\ /\ 10] = 0 && &&\\ &[1,8\ /\ 10] = [0,8\ /\ 10] &&= 0, &&\text{since } (0 \otimes_{10} 8) + 8 = 8 < 10\\ &[2,8\ /\ 10] = [1,8\ /\ 10] + 1 &&= 1, &&\text{since } \neg\ (1 \otimes_{10} 8) + 8 < 10.\\ &[3,8\ /\ 10] = [2,8\ /\ 10] + 1 &&= 2, &&\text{since } \neg\ (2 \otimes_{10} 8) + 8 < 10.\\ &[4,8\ /\ 10] = [3,8\ /\ 10] + 1 &&= 3, &&\text{since } \neg\ (3 \otimes_{10} 8) + 8 < 10.\\ &[5,8\ /\ 10] = [4,8\ /\ 10] + 1 &&= 4, &&\text{since } \neg\ (4 \otimes_{10} 8) + 8 < 10.\\ &[6,8\ /\ 10] = [5,8\ /\ 10] &&= 4, &&\text{since } (5 \otimes_{10} 8) + 8 < 10.\\ &[7,8\ /\ 10] = [6,8\ /\ 10] + 1 &&= 5, &&\text{since } \neg\ (6 \otimes_{10} 8) + 8 < 10.\end{aligned}$$

So $[a,b\ /\ n]$ counts the number of times that adding b to the previous sum puts the new sum to or over n. This is the same as the quotient of $(a * b)$ upon division by n, provided the product exists. □

Prop 9.11. Let $n > 0$ & Na & $b \le n$. Then $[a,b / n]$ exists.
Pf:

Since $n > 0$, there exists 1 such that *one*(1).

It suffices to check that $r_j + 1$ always exists should $j < k$. But an easy induction shows that $r_j \le j$. Hence $r_j + 1 \le k$. □

Prop 9.12. Let $n > 0$ & *one*(1) & $n \ge b$ & Na.

a. $[0, b / n] = 0$.

b. $[a, 0 / \mathrm{n}] = 0$.

c. If $a > 0$, then

$$[a,b/n] = \begin{cases} [(a-1),b/n] & \text{if } (((a-1) \otimes_n b) + b) < n \\ [(a-1),b/n]+1 & \text{otherwise} \end{cases}$$

d. $[1,b / n] = \begin{cases} 0 & \text{if } b < n \\ 1 & \text{if } b = n \end{cases}$

e. If $a > 0$, then $[(a - 1),b / n] \le [a,b / n] \le [(a - 1),b / n] + 1$.

f. If $k > 0$, a is the least number x s.t. $[x,b / n] = k$ if and only if $[a,b / n] = [(a -1),b / n] + 1$.

Pf:

a. By *Def 9.10*.

b. By an easy induction.

c. By *Def 9.10*.

d. If $b < n$, then $(0 + b) < n$, so $[1,b / n] = [0,b / n] = 0$, by (*a*).
And if $b = n$, then $(0 + b) = n$, so $[1,b / n] = [0,b / n] + 1 = 1$, again by (*a*).

e. Follows immediately from (*c*).

f. Follows immediately from (*e*). □

The conditions of *Prop 9.12c* are the same for congruence multiplication in *Prop 8.13*. So

$$[a,b / n] = [(a - 1),b / n] \Leftrightarrow ((a - 1) \otimes_n b) + b < n$$

$$\Leftrightarrow (a \otimes_n b) = ((a - 1) \otimes_n b) + b$$

and

$$[a,b / n] = [(a - 1),b / n] + 1 \Leftrightarrow \neg ((a - 1) \otimes_n b) + b < n$$
$$\Leftrightarrow (a \otimes_n b) = b - (n - ((a - 1) \otimes_n b)).$$

Prop 9.13. Let $n > 0$ & $n \geq b$ & Na.

a. If $a' \leq a$, then $[a',b / n] \leq [a,b / n]$

b. If $b \leq n' \leq n$, then $[a,b / n] \leq [a,b / n']$

Pf:

a. By *Prop 9.12e*.

b. Since $n > 0$, there exists 1 such that $one(1)$.

A stronger assertion will be proven:

If $b \leq n' \leq n$, then $[a,b / n] \leq [a,b / n']$ &
$([a,b / n] = [a,b / n'] \Rightarrow a \otimes_n b \leq a \otimes_{n'} b)$

By induction on a. If $a = 0$, then the claim holds by *Prop 9.12a*.
Now assume the claim holds for $(a -1)$. If $[(a - 1),b / n] < [(a - 1),b / n']$ then the result follows easily, since $[a,b / n] \leq [(a - 1),b / n] + 1 \leq [(a - 1),b / n'] \leq [a,b / n']$, using *Prop 9.12e*.
So suppose $[(a - 1),b / n] = [(a - 1),b / n']$. Then by the induction hypothesis, $(a -1) \otimes_n b \leq (a -1) \otimes_{n'} b$. A consideration of the relevant cases yields the result. □

Prop 9.14. Let $n > 0$, $n \geq a,b$. Then $[a,b / n] = [b,a / n]$.
Proof:
Since $n > 0$, there exists 1 s.t. $one(1)$.
By a double induction, first on a, then on b. The assertion is true for $a = 0$, by *Prop 9.12a*. So assume $a > 0$ and the claim is true for $(a -1)$. Now the assertion is true for $b = 0$, by *Prop 9.12b*. So assume $b > 0$ and the claim is true for $(b -1)$.
Set

$$x = [(a - 1),(b - 1) / n]$$
$$y = (a - 1) \otimes_n (b - 1).$$

By the induction hypothesis

$$x = [(b - 1),(a - 1) / n].$$

and by *Prop 8.14i*,

$$y = (b - 1) \otimes_n (a - 1).$$

Now

$$[a,(b-1)/n] = \begin{cases} x & \text{if } y + (b-1) < n \\ (x+1) & \text{otherwise} \end{cases}$$

and

$$[b,(a-1)/n] = \begin{cases} x & \text{if } y + (a-1) < n \\ (x+1) & \text{otherwise} \end{cases}.$$

By the induction hypothesis again,

$[(b - 1),a / n] = [a,(b - 1) / n]$ and
$[(a - 1),b / n] = [b,(a - 1) / n]$.

Thus:

$$[b,a/n] = \begin{cases} x & \text{if } ((b-1) \otimes_n a) + a < n \;\&\; y + (b-1) < n \\ (x+2) & \text{if } \neg\, ((b-1) \otimes_n a) + a < n \;\&\neg\; y + (b-1) < n \\ (x+1) & \text{otherwise} \end{cases}$$

and

$$[a,b/n] = \begin{cases} x & \text{if } ((a-1) \otimes_n b) + b < n \;\&\; y + (a-1) < n \\ (x+2) & \text{if } \neg\, ((a-1) \otimes_n b) + b < n \;\&\neg\; y + (a-1) < n \\ (x+1) & \text{otherwise} \end{cases}.$$

where *two*(2), noting that in the cases exhibited there exists such 2.

Hence it suffices to show that the two first pairs of conditions are respectively equivalent.

Note

$$\begin{aligned} (b - 1) \otimes_n a &= a \otimes_n (b - 1) \\ &= y \oplus_n (b - 1). \end{aligned}$$

Case 1. Suppose $(y \oplus_n (b - 1)) + a < n \;\&\; y + (b - 1) < n$.

By the second conjunct, by *Def 8.5*,

$$y \oplus_n (b - 1) = y + (b - 1).$$

So

$$y + (b - 1) + a < n.$$

This implies:

$$y + (a - 1) + b < n \;\&\; y + (a - 1) < n.$$

Again

$$y \oplus_n (a - 1) = y + (a - 1).$$

Thus

$$(y \oplus_n (a - 1)) + b < n \,\&\, y + (a - 1) < n.$$

Case 2. Now suppose $\neg\, (y \oplus_n (b - 1)) + a < n \,\&\, \neg\, y + (b - 1) < n$.
By the second conjunct, by *Def 8.5*,

$$y \oplus_n (b - 1) = (b - 1) - (n - y).$$

Thus

$$\neg\, ((b - 1) - (n - y)) + a < n$$

and

$(b - 1) - (n - y)$ exists.

So

$$n - y \leq b - 1$$
$$(n - y) +1 \leq b.$$

Suppose

$$y + (a - 1) < n.$$

Then:

$(a - 1) < (n - y)$
$a \leq (n - y) + 1$ (which exists by the above, being $\leq b$).

Since $(a - 1) < (n - y) \leq (b - 1)$,

$$b > a.$$
$$(b - a) \geq b - ((n - y) + 1) = (b - 1) - (n - y)$$

Since $n > b$,

$$\begin{aligned} n &> (b - a) + a \\ &> ((b - 1) - (n - y)) + a, \end{aligned}$$

a contradiction. Therefore

$$\neg\, y + (a - 1) < n.$$

So by *Def 8.5*,

$$y \oplus_n (a - 1) = (a - 1) - (n - y).$$

Suppose

$$(y \oplus_n (a - 1)) + b < n$$

Then

$$((a - 1) - (n - y)) + b < n.$$

If $(b - 1) \geq (n - y)$, then $(b - 1) - (n - y)$ exists, so

$$((b - 1) - (n - y)) + a = ((a - 1) - (n - y)) + b \; < n,$$

a contradiction. Thus

$$(b - 1) < (n - y).$$
$$y + (b - 1) < n,$$

another (and the final) contradiction. Hence $\neg\, (y \oplus_n (a - 1)) + b < n$. □

Prop 9.15. Let $n > 0$ & $n \geq b$ & Na.

a. $[b,n / n] = b$

b. If $(a + n)$ exists, then $[(a + n),b / n] = b + [a,b / n]$.

c. If $y = (q * n) + r$, then $[y,b / n] = (q * b) + [r,b / n]$.

Pf:

Since $n > 0$, there exists 1 such that *one*(1).

a. By induction on b. Holds for $b = 0$ by *Prop 9.12a*. For $b > 0$, assume true for $(b - 1)$. Then

$$[b,n / n] = [(b - 1),n / n] + 1$$

by *Prop 9.12c*, since there is no x s.t. $(x + n) < n$, so in particular $\neg\, (((b - 1) \otimes_n n) + n) < n$. So, using the induction hypothesis,

$$[b,n / n] = b.$$

b. By induction on a. Holds for $a = 0$ by (a). For $a > 0$, assume true for $(a - 1)$, and suppose $((a + n) +1)$ exists. Then

$$[(a+n)+1,b/n] = \begin{cases} [(a+n),b/n] & \text{if } ((a+n) \otimes_n b) + b < n \\ [(a+n),b/n]+1 & \text{otherwise} \end{cases}$$

and

$$[(a+1),b/n] = \begin{cases} [a,b/n] & \text{if } (a \otimes_n b) + b < n \\ [a,b/n]+1 & \text{otherwise} \end{cases}$$

But $(a + n) \otimes_n b = (a \otimes_n b)$ by *Prop 8.14f*. The result follows by a consideration of the two pairs of equivalent cases.

c. By induction on q. Obviously holds for $q = 0$. For the induction step use (b). ▯

Prop 9.16. Let $n > 0$ & $n \geq b$ & Na. Suppose $(a * b)$ exists. Then

$$(a * b) = ([a,b / n] * n) + (a \otimes_n b).$$

Moreover, suppose $(a * b) = (q * n) + r$, where Nq and $r < b$. Then $q = [a,b / n]$ and $r = (a \otimes_n b)$.

Pf:

By induction on a. Since $n > 0$, there exists 1 such that $one(1)$. For the induction step, note that

$$[(a+1),b/n] = \begin{cases} [a,b/n] & \text{if } (a \otimes_n b) + b < n \\ [a,b/n]+1 & \text{otherwise} \end{cases}$$

Now if $(a \otimes_n b) + b < n$, then $(a + 1) \otimes_n b = (a \otimes_n b) + b$; and otherwise $(a + 1) \otimes_n b = (a \otimes_n b) - (n - b)$. The first assertion follows by a consideration of cases.

The second assertion follows by the uniqueness condition of the *Division Algorithm*. ▯

Corollary 9.17. Let $n > 0$ & $n \geq b$ & Na. Suppose $(a \otimes_n b)$ is non-zero. Then:

a. If $(a * b)$ exists, then $([a,b / n] * n) < (a * b)$.

b. In particular, if $n > (a * b)$, then $[a,b / n] = 0$.

c. In particular, if $n > (a * b)$, then $[i,b / n] = 0$ for all $i \leq a$. ▯

Corollary 9.18. Let $b > 0$ & $[a,b / n] > 0$ & $n = (q * b) + r$, where Nq and $r < b$. Then $a \geq q$, with equality only in the case $r = 0$.

Pf:

Suppose $r =0$, i.e. $(q * b) = n$. If $a < q$, then $(a * b) < (q * b) = n$, so $[a,b / n] = 0$ by *Corollary 9.17b*, a contradiction. Hence $a \geq q$.

Now suppose $r > 0$. Then $(q * b) < n$, so $[q,b / n] = 0$, again by *Prop 9.17b*. But then $a \leq q$ implies $[a,b / n] = 0$, by *Prop 9.13a*, a contradiction, so $a > q$. ▯

Prop 9.19. Let $n = (q * b) + r$, where $r < b \leq n$. Also let $one(1)$.

a. If $(((a + i) \otimes_n b) + b) < n$ for all $i < u$, then

$$[a,b\ /\ n] = [(a + u),b\ /\ n]$$

b. $[a,b\ /\ n] = [(a + u),b\ /\ n]$ if and only if, for all $i \leq u$,

$$(a + i) \otimes_n b = (a \otimes_n b) + (i * b).$$

c. If $[a,b\ /\ n] = [(a + u),b\ /\ n] = [(a + u + 1),b\ /\ n] - 1$, then

$$(a + u + 1) \otimes_n b = (a \otimes_n b) + ((u * b) - (n - b))$$

d. If $a \otimes_n b < r$, then $[(a + q),b\ /\ n] = [a,b\ /\ n]$.

e. If $a \otimes_n b \geq r$, then $[(a + q),b\ /\ n] = [a,b\ /\ n] + 1$.

f. If Na, then $[(a + q + 1),b\ /\ n] \geq [a,b\ /\ n] + 1$.

Pf:

a. Follows by an easy induction from *Prop 9.12c*.

b. Assume $[a,b\ /\ n] = [(a + u),b\ /\ n]$. An easy induction proves $(((a + i) \otimes_n b) + b) < n$, and so $((a + (i + 1)) \otimes_n b) = (a \otimes_n b) + ((i + 1) * b)$, for all $i \leq (u - 1)$.

Now assume $(a + i) \otimes_n b = (a \otimes_n b) + (i * b)$ for all $i \leq u$. By an easy induction, $(a + i) \otimes_n b = ((a + (i - 1)) \otimes_n b) + b$, for all i, where $1 \leq i \leq u$. So for such i, $((a + (i - 1)) \otimes_n b) + b < n$, i.e. $[(a + i),b\ /\ n] = [(a + (i - 1)),b\ /\ n]$.

c. Assume $[a,b\ /\ n] = [(a + u),b\ /\ n] = [(a + u + 1),b\ /\ n] - 1$.
Then $\neg\ (((a + u) \otimes_n b) + b) < n$, so

$$\begin{aligned}(((a + u) + 1)) \otimes_n b &= ((a + u) \otimes_n b) \oplus_n b && \text{by } \textit{Prop 8.13}\\ &= b - (n - ((a + u) \otimes_n b)) && \text{by } \textit{Def 8.5}\\ &= b - (n - ((a \otimes_n b) + (u * b))) && \text{by } (b)\end{aligned}$$

By appropriate manipulation the right-hand side becomes $(a \otimes_n b) + ((u * b) - (n - b))$.

d. Assume $a \otimes_n b < r$. Let $i < q$.

$$\begin{aligned}(a + i) \otimes_n b = &\ (a \otimes_n b) + (i \otimes_n b) && \text{by } \textit{Prop 8.14k}\\ &< r + (i * b)\end{aligned}$$

So $((a + i) \otimes_n b) + b < r + (q * b) = n$. By ($a$), $[(a + q),b\ /\ n] = [a,b\ /\ n]$.

e. Assume $a \otimes_n b \geq r$. Suppose $[(a + q),b\ /\ n] = [a,b\ /\ n]$. Then by ($b$), $(a + q) \otimes_n b = (a \otimes_n b) + (q * b) \geq n$, contradicting *Prop 8.14a*. Thus for some least $u < q$, $[a,b\ /\ n] = [(a + u),b\ /\ n] = [(a + u + 1),b\ /\ n] - 1$. So $\neg\ (((a + u) \otimes_n b) + b) < n$, by *Prop 9.12c*. And so $(a + u + 1) \otimes_n b = ((a + u) \otimes_n b) \oplus_n b < b$, by *Prop 8.6k*. But then

$$(((a + u + 1) \otimes_n b) + (i * b) < b + (i * b) \leq n,$$

for all $i < q$. By (b),

$$[(a + u + q),b \,/\, n] = [(a + u + 1),b \,/\, n].$$

But $a + u + q \geq a + q \geq a + u + 1$. So by *Prop 9.13a*,

$$\begin{aligned}[(a + q),b \,/\, n] &= [(a + u + 1),b \,/\, n] \\ &= [a,b \,/\, n] + 1.\end{aligned}$$

□

Prop 9.20. Let $n,m > 0$, $a \leq m$, and Nk. Then:

$$k \otimes_n a = ([k,a \,/\, m] \otimes_n m) \oplus_n (k \otimes_m a)$$

Note: This is essentially the Division Algorithm taken modulo n. If $(k * a)$ exists, then by *Prop 9.16*

$$(k * a) = ([k,a \,/\, m] * m) + (k \otimes_m a).$$

However in the present proposition, one is not given that $(k * a)$ exists.

Example. Let $n = 10$, $a = 7$, $k = 5$, $m = 4$. Then

$$\begin{aligned}&k \otimes_n a = 5 \\ &[k,a \,/\, m] = 8 \\ &[k,a \,/\, m] \otimes_n m = 8 \otimes_{10} 4 = 2 \\ &k \otimes_m a = 3 \\ &([k,a \,/\, m] \otimes_n m) \oplus_n (k \otimes_m a) = 2 \oplus_{10} 3 = 5.\end{aligned}$$

Pf:

Since $n > 0$, there exists 1 such that *one*(1).
Proceed by induction on k. If $k = 0$, both sides reduce to 0.
Next, suppose $k > 0$ and that

$$(k - 1) \otimes_n a = ([k - 1,a \,/\, m] \otimes_n m) \oplus_n ((k - 1) \otimes_m a).$$

Adding (modulo n) a to both sides, and using associativity of modulo addition,

$$(k \otimes_n a) = ([(k - 1),a \,/\, m] \otimes_n m) \oplus_n ((k - 1) \otimes_m a) \oplus_n a$$

Case 1. $((k - 1) \otimes_m a) + a < m$.
Then $[k,a \,/\, m] = [(k - 1),a \,/\, m]$, and

$$((k - 1) \otimes_m a) \oplus_n a \equiv_n ((k - 1) \otimes_m a) + a = k \otimes_m a,$$

from which the result follows.

Case 2. $\neg\, ((k - 1) \otimes_m a) + a < m$.
Then $[k,a \,/\, m] = [(k - 1),a \,/\, m] + 1$, and

$$\begin{aligned}&k \otimes_m a = ((k - 1) \otimes_m a) - (m - a), \text{ i.e.} \\ &(k - 1) \otimes_m a = (k \otimes_m a) + (m - a).\end{aligned}$$

So

$$((k - 1) \otimes_m a) \oplus_n a = (k \otimes_m a) \oplus_n m.$$

But

$$\begin{aligned}([(k - 1),a / m] \otimes_n m) \oplus_n m &= ([(k - 1),a / m] \oplus_n 1) \otimes_n m \\ &= [k,a / m] \otimes_n m,\end{aligned}$$

from which the result follows. □

Lemma 9.21. Suppose $r \le b$ & $0 < b$ & $0 < k$ & $one(1)$. Then

$$r = ([k,r / b] - [(k - 1),r / b]) * b + ((k \otimes_b r) - ((k - 1) \otimes_b r))$$

Pf:

By *Prop 9.12c* (see the remarks following the proposition), if $[k,r / b] = [(k - 1),r / b]$, then $k \otimes_b r = ((k - 1) \otimes_b r) + r$. Otherwise, $[k,r / b] = [(k - 1),r / b] + 1$, and then $k \otimes_b r = ((k - 1) \otimes_b r) - (b - r)$, which can then be manipulated into the result. □

Prop 9.22. Let $n \ge b \ge k > 0$, where $\neg\, b \mid n$. And let $one(1)$. Suppose a is the least number s.t. $[a,b / n] = k$. Then:

a. $[n,k / b] = (a - 1)$

b. $(a \otimes_n b) + (k \otimes_b n) = b$

Example. Let $n = 10$, $a = 7$, $b = 8$, and $k = 5$. Note that

$[7,8 / 10] = 5$ and
$[6,8 / 10] = 4$,

so the least number x such that $[x,8 / 10] = 5$ is indeed $x = 7$. Then

a. $[10,5 / 8] = 6 = (7 - 1)$.

Since $(7 \otimes_{10} 8) = 6$ and $(5 \otimes_8 10) = 2$,

b. $6 + 2 = 8$.

Pf:

Set $n = (q * b) + r$, for some q,r where $r < b$. In fact, $0 < r$, since by assumption $\neg\, b \mid n$. Proceed by induction on k. Consider $k = 1$. Then

$$\begin{aligned}[n,1 / b] &= q + [r,1 / b] && \text{by } \textit{Prop 9.15c} \\ &= q && \text{by } \textit{Prop 9.12d}\end{aligned}$$

On the other hand, $[q,b / n] = 0$ by *Corollary 9.17b* and so *Prop9.19f* forces $[(q + 1),b / n] = 1$. Hence $a = (q + 1)$, whence $[n,1 / b] = (a - 1)$. So (*a*).

As for (*b*),

$$0 = (q \otimes_n b) \oplus_n r.$$

This forces $q \otimes_n b = (n - r)$ by *Prop 8.8a*. Note $r < b$, so $\neg\ (n - r) + b \leq n$, and hence $\neg\ (q \otimes_n b) + b \leq n$. Thus

$$\begin{aligned}(q + 1) \otimes_n b &= (q \otimes_n b) - (n - b)\\ &= (n - r) - (n - b)\\ &= b - r\end{aligned}$$

So

$$\begin{aligned}(a \otimes_n b) + (1 \otimes_b n) &= ((q + 1) \otimes_n b) + r\\ &= (b - r) + r\\ &= b.\end{aligned}$$

Now suppose $k > 0$ and (*a*) and (*b*) are true for $(k - 1)$, and let a be the least number such that $[a,b / n] = k$. Also let u be such that $(a - u)$ is the least number x such that $[x,b / n] = (k - 1)$. Then $[(a - u),b / n] = (k - 1)$, and by the induction hypothesis

$$[n,(k - 1) / b] = (a - u) - 1 \qquad \text{and}$$
$$((a - u) \otimes_n b) + ((k - 1) \otimes_b n) = b.$$

Remark by *Corollary 9.18*, $a \geq q$.

Claim. Either:

(i) $u = q \ \&\ (a - u) \otimes_n b \geq r$ or

(ii) $u = (q + 1) \ \&\ (a - u) \otimes_n b < r$

Pf of Claim:

Suppose $u < q$. Then $[(a - q),b / n] \leq [(a - u),b / n] = k - 1$, using *Prop 9.13a* for the inequality. Since $(a - u)$ is least, this implies that $[(a - q),b / n] \leq (k - 2)$, where *two*(2). But *Props 9.19d and 9.19e* imply that $[(a - q) + q,b / n]$ equals $[(a - q),b / n]$ or $[(a - q),b / n] + 1$, contradicting the fact that $[a,b / n] = k$. Thus $u \geq q$.

Suppose $u \geq (q + 1)$. Then $a > (a - u) + (q + 1)$. So

$$k = [a,b / n] \geq [(a - u) + (q + 1),b / n] \qquad \text{by } \textit{Prop 9.13a}$$

and

$$[(a - u) + (q + 1),b / n] \geq [(a - u),b / n] + 1 = k \qquad \text{by } \textit{Prop 9.19f.}$$

So $[(a - u) + (q + 1),b / n] = k$, contradicting the leastness of a unless $a = (a - u) + (q + 1)$, i.e. $u = (q + 1)$.

Hence $u = q$ or $u = (q + 1)$.

Finally,

$$\begin{aligned}&(a - u) \otimes_n b < r\\ &\Leftrightarrow [(a - u),b / n] = [((a - u) + q),b / n] \qquad \text{by } \textit{Props 9.19d \& 9.19e}.\end{aligned}$$

$[(a - 1),b / n] < [a,b / n]$ by the definition of a, so $u = q$ implies $\neg\ (a - u) \otimes_n b < r$, i.e. $(a - u) \otimes_n b \geq r$. And if $(a - u) \otimes_n b \geq r$, then

$$\begin{aligned}[((a - u) + q),b / n] &= [(a - u),b / n] + 1\\ &= (k - 1) + 1\\ &= k,\end{aligned}$$

and so by the assumption of leastness for a, $((a - u) + q) \geq a$, which forces $u = q$. *End of Pf of Claim.*

Now

$$[n,(k - 1) / b] = q * (k - 1) + [r,(k - 1) / b]$$

and

$$[n,k / b] = q * k + [r,k / b] \qquad \text{both by } \textit{Prop 9.15c}.$$

So,

$$\begin{aligned}[n,k / b] &= [(n,(k - 1) / b] + q + ([r,k / b] - [r,(k - 1) / b])\\ &= (a - u - 1) + q + ([k,r / b] - [(k - 1),r / b]) \qquad (*)\end{aligned}$$

Recall

$$((a - u) \otimes_n b) + ((k - 1) \otimes_b n) = b$$

So

$$((a - u) \otimes_n b) + ((k - 1) \otimes_b r) = b$$

Thus

$$\begin{aligned}(a - u) \otimes_n b < r &\Leftrightarrow (k - 1) \otimes_b r > (b - r).\\ &\Leftrightarrow \neg\, ((k - 1) \otimes_b r) + r < b\\ &\Leftrightarrow [k,r / b] = [(k - 1),r / b] + 1\end{aligned}$$

Hence either:

$$u = q \;\&\; ([k,r / b] - [(k - 1),r / b]) = 0$$

or

$$u = (q + 1) \;\&\; ([k,r / b] - [(k - 1),r / b]) = 1.$$

Plugging into the formula (*), both cases imply

$$[n,k / b] = (a - 1).$$

Finally, it needs to be shown that

$$(a \otimes_n b) + (k \otimes_b n) = b,$$

or equivalently, since $n \equiv r \pmod{b}$,

$$(a \otimes_n b) + (k \otimes_b r) = b,$$

Now $[(a - u),b / n] = k - 1 = [a,b / n] - 1$. Also, $[a,b / n] = [(a - 1),b / n] + 1$, by the leastness of a. Thus

$$[(a - u),b / n] = [((a - u) + (u - 1)),b / n] = [((a - u) + (u - 1) + 1),b / n] - 1.$$

Hence by *Prop 9.19c*,

$$((a - u) + (u - 1) + 1) \otimes_n b = ((a - u) \otimes_n b) + (((u - 1) * b) - (n - b))$$

which becomes

$$a \otimes_n b = ((a - u) \otimes_n b) + ((u - 1) * b - (n - b)).$$

By *Lemma 9.21*,

$$k \otimes_b r = (r + ((k - 1) \otimes_b r)) - ([k,r / b] - [(k - 1),r / b]) * b.$$

Add the last two equations and use the induction hypothesis $((a - u) \otimes_n b) + ((k -1) \otimes_b n) = b$:

$$(a \otimes_n b) + (k \otimes_b r) = r + (u * b) - (n - b) - ([k,r / b] - [(k - 1),r / b]) * b.$$

If $[k,r / b] - [(k -1),r / b] = 0$, then $u = q$; while if $[k,r / b] - [(k - 1),r / b] = 1$, then $u = (q + 1)$. A consideration of both cases results in

$$(a \otimes_n b) + (k \otimes_b r) = b. \qquad \square$$

The next proposition could be proven in greater generality, but the form given suffices for our needs in the proof of Quadratic Reciprocity.

Prop 9.23. Let $one(1)$ & $two(2)$. If $a > b$ & $n = (2 * a) + 1$, then

$$[a,(2 * b) + 1 / n] = b.$$

Pf:

In fact a stronger claim will be proven:

$$\begin{aligned}&(a > b \;\&\; n = (2 * a) + 1)\\ &\Rightarrow [a,(2 * b) + 1 / n] = b \;\&\; ((2 * b) + 1) \otimes_n a = (a - b).\end{aligned}$$

Proceed by induction on b. For the case $b = 0$, note that $[a,1 / n] = 0$ by *Prop 9.12d*, and that $1 \otimes_n a = a$.

Suppose $b > 0$ and the claim true for $(b - 1)$, and let $a > b$ & $n = (2 * a) + 1$. Then $a > (b - 1)$, so by the induction hypothesis,

$$\begin{aligned}&[a,2*(b - 1) / n] = (b - 1)\\ &\& \; ((2 * b) - 1) \otimes_n a = a - (b - 1).\end{aligned}$$

Then

$$(((2 * b) - 1) \otimes_n a) + a = (2 * a) - (b - 1) < (2 * a) + 1 = n.$$

Hence

$$\begin{aligned}(2 * b) \otimes_n a &= (2 * a) - (b - 1) && \text{and}\\ [(2 * b),a / n] &= [(2 * b) - 1,a / n] &&\\ &= [a,(2 * b) - 1 / n] && \text{by } \textit{Prop 9.14}\\ &= b && \text{by the Induction Hypothesis.}\end{aligned}$$

Since $a > b$ and $n = (2 * a) + 1$,

$$\neg\, (2 * a) - (b - 1) + a < n.$$

Hence

$$\begin{aligned}((2 * b) + 1) \otimes_n a &= (2 * a) - (b - 1) - (n - a)\\ &= (2 * a) - (b - 1) - (a + 1)\\ &= (a - b)\end{aligned}$$

and

$$\begin{aligned}[(2 * b) + 1, a / n] &= [(2 * b), a / n] + 1\\ &= b + 1.\end{aligned} \qquad \square$$

9C. Quadratic Reciprocity

Prop 9.24. Let $one(1)$, $two(2)$, $\pi^*(p)$, $(a \,\Delta\, p) = 1$, $\neg\, 2 \mid a$, $(2 * r) = p - 1$. Then $Res(a,p)$ if and only if

$$2\sum_{k=1}^{r} [k,a / p] = 0.$$

(Recall the "2" before the summation sign means that the summation is done modulo 2. It will be dropped for the proof, and any modulo not specified is assumed to be modulo 2.)

Pf:

By *Prop 9.20*, for all k where $1 \le k \le r$,

$$k \otimes_2 a = ([k,a / p] \ \otimes_2 p) \oplus_2 (k \otimes_p a).$$

a and p are odd, so $a \equiv 1$ & $p \equiv 1$. Thus, for all k where $1 \le k \le r$,

$$k = k \otimes_2 a = [k,a / p] \oplus_2 (k \otimes_p a).$$

Summing (modulo 2),

$$\sum_{k=1}^{r} k \ = \ \sum_{k=1}^{r} [k,a / p] \oplus_2 \sum_{k=1}^{r} (k \otimes_p a),$$

equality because both the left- and right-hand sides are either 0 or 1.

By *Lemma 9.8*, $\{x : 1 \le x \le r\}$ are just the numbers $(i \otimes_p a)$ and $(p - (j \otimes_p a))$, where

$$\begin{aligned}&0 < i \le r \ \& \ (i \otimes_p a) \le r \qquad \text{and}\\ &0 < j \le r \ \& \ (j \otimes_p a) > r.\end{aligned}$$

So, summing up these numbers mod 2 (using I and J to indicate the restriction on the indices),

$$\sum_{I} (i \otimes_p a) \oplus_2 \sum_{J} (p - (j \otimes_p a)) = \sum_{k=1}^{r} [k,a / p] \oplus_2 \sum_{k=1}^{r} (k \otimes_p a).$$

Because the sums are modulo 2,

$$\sum_{I}(i \otimes_p a) \oplus_2 \sum_{I}(i \otimes_p a) = 0,$$

so adding $\sum_{I}(i \otimes_p a) \oplus_2 \sum_{J}(j \otimes_p a)$ to both sides,

$$\sum_{J} p = \sum_{k=1}^{r} [k,a/p] \oplus_2 \sum_{k=1}^{r} (2 \otimes_2 (k \otimes_p a)).$$

The last term equals 0, so

$$\sum_{J} p = \sum_{k=1}^{r} [k,a/p].$$

Since $p \equiv 1$, the term on the left-hand-side is 0 if the number of elements in J is even, 1 otherwise. By *Gauss' Lemma 9.9*, this means that the term on the left-hand-side is 0 if *Res*(a,p), 1 otherwise. □

Lemma 9.25. Let *one*(1), *two*(2), $\pi^*(p)$, $\pi^*(q)$, $p > q$, $(2 * r) = (p - 1)$, $(2 * s) = (q - 1)$. Then:

$$r \otimes_2 s = \sum_{i=1}^{r} [q,i/p] \oplus_2 \sum_{i=1}^{s} [p,i/q].$$

Note: all $\sum$ summations are sums modulo 2.

Pf:

It will be shown by induction that, for all k, $1 \leq k < p$,

$$\sum_{i=1}^{k} [q,i/p] \oplus_2 \sum_{i=1}^{f(k)} [p,i/q] = k \otimes_2 f(k),$$

where $f(k) = [k,q/p]$. This suffices, since one may set $k = r$, as then $f(r) = s$ by *Prop 9.23*.

Let $k = 1$. Set $q = (u * p) + v$, where Nu and $v < p$. Remark, since p and q are distinct primes, that $v > 0$, so $q > (u * p)$. Then

$$f(1) = [1,q/p] = 0 \qquad \text{by } \textit{Prop 9.12d}.$$

So,

$$\sum_{i=1}^{f(1)} [p,i/q] = 0,$$

and thus

$$\sum_{i=1}^{1}[q,i\,/\,p] \oplus_2 \sum_{i=1}^{f(1)}[p,i\,/\,q] \equiv_2 f(1) \equiv_2 1 \otimes_2 f(1).$$

Hence equality holds between the left-most and right-most terms, because both are results of operations modulo 2, and so must be either 0 or 1.

Thus the claim holds when $k = 1$.

Now let $k > 1$, and suppose the claim holds for $(k - 1)$. Then:

$$\sum_{i=1}^{k-1}[q,i\,/\,p] \oplus_2 \sum_{i=1}^{f(k-1)}[p,i\,/\,q] = (k - 1) \otimes_2 f(k - 1).$$

Case 1. $f(k) = f(k - 1)$.

Then the claim follows by adding, modulo 2, $f(k - 1) = f(k) = [q,k\,/\,p]$ to both sides.

Case 2. $f(k) = f(k - 1) + 1$.

That is, $[k,q\,/\,p] = [(k - 1),q\,/\,p] + 1$, so k is the least number x such that $[x,q\,/\,p] = \mathrm{f}(k)$. By *Prop 9.22*, $[p,f(k)\,/\,q] = (k - 1)$. Adding $f(k) \oplus_2 [p,f(k)\,/\,q]$ to both sides, the left-hand side becomes

$$\sum_{i=1}^{k}[q,i\,/\,p] \oplus_2 \sum_{i=1}^{f(k)}[p,i\,/\,q],$$

while the right-hand side, given that $[p,f(k)\,/\,q] = (k - 1)$, becomes

$$\begin{aligned}&((k - 1) \otimes_2 f(k - 1)) \oplus_2 f(k) \oplus_2 (k - 1)\\ &\quad = ((k - 1) \otimes_2 (f(k - 1) + 1)) \oplus_2 f(k)\\ &\quad = ((k - 1) \otimes_2 f(k)) \oplus_2 f(k)\\ &\quad = k \otimes_2 f(k)\end{aligned}$$

□

Theorem 9.26, Quadratic Reciprocity (*Gauss*). Let $\pi^*(p)$, $\pi^*(q)$, $\neg\, p = q$, *one*(1), and *four*(4). Then $(Res(p,q) \Leftrightarrow Res(q,p)) \Leftrightarrow (p \equiv_4 1 \vee q \equiv_4 1)$.

Note: all $\sum$ summations in the proof are sums modulo 2.

Pf:

WLOG suppose $p > q$. Let *two*(2).

By *Prop 9.24* it suffices to show that

$$\sum_{k=1}^{r}[k,q\,/\,p] \equiv_2 \sum_{k=1}^{s}[k,p\,/\,q] \Leftrightarrow (p \equiv_4 1 \vee q \equiv_4 1),$$

where $(2 * r) = (p - 1)$ and $(2 * s) = (q - 1)$.

Now

$$\sum_{k=1}^{r}[k,q/p] \equiv_2 \sum_{k=1}^{s}[k,p/q] \Leftrightarrow \sum_{k=1}^{r}[k,q/p] \oplus_2 \sum_{k=1}^{s}[k,p/q] = 0$$

$$\Leftrightarrow r \otimes_2 s = 0 \qquad \text{by } \textit{Lemma 9.25}$$

$$\Leftrightarrow p \equiv_4 1 \vee q \equiv_4 1. \qquad \square$$

10. VARIATIONS.

We will continue to regard consequences of **F** in the next chapter, where the subject will be syntax and consistency proofs. In this chapter a small detour will be taken, and various variations on **F** will be presented.

10A. F.n, F/k, and F.n/k.

Let the formula

$$\exists x_1 \exists x_2 ... \exists x_n \,(\, \mathrm{N}x_1 \;\&\; \sigma 0{,}x_1 \;\&\; \mathrm{N}x_2 \;\&\; \sigma x_1{,}x_2 \;\&\; ... \;\&\; \mathrm{N}x_n \;\&\; \sigma x_{n\text{-}1}{,}x_n\,)$$

be abbreviated σ^n, with σ^0 just N0. And let **F.n** be **F** + $\{\sigma^n\}$. Then **F.n** assumes the existence of all numbers up to and including *n*. For instance, **F.3** supposes that 0,1,2, and 3 exist.

The reader may recall that **F** can prove that *two*(*2) & four*(4) ⇒ (2 + 2) = 4. (This was *Prop 6.16*.) **F.4** is able to prove (2 + 2) = 4.

The sequence **F**,**F.0**, **F.1**, **F.2**, **F.3**, ... is a better and better approximation of **FF**, which, as has been shown, is just **PA2**, full second-order Peano Arithmetic.

The formula σ^n may be unreasonably long, and it will be possible to assert the existence of certain numbers *n* with shorter formula than σ^n.

Restrict now a system **X** to relationships with arity *k* or less, and call the resulting system **X/k**. It can be verified that the development of arithmetic in **F** has used only relationships with arity 2 or less, so the system **F/2** has been used *de facto* here, and is quite powerful. If one takes addition and multiplication as primitive predicates and uses their definitions to state axioms, then one would need to work in **F/3**.

The simplest model of system **F.n/k** has (*n* + 1) first-order entities and 2 ^ ((*n* + 1) ^ *k*) second-order entities of arity *k*, and

$$2 \wedge ((n + 1) \wedge 1) + 2 \wedge ((n + 1) \wedge 2) + ... + 2 \wedge ((n + 1) \wedge (k - 1))$$

second-order entities of arity less than *k*. But this number is < 2 ^ ((*n* + 1) ^ *k*), provided *n* > 0. So these systems have models with a strict upper bound on the number of entities, both first- and second-order.

10B. G

F assumes the existence of only one first-order thing, 0, which, because of the lack of (F5), may or may not be a natural number. **G** does one better and does not even assume the existence of 0 and instead uses a predicate to represent a thing being zero.

Let *zero*(*z*) abbreviate

$$\forall P \,(\, \mathrm{M}z{,}P \Leftrightarrow \neg\, \exists z\, Pz\,)$$

Consider the following axioms:

(G1) $\forall n \forall m \forall P$ (Mn,P & Mm,$P \Rightarrow n = m$)
(G2) $\forall P \forall n$ (Mn,P & $\neg$ *zero*(n) $\Rightarrow \exists x\ Px$)
(G3) $\forall n \forall m \forall P \forall Q \forall a$ (Nn & $\sigma n,m$ & $\neg Pa$ & $Q \equiv (P \cup \{a\})$
$\Rightarrow$ (Mn,$P \Leftrightarrow$ Mm,Q))
(G4) Induction schema. Let ϕ be a well-formed formula. Suppose $\forall n$ (*zero*(n) $\Rightarrow \phi$) and $\forall n \forall m$ (Nn & $\sigma n,m$ & $\phi \Rightarrow \phi\ [m \backslash n]$). Then $\forall n$ (N$n \Rightarrow \phi$).

Remark that (G1) and (G3) are just (F1) and (F3), respectively.

Use **G** to refer to the system with these axioms. **G** has substantially the same power as **F** because of this proposition:

(***G***) *Prop 10.1*. Let $\exists x$ Nx. Then $\exists z$ (Nz & *zero*(z)).
Pf:
Prove $\forall n$ (N$n \Rightarrow \exists z$ (Nz & *zero*(z)) by Induction (G4), with ϕ as

(N$n \Rightarrow \exists z$ (Nz & *zero*(z)). □

Note that by (G1), there can only be one z such that *zero*(z).

Standard two-typed first-order logic assumes that there is at least one thing, so $\exists x\ (x = x)$ is a theorem. This kind of logic limits the usefulness of **G**, since its whole *raison d'etre* is to avoid the assumption of the existence of any first-order thing. With this in mind, it is perhaps better to embed the axioms (G1) to (G4) in a non-standard two-typed first-order logic which does not assume the existence of anything, and so where $\exists x\ (x = x)$ is not a theorem. In this environment **G** can assert the existence of only one second-order thing, for any given arity, namely the empty relationship. Still, **G** is able to develop the same substantial part of arithmetic as **F**.

10C. N (One)

Instead of starting with 0, it is possible to begin with 1. Consider the system **N** with axioms:

(N1) $\forall n \forall m \forall P$ (Mn,P & Mm,$P \Rightarrow n = m$)
(N2) $\forall P \forall n$ (M1,$P \Leftrightarrow \exists x\ P \equiv \{x\}$)
(N3a) $\forall n \forall m \forall P \forall Q \forall a$ (Nn & $\sigma n,m$ & $\neg$ Pa & $Q \equiv (P \cup \{a\})$
& Mn,$P \Rightarrow$ Mm,Q)
(N3b) $\forall n \forall m \forall Q$ (Nn & $\sigma n,m$ & Mm,$Q \Rightarrow \exists a$ (Qa & Mn,($Q \setminus \{a\}$)))
(N4) Induction schema. Let ϕ be a well-formed formula. Suppose $\phi\ [1 \backslash n]$ and $\forall n \forall m$ (Nn & $\sigma n,m$ & $\phi \Rightarrow \phi\ [m \backslash n]$). Then $\forall n$ (N$n \Rightarrow \phi$).

Notice that (F3) no longer appears and has been replaced by (N3a) and (N3b). This is because (N1) + (N2) + (F3) + (N4) could have as model {1,2}, where:

N1 & N2

$$\sigma 1,2 \;\&\; \forall x \neg \sigma 2,x$$
$$\mathrm{M}1,P \Leftrightarrow \exists x\, P \equiv \{x\}$$
$$\mathrm{M}2,P \Leftrightarrow (\neg \exists x\, Px \vee \exists x \exists y\, (\neg x = y \;\&\; P \equiv \{x,y\})).$$

Clearly this model is undesirable.

(N3) makes sense in terrms of counting. If one has counted *P* as *n* and there is one new thing *a* to count, and *m* follows *n* in the natural number series, then one counts *a* as *m*, hence (N3a). And if one has counted *Q* as *m*, and *n* precedes *m* in the natural number series, then one must have counted all but one thing of *Q* as *n*, hence (N3b).

This system like **F** has a model with only one first-order entity. Let us as also change the *Comprehension Axiom Schema* to:

Let ϕ be any formula not containing any free "*P*", and let $n \geq 1$. Then

$$\exists x_1,\ldots,x_n \phi \Rightarrow \exists P\, \forall x_1 \ldots \forall x_n\, (\, Px_1,\ldots,x_n \Leftrightarrow \phi\,).$$

Call this system **N**. Then **N** has a model with only one second-order entity, as well as only one first-order entity.

It remains to verify that **N** can build the whole arithmetical structure constructed in **F**. Here are certain highlights, with the number in parenthesis indicating the corresponding proposition proved by **F**.

(**N**) *Prop 10.2*. (*2.1*) $\forall n \forall P\, (\mathrm{N}n \;\&\; \mathrm{M}n,P \Rightarrow \exists x\, Px)$.
Pf:

By induction, with ϕ as $\forall P\, (\mathrm{N}n \;\&\; \mathrm{M}n,P \Rightarrow \exists x\, Px)$.

$\forall P\, (\mathrm{N}1 \;\&\; \mathrm{M}1,P \Rightarrow \exists x\, Px)$ holds because of (N2).

Now assume Nn & $\sigma n,m$ & ϕ and also Nm & Mm,P. Then by (N3b) there exists *a* s.t. Pa & Mn,(P\{a}). □

(**N**) *Prop 10.3*. (*Finite Hume's Principle*, *2.3*). $\forall n \forall P \forall Q\, (\, \mathrm{N}n \;\&\; \mathrm{M}n,P \Rightarrow (P \sim Q \Leftrightarrow \mathrm{M}n,Q)\,)$.
Pf:

By induction, with ϕ as $\forall P \forall Q\, (\mathrm{N}n \;\&\; \mathrm{M}n,P \Rightarrow (P \sim Q \Leftrightarrow \mathrm{M}n,Q))$.

Assume first N1 & M1,*P*. Then by (N2) $P \equiv \{p\}$ for some *p*. If $P \sim Q$, then evidently $Q \equiv \{q\}$ for some *q*, and so by (N2) M1,*Q*. On the other hand, if M1,*Q*, then by (N2) $Q \equiv \{q\}$ for some *q*, and thus $P \sim Q$.

Now assume Nn & $\sigma n,m$ & ϕ and also Nm & Mm,P. Then by (N3b) there exists *a* s.t. Pa & Mn,($P \setminus \{a\}$). By *Prop 10.2*, $\exists x \neg (P \setminus \{a\})x$.

Suppose $P \sim Q$. Then Ra,b for some *b*, and $R \setminus \{(a,b)\}$ is non-empty and so exists. By logic, $P\setminus\{a\} \sim Q \setminus \{b\}$. By the induction hypothesis, Mn,($Q \setminus \{b\}$). By (N3a) Mm,Q.

Now suppose Mm,Q. Then by (N3b) there exists *b* s.t. Qb & Mn,($Q \setminus \{b\}$). By the induction hypothesis, $P \setminus \{a\} \sim Q \setminus \{b\}$, whence $P \sim Q$. □

It might seem that the system is to weak to recuperate (F3), but with *Hume's Principle* estabilished, it is now in fact possible to do so:

(**N**) *Corollary 10.4*. (F3) $\forall n\forall m\forall P\forall Q\forall a\ (\ \mathrm{N}n\ \&\ \sigma n,m\ \&\ \neg Pa\ \&\ Q \equiv (P \cup \{a\}) \Rightarrow (\mathrm{M}n,P \Leftrightarrow \mathrm{M}m,Q)\ )$

Pf:

One direction is just (N3a). For the other direction, suppose $\mathrm{N}n\ \&\ \sigma n,m\ \&\ \neg Pa\ \&\ Q \equiv (P \cup \{a\})\ \&\ \mathrm{M}m,Q$. Then $Qb\ \&\ \mathrm{M}n,(Q \setminus \{b\})$, for some b, by (N3b). Then $\{(x,y) : (x = y\ \&\ \neg\, x = a\ \&\ \neg\, x = b) \vee (x = a\ \&\ y = b)\}$ exists since the predicate is non-empty. Call it R. By logic and using R, it can be seen that $P \sim (Q \setminus \{b\})$. By *Finite Hume's Principle*, $\mathrm{M}n,P$. □

(**N**) *Prop 10.5. (Pigeon Hole Principle, 2.6)* $\forall n\forall P\forall Q\ (\ \mathrm{N}n\ \&\ \mathrm{M}n,P\ \&\ \mathrm{M}n,Q\ \&\ P \subseteq Q \Rightarrow P \equiv Q\ )$.

Pf:

By induction, with ϕ as $\forall P\forall Q\ (\ \mathrm{N}n\ \&\ \mathrm{M}n,P\ \&\ \mathrm{M}n,Q\ \&\ P \subseteq Q \Rightarrow P \equiv Q\ )$.

When $n = 1$, ϕ follows from (N2).

Now assume $\mathrm{N}n\ \&\ \sigma n,m\ \&\ \phi$ and also $\mathrm{N}m\ \&\ \mathrm{M}m,P\ \&\ \mathrm{M}m,Q\ \&\ P \subseteq Q$. By (N3b) $Pa\ \&\ \mathrm{M}n,(P \setminus \{a\})\ \&\ Qb\ \&\ \mathrm{M}n,(Q \setminus \{b\})$ for some a,b. Since evidently $Q \setminus \{a\} \sim Q \setminus \{b\}$, by *Finite Hume's Principle*, $\mathrm{M}n,(Q \setminus \{a\})$. Evidently $P \setminus \{a\} \subseteq Q \setminus \{a\}$, so by the induction hypothesis, $P \setminus \{a\} \equiv Q \setminus \{a\}$. Thus $P \equiv Q$. □

Perhaps the most important proposition early on which **N** *cannot* prove, is *POTINF*, namely $\forall n\ (\ \mathrm{N}n \Rightarrow \exists P\exists a\ (\mathrm{M}n,P\ \&\ \neg\, Pa))$. *POTINF* is not even true in the singleton model $\{1\}$. Still, **N** can prove

(*WEAKPOTINF*) $\forall n\ (\ \mathrm{N}n \Rightarrow \exists P\ \mathrm{M}n,P)$.

The proof of *WEAKPOTINF* is substantially the same as that in **F** of *POTINF* (see *Section 2D*).

It can be checked that most appeals to *POTINF* in **F**'s reconstruction of arithmetic can in fact be replaced by appeals to *WEAKPOTINF*. Consider, however, the proofs of (PA4) and (PA5), in *Prop 2.9*. (PA4) and (PA5) as stated really need *POTINF*, but they can be modified, in a way which does not detract from their later usefulness, so they can be proven in the context of **N** with only *WEAKPOTINF*. That is, let

(PA4') be $\forall n\forall m\forall m'\ (\ \mathrm{N}n\ \&\ \mathrm{N}m\ \&\ \mathrm{N}m'\ \&\ \sigma n,m\ \&\ \sigma n,m' \Rightarrow m = m'\ )$, and
(PA5') be $\forall n\forall m\forall n'\ (\ \mathrm{N}n\ \&\ \mathrm{N}n'\ \&\ \mathrm{N}m\ \&\ \sigma n,m\ \&\ \sigma n',m \Rightarrow n = n'\ )$.

Then:

(**N**) *Prop 10.6*. (*2.9*) *WEAKPOTINF* $\Rightarrow$ (PA4') & (PA5').

Pf:

Assume *WEAKPOTINF*.

Let $\mathrm{N}n\ \&\ \mathrm{N}n'\ \&\ \mathrm{N}m\ \&\ \mathrm{N}m'\ \&\ \sigma n,m\ \&\ \sigma n',m'$. By *WEAKPOTINF*, $\mathrm{M}m,P$ for some P. By (N3b) $Pa\ \&\ \mathrm{M}n,(P \setminus \{a\})$ for some a.

If $n = n'$, then by (N3a), $\mathrm{M}m',P$, and so by (N1) $m = m'$.

Now suppose $m = m'$. By (N3b) $Pb\ \&\ \mathrm{M}n',(P \setminus \{b\})$ for some b. By logic, $(P \setminus \{a\}) \sim (P \setminus \{b\})$. By *Finite Hume's Principle* (*Prop 10.3*), $\mathrm{M}n,(P \setminus \{b\})$. And so by (N1),

$n = n'$. □

Since (PA6) mentions 0, it must be replaced with the equivalent assertion with 1 replacing 0:

$$\text{(PA6')} \quad \forall n \, (\mathrm{N}n \Rightarrow \neg \, \sigma n{,}1).$$

It can then be proved without even assuming *WEAKPOTINF*:

(**N**) *Prop 10.7*. (*2.10*) (PA6).
Pf:

Let $\mathrm{N}n$ & $\sigma n{,}1$. By (N2), $\mathrm{M}1{,}\{1\}$. By (N3b), $\{1\}a$ and $\mathrm{M}n{,}(\{1\} \setminus \{a\})$. By the first conjunct, $a = 1$. But this contradicts the second conjunct and *Prop 10.2*. □

11. SYNTAX AND CONSISTENCY

In order for a logical system to be able to talk about its own consistency, it is necessary that it be able to represent proofs and syntactic objects which make up proofs, like terms and well-formed formulas. Now terms, wffs, and proofs, are all sequences of symbols, and so the system must, at the bare minimum, have have some manner of representing sequences. **F** has two ways. The first is the way used originally by Godel, where numbers stand for syntactical objects via some kind of coding. The second is to use second-order letters as sequences, as in *Def 7.1*. The two definitions give rise to two non-equivalent definitions of consistency. It will be shown that **F** can show itself Godel consistent and that **N** can show itself consistent in both ways..

The proof of consistency proceeds by contradiction. Suppose **X** (**X** being **F** or **N**) is inconsistent. Then there exists a proof P in **X** of $\neg\, 0 = 0$. This proof, either because it is represented by a Godel code or by a sequence, implies that a large or largish natural number, call it n, exists. It has already been noted that **X** has a model with only one first-order thing, 0. It turns out that n is sufficiently big to be able to define a formula which essentially expresses *true-in-{0}* for all wffs in the proof P. But the axioms or axiom instances used in P must be *true-in-{0}*, and rules of inference can only go from wffs which are *true-in{0}* to other wffs which are *true-in-{0}*. But $\neg\, 0 = 0$ is not *true-in-{0}*. This is a contradiction, hence **X** is not inconsistent. Since the proof is conducted in **X**, **X** has proven its own consistency.

11A. Sequences of Sequences

Sequences are second-order entities, and values of sequences must be first-order entities, so one must use a work-around to talk about sequences of sequences.

Def 11.1. Let Nn. *B is a sequence to n of sequences* - written $SeqOfSeq(B,n)$ - if and only if

$$\begin{aligned}&\forall i \forall j \forall k\ (\ Bi,j,k \Rightarrow i \leq n\ )\\ &\&\ \forall i\ (\ i \leq n \Rightarrow Seq(\{(j,k) : Bi,j,k\})\ )\end{aligned}$$

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

Def 11.2. Suppose $SeqOfSeq(B)$. We say *X is the* i^{th} *sub-sequence of B* if and only if

$$Seq\ (X)\ \&\ \forall j \forall k\ (\ Bi,j,k \Leftrightarrow X_j = k\ ).$$

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

□

Note that, if $SeqOfSeq(B)$ and Bi,j,k, then $(B_i)_j = k$.

11B. Formal Description of the Language

It will be useful to provide a formal description of the language and syntax of **F**, so that it can be seen exactly what needs to be represented in **F**.

The symbols in the language **F** are:

(	*left parenthesis*
)	*right parenthesis*
$\Rightarrow$	*implication connective*
$\neg$	*negation connective*
$\forall$	*universal quantifier*
,	*comma, used to separate arguments in a multi-arity predicate*
;	*semi-colon, used for breaks between different lines of a proof*
$x,y,z,...$	*lower-case variables*
$R,S,T,...$	*upper-case variables*
0	*zero*
σ	*sucessor predicate*
M	*numbering predicate*
N	*is-a-natural-number predicate*
=	*equality*

The first-order terms (*Term1*) are 0 and the lower-case variables.
The second-order terms (*Term2)* are the upper-case variables.
The atomic wffs (*AtomicWff*) must be one of these sorts:

<Term1> = <Term1>	*ex.* $x = y$
N*<Term1>*	*ex.* N0
σ*<Term1>,<Term1>*	*ex.* σx,0
M*<Term1>,<Term2>*	*ex.* Mn,P
<Term2> <SeqTerm1>	*ex.* P0,x,y

where a sequence of first-order terms (*SeqTerm1*) is one of these sorts:

<Term1>
<Term1>,<SeqTerm1>.

The wffs (*Wff*) are one of these sorts:

AtomicWff
(*Wff* $\Rightarrow$ *Wff*)
$\neg$ *Wff*
$\forall$*Term1* (*Wff*)
$\forall$*Term2* (*Wff*)

Remark that according to this definition $\forall x \forall y(x = y \Rightarrow y = x)$ is not a wff. In fact two pairs of parentheses too many must be put in, in order to get a wff: $\forall x(\forall y((x = y \Rightarrow y = x)))$. In practice the extra pairs are not written.

Consider any standard axiomatization of two-typed first-order logic with equality, where comprehension is arithmetic or predicative, and which has two rules of inference, *Modus Ponens* - from ϕ and φ, deduce ($\phi \Rightarrow \varphi$) - and *Generalization* - from *Wff*, infer $\forall$*Term1* (*Wff*) and $\forall$*Term2* (*Wff*).

The axioms of *F* (*Axiom*) are the logical axioms, the three axioms of **F** (F1, F2, and F3), and all instance of the induction rule of inference (F4) written in one line as an axiom schema.

A proof (*Proof*) of a wff *W* is a sequence of wffs, where the last wff in the sequence is just *W* and where each wff in the sequence:

is an axiom, or
follows from previous wffs in the sequence by *Modus Ponens*, or
follows from previous wffs in the sequence by *Generalization*.

11C. Godel Coding and Proof of Godel Consistency

Def 11.3. Let *R* be a sequence to *s*, for some *s*. *n* is said to be *the Godel code of R* if

$$n = (p_1 \wedge R_1) * \ldots * (p_s \wedge R_s),$$

where p_i is the *i*-th prime number. This will be written *GSeq*(*n*,*R*). □

Clearly, if *n* is the Godel code of a sequence, then $n \geq 2$ ^ (length of the sequence).

Remark that there is no claim that every sequence can be represented by a Godel code, which of course is unprovable in **F**. Rather, given a natural number *n* and a sequence *R*, one has defined conditions when the former to represent the latter; no ontological assertion has been made.

Informally, the symbols of **F** will be coded by the number on the same line:

(	0
)	1
⇒	2
¬	3
∀	4
,	5
=	6
x,*y*,*z*,...	even numbers greater than or equal to 11
R,*S*,*T*,...	odd number greater than or equal to 11
0	7
σ	8
M	9
N	10

Formally, define the wff *Term1*(*n*) by

$$\mathit{seven}(n) \vee \exists y \exists z\ ((y + y) = n \ \&\ \mathit{eleven}(z) \ \&\ n \geq z)$$

Define the wff *Term2*(*n*) by

$$\exists z\ (\mathit{eleven}(z) \ \&\ n \geq z \ \&\ \neg \exists y\ (y + y) = n)$$

Define *AtomicWff*(*n*) by

$$\begin{array}{l}
\exists R \exists 1 \exists 2 \exists 3 \; (\; GSeq(n,R) \mathbin{\&} one(1) \mathbin{\&} two(2) \mathbin{\&} three(3) \\
\qquad (\, (Seq(R,2) \mathbin{\&} Term1(R_0) \mathbin{\&} six(R_1) \mathbin{\&} Term1(R_2)) \\
\qquad \lor \; (Seq(R,1) \mathbin{\&} ten(R_0) \mathbin{\&} Term1(R_1)) \\
\qquad \lor \; (Seq(R,3) \mathbin{\&} eight(R_0) \mathbin{\&} Term1(R_1) \mathbin{\&} five(R_2) \mathbin{\&} Term1(R_3)) \\
\qquad \lor \; (Seq(R,3) \mathbin{\&} nine(R_0) \mathbin{\&} Term1(R_1) \mathbin{\&} five(R_2) \mathbin{\&} Term2(R_3)) \,) \,) \\
\lor \; \exists R \exists k \; (\; Seq(R,k) \mathbin{\&} Term2(R_0) \mathbin{\&} Term1(R_k) \mathbin{\&} \\
\qquad \forall i \; (\; 0 < i \le k \mathbin{\&} \exists y \; (y + y) = i \Rightarrow five(R_i)) \mathbin{\&} \\
\qquad \forall i \; (\; 0 < i \le k \mathbin{\&} \neg \exists y \; (y + y) = i \Rightarrow Term1(R_i)) \;).
\end{array}$$

The definition of *Wff* uses some preliminary definitions. First, recall that ^ in the context of second-order letters means concatentation. Secondly, use $\langle x \rangle$ to refer to the singleton sequence whose value is x, i.e. $\{(0,x)\}$.

Then define $Impl(j,k,n)$ by

$$\begin{array}{l}
\exists R \exists S \exists T \exists 1 \exists 2 \; (\; GSeq(j,R) \mathbin{\&} GSeq(k,S) \mathbin{\&} GSeq(n,T) \mathbin{\&} one(1) \mathbin{\&} two(2) \\
\qquad\qquad \mathbin{\&} T \equiv \langle 0 \rangle \wedge R \wedge \langle 2 \rangle \wedge S \wedge \langle 1 \rangle \;).
\end{array}$$

Define $Negat(k,n)$ by

$$\exists R \exists S \exists 3 \; (\; GSeq(k,R) \mathbin{\&} GSeq(n,S) \mathbin{\&} three(3) \mathbin{\&} S \equiv \langle 3 \rangle \wedge R \;).$$

Define $ForAll1(k,n)$ by

$$\begin{array}{l}
\exists R \exists S \exists j \exists 1 \exists 4 \; (\; GSeq(k,R) \mathbin{\&} GSeq(n,S) \mathbin{\&} Term1(j) \mathbin{\&} one(1) \mathbin{\&} four(4) \\
\qquad\qquad \mathbin{\&} S \equiv \langle 4 \rangle \wedge \langle j \rangle \wedge \langle 0 \rangle \wedge R \;\; \wedge \langle 1 \rangle \;),
\end{array}$$

$ForAll2Term2(k,n,j)$ by

$$\begin{array}{l}
\exists R \exists S \exists 1 \exists 4 \; (\; GSeq(k,R) \mathbin{\&} GSeq(n,S) \mathbin{\&} Term2(j) \mathbin{\&} one(1) \mathbin{\&} four(4) \\
\qquad\qquad \mathbin{\&} S \equiv \langle 4 \rangle \wedge \langle j \rangle \wedge \langle 0 \rangle \wedge R \;\; \wedge \langle 1 \rangle \;),
\end{array}$$

$ForAll2(k,n)$ by

$$\exists j \; (\; Term2(j) \mathbin{\&} ForAll2Term2(k,n,j))$$

and $ForAll(k,n)$ by

$$ForAll1(k,n) \lor ForAll2(k,n).$$

Finally, define $Wff(n)$ by

$$\begin{array}{l}
\exists W \exists u \; (\; Seq(W,u) \mathbin{\&} n = W_u \mathbin{\&} \forall i \; (i \le u \Rightarrow (AtomicWff(W_i) \\
\lor \; \exists j \exists k \; (j < i \mathbin{\&} k < i \mathbin{\&} (Impl(W_j,W_k,W_i) \lor Negat(W_j,W_i) \lor ForAll(W_j,W_i))))))
\end{array}$$

It is important to note that n is the Godel number of a wff only if $n \ge 2$ ^ (length of the wff).

Hopefully the reader accepts that one can produce a formula $Axiom_{\mathbf{F}}(n)$, which says that n is the Godel coding of an axiom of **F**. A subscript is employed so that discussion of a different axiomatization, while still working in the same underlying logic, can be undertaken.

Define $\mathit{ModusPonens}(j,k,n)$ by $\mathit{Impl}(j,n,k)$.

Define $\mathit{Generalization}(k,n)$ by $\mathit{ForAll}(n,k)$

And finally define $\mathit{GProof}_{\mathbf{F}}(p,n)$ - meaning p is the Godel code of a proof in **F** of the wff whose Godel code is n - by

$$\exists P \exists u\ (\ \mathit{GSeq}(p,P)\ \&\ \mathit{Seq}(P,u)\ \&\ n = P_u\ \&\ \forall i\ (i \le u \Rightarrow (\mathit{Axiom}_{\mathbf{F}}(P_i) \\ \vee\ \exists j \exists k\ (j < i\ \&\ k < i\ \&\ (\mathit{ModusPonens}(P_j,P_k,P_i) \vee \mathit{Generalization}(P_j,P_i)))))).$$

It is now possible to produce a formula which says that there is no Godel number representing a proof which proves $\neg\ 0 = 0$. This is standardly taken to mean that a system is consistent. However, below some doubt will be cast on this claim, so “consistent” will be prefaced by “Godel” and reserved when unqualified for a later usage. That is, a system is *Godel Consistent* if there is no Godel number representing a proof of $\neg\ 0 = 0$. Formally, $\mathit{GCon}(\mathbf{F})$ if and only if

$$\neg\ \exists p \exists R \exists n \exists 3\ (\ \mathit{GProof}_{\mathbf{F}}(p,n)\ \&\ \mathit{GSeq}(n,R)\ \&\ \mathit{three}(3) \\ \&\ \mathit{Seq}(R,3)\ \&\ \mathit{three}(R_0)\ \&\ \mathit{seven}(R_1)\ \&\ \mathit{six}(R_2)\ \&\ \mathit{seven}(R_3)\ ).$$

It is our claim that **F** can prove $\mathit{GCon}(\mathbf{F})$. The proof proceeds by contradiction, so at the beginning one supposes that $\neg\ \mathit{GCon}(\mathbf{F})$. Thus, for some $p,R,n,3$,

$$(\mathit{Assumption})\ \ \mathit{GProof}_{\mathbf{F}}(p,n)\ \&\ \mathit{GSeq}(n,R)\ \&\ \mathit{three}(3) \\ \&\ \mathit{Seq}(R,3)\ \&\ \mathit{three}(R_0)\ \&\ \mathit{seven}(R_1)\ \&\ \mathit{six}(R_2)\ \&\ \mathit{seven}(R_3).$$

(*Assumption*) will be assumed for the rest of the section. It says that a number, p, representing the proof of a contradiction, exists. It will be shown that p is large enough - indeed, much larger than needed - to construct a limited definition of truth, whereby all wffs used in the proof are true, yet $\neg\ 0 = 0$ is not. This produces a contradiction, and shows that (*Assumption*) is false.

Remark that (*Assumption*) asserts that 3 exists, so it is permitted to assume that 1,2, and 3 exist. It is crucial for the subsequent to note also that, for any wff represented in the sequnce, its Godel number must be greater than or equal to 2 ^ (length of the wff).

The proof relies crucially on the fact that **F** has the following singleton model:

0 satisfies N,
(0,0) does not satisfy σ,
$(0,P)$ satisfies M if and only if $P \equiv \phi$.

This model has only one lower-case entity. So in this model, for any given arity, there are only two sorts of upper-case entities, those which are empty, and those which are satisfied by the unique element of that arity. For instance, for the arity four, there is the empty relationship and the relationship {(0,0,0,0)}.

The limited notion of truth, mentioned a few paragraphs back, will be constructed based on the singleton model. It will be defined in the classical way, by defining first satisfaction for an interpretation of variables, and then talking about satisfaction under all such interpretations. Notice that in the singleton model, lower-case variables can only be interpreted as one entity, 0, so an interpretation is actually only concerned with mapping upper-case variables, and these can be mapped to only two things, either the empty or non-empty relationship. 0 will be used to represent the empty, and 1 the non-empty, relationship.

Formally, call I an *interpretation* if

$$IsFunction(I)\ \&\ Im(I) \equiv \{0,1\}\ \&\ \forall a\ (\ \exists b\ Ia,b \Leftrightarrow Term2(a)\ ).$$

Write this as *Interpret*(*I*).

Informally the following atomic wffs are satisfied under an interpretation *I*:

<*Term1*> = <*Term1*>
N<*Term1*>
M<*Term1*>,<*Term2*> if *I* maps *Term2* to 0 (*empty*)
<*Term2*> <*SeqTerm1*> if *I* maps *Term2* to 1 (*non-empty*)

No other atomic wff is satisfied-in-{0}. Notice how this definition makes sense in the context of the singleton model {0}. The only way to interpret a lower-case letter in the singleton model is as 0. So $x = y$ and Nx must always be satisfied, under any interpretation. Since <*Term1*> must be interpretted as 0, M<*Term1*>,<*Term2*> will be satisfied if and only if <*Term2*> is interpretted as the empty relationship. Similarly, *SeqTerm1* will always be interpreted as a sequence of 0's, so <*Term2*> <*SeqTerm1*> is satisfied precisely when *Term2* is mapped to 1, the non-empty relationship.

Formally, suppose *Interpret*(*I*). Define *AtomSatIn0*(*w*,*I*) by

$$\begin{aligned}
&\exists R\ (\ GSeq(w,R)\ \&\\
&\qquad (\ (Seq(R,2)\ \&\ Term1(R_0)\ \&\ six(R_1)\ \&\ Term1(R_2))\\
&\qquad\ \vee\ (Seq(R,1)\ \&\ ten(R_0)\ \&\ Term1(R_1))\\
&\qquad\ \vee\ (Seq(R,3)\ \&\ nine(R_0)\ \&\ Term1(R_1)\ \&\ five(R_2)\ \&\ Term2(R_3)\ \&\\
&\qquad\quad I(R_3),1\ )))\\
&\ \vee\ \exists R \exists r\ (\ Seq(R,r)\ \&\ Term2(R_0)\ \&\ I(R_0),1\ \&\ Term1(R_r)\ \&\\
&\qquad \forall j\ (\ 0 < j \leq r\ \&\ \exists y\ (y + y) = j \Rightarrow five(R_j))\ \&\\
&\qquad \forall j\ (\ 0 < j \leq r\ \&\ \neg \exists y\ (y + y) = j \Rightarrow Term1(R_j))\ ).
\end{aligned}$$

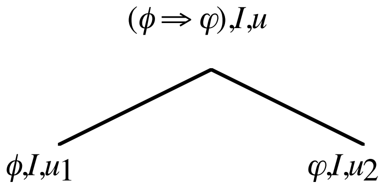
For an interpretation *I* and *t* with *Term2*(*t*), let the *inverse* of *I* on *t* be that *J* (unique up to equivalence) where

$$\forall a \forall b\ (\ \neg\ a = t \Rightarrow (Ia,b \Leftrightarrow Ja,b)\ )\ \&\ \forall b\ (It,b \Leftrightarrow Jt,(1 - b)).$$

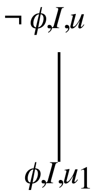
Write *J* as *Inv*(*I*,*t*). Then intuitively,

> $\forall R\ \phi$ is satisfied-in-{0} under intepretation *I* if and only if ϕ is both satisfied-in-{0} under *I* and under *Inv*(*I*,*t*), where *R* is coded by *t*.

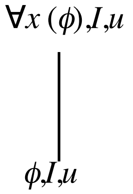
So informally, to construct the definition of satisfaction-in-{0} under *I*, one constructs a tree, where every node is labelled by a three-tuple. One node is distinguished by having only descendents and no ancestors; this is (*W*,*I*,*v*), for some value *v* which is either *true* or *false*. A node labelled by (*A*,*I*,*u*) where *A* is an atomic wff, has no descendents; *u* is *true* if *A* is satisfied-in-{0} under *I*, and *false* otherwise. Otherwise, all nodes have descendents, with there being four cases:



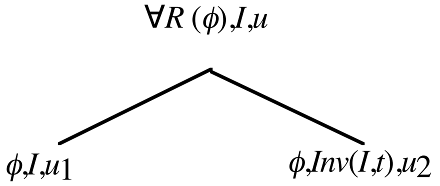
where $u = false$ if $u_1 = true$ and $u_2 = false$, otherwise $u = true$.



where $u = false$ if $u_1 = true$, otherwise $u = true$.



And



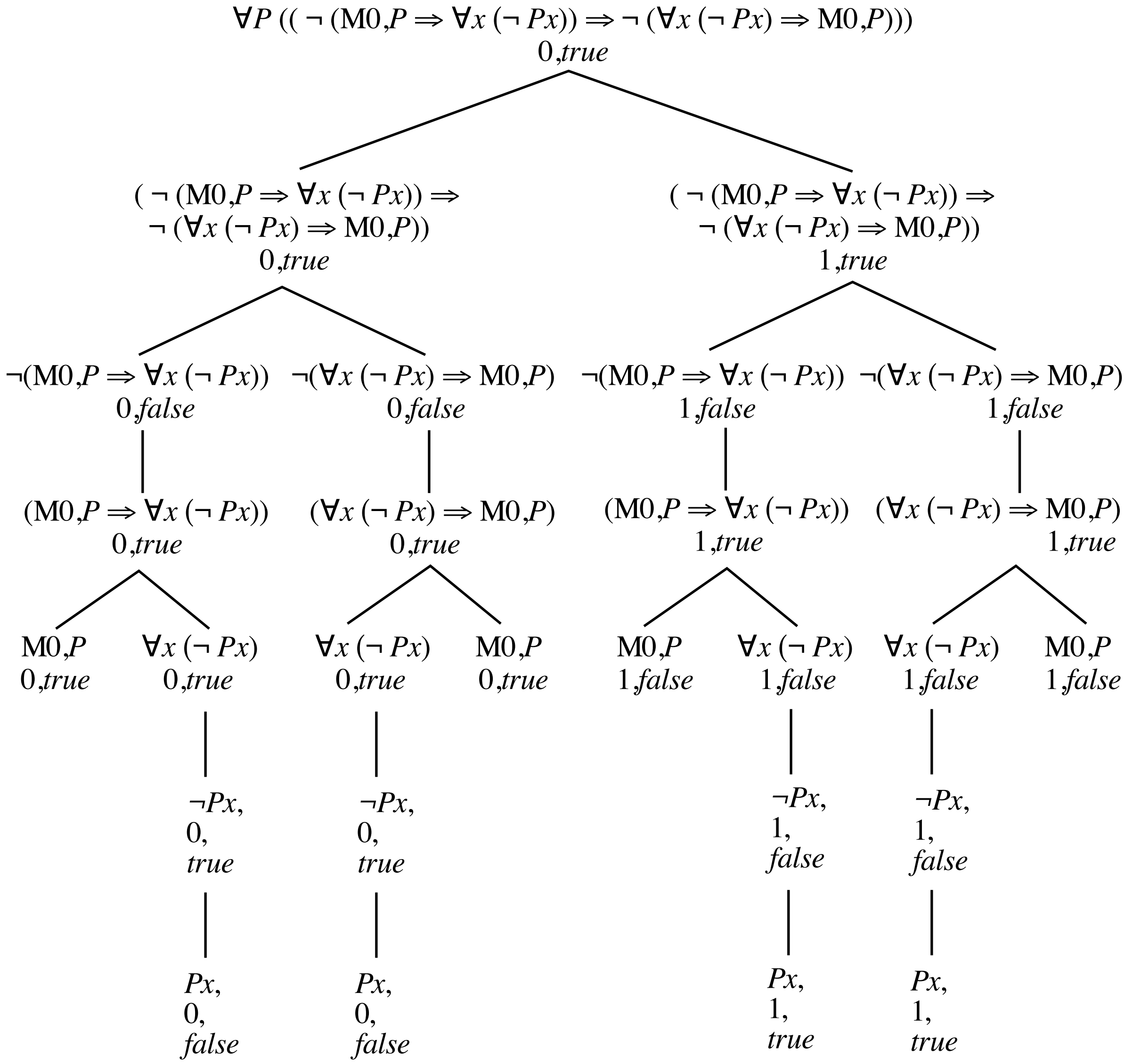
where $u = true$ if $u_1 = true$ and $u_2 = true$, otherwise $u = false$, and where t is the coding of R.

It should be clear that a tree of this type uniquely determines the value of the third tuple v of the distinguished node. W is satisfied-in-{0} under I if $v = true$.

For instance, consider the wff

$$\forall P \neg ((\mathrm{M0},P \Rightarrow \forall x\ (\neg\ Px)) \Rightarrow \neg\ (\forall x\ (\neg\ Px) \Rightarrow \mathrm{M0},P)),$$

There are two possible interpretations, the one (0) which maps P to the empty property, and the one (1) which maps P to the non-empty property. Here is the tree for the wff under the 0 interpretation:



Note that the number of nodes required for a wff is less than 2 ^ *l*, where *l* is the length of the wff, which can be proved by an easy induction.[2] So the number *n* of nodes exists, since *l* exists, and so sequences to *n* can be defined.

To improve perspicacity, use *true* to abbreviate 1 and *false* to abbreviate 0. So *true* - *false* = *true*, while *true* - *true* = *false*.

Let *Interpret*(*P*). Define *SatIn0*(*n*,*P*) by

[2] It is here that an error in the original version of this treatise intervened, as it was wrongly claimed that the number of nodes was less than *n*. The error was all the more inexplicable in that *Consistency* did not make the error.

$\exists W \exists I \exists V \exists F \exists u\ (\ \mathit{Seq}(W,u)\ \&\ \ n = W_u\ \&\ \mathit{SeqOfSeq}(I,u)\ \&\ P \equiv I_u\ \&\ \mathit{true} = V_u$
$\&\ \forall x\ (x \leq u \Rightarrow$
$(\mathit{AtomSatIn0}(W_x,I_x)\ \&\ \mathit{true} = V_x)$
$\vee\ (\mathit{AtomicWff}(W_x)\ \&\ \neg\ \mathit{AtomSatIn0}(W_x,I_x)\ \ \&\ \mathit{false} = V_x)$
$\vee\ \exists j \exists k\ (j < x\ \&\ k < x\ \&$
$((\mathit{Impl}(W_j,W_k,W_x)\ \&\ I_j \equiv I_x\ \&\ I_k \equiv I_x\ \&\ V_x = \mathit{true}\ \text{-}\ V_j * (\mathit{true}\ \text{-}\ V_k))$
$\vee\ (\mathit{Negat}(W_j,W_x)\ \&\ I_j \equiv I_x\ \&\ V_x = \mathit{true}\ \text{-}\ V_j)$
$\vee\ (\mathit{ForAll1}(W_j,W_x)\ \&\ I_j \equiv I_x\ \&\ V_x = V_j)$
$\vee\ \exists t\ (\mathit{ForAll2}(W_j,W_x)\ \&\ \mathit{ForAll2}(W_k,W_x,t)\ \&\ I_j \equiv I_x\ \&\ I_k \equiv \mathit{Inv}(I_x,t)\ \&$
$V_x = V_j * V_k))\ )))).$

And then define *TrueIn0*(*n*) by

$\forall I(\mathit{Interpret}(I) \Rightarrow \mathit{SatIn0}(n,I)\ ).$

It is now just a process of straight-foward checking by induction that every wff in the proof of the contradiction must have a Godel number *n* which is *TrueIn0*(*n*). But the Godel number of "¬ 0 = 0" cannot be *TrueIn0*. This is a contradiction, so (*Assumption*) is false, i.e. *GCon*(**F**), that is, **F** is Godel consistent. Since the reasoning has been formalized in **F**, **F** proves its own Godel consistency.

Not only can **F** prove its own Godel consistency, **F** can prove *stronger* and even *much stronger* systems to be consistent. The same reasoning allows **F** to prove that **F** + (F5) and **F** + (F6) are Godel consistent, since both of these systems also have models with a singleton domain {0}. Indeed **F** + (F5) has the same singleton model as **F**, while **F** + (F6) has the model {0} where

0 does *not* satisfy N,
(0,0) does not satisfy σ,
(0,*P*) satisfies M if and only if $P \equiv \phi$

Even with the addition of full (impredicative) comprehension to **F**, **F** + (F5), and **F** + (F6) both retain a model of one element. That is **F** (with only predicative comprehension) can prove the Godel consistency of these extensions with *full* comprehension. Note that **F** + (F6) with full comprehension is in fact a very strong theory, and in particular once a natural number exists (from which (F5) follows, by *Prop 1.1*), it becomes **PA2** (because **F** + (F5) + (F6) + {full comprehension} is just **PA2**).

A slight adaption in our argument allows **F** to prove the Godel consistency of systems which are stronger ontologically. Suppose ¬ *GCon*(**X**), for some system **X**. Then $\mathit{Proof}_{\mathbf{X}}(p,n)$, where *p* represents a proof and *n* represents the wff ¬ 0 = 0. It can be seen that *p* must be greater than 2 ^ (2 ^ *n*)), where *n* is the length of the longest wff in the proof. In particular, since ¬ 0 = 0 is the last step in any such proof, *p* must be greater than 2 ^ (2 ^ 4)).

Consider **X** = **F.1/3**, that is a system whose language is limited to 3-arity relationships or less, and which asserts the existence of the number 1. **F** proves the Godel consistency of **F.1/3**. For **F.1/3** has two first-order entities, and 2 ^ (2 ^ 3) second-order entities of arity 3, and fewer than 2 ^ (2 ^ 3) of arity less than 3. It is then possible to follow the proof of consistency given in the previous section, because one can have separate interpretations sequences for first-order, second-order of arity 3, and second-order of less than arity 3, with the result that the largest number needed is 2 ^ (2 ^ 3), which exists because it is less than *p*.

The same reasoning shows that **F** can prove the Godel consistency of **F.2/3**, because this system has three first-order entities and 2 ^ (3 ^ 3) second-order entities of arity 3. But clearly any proof of inconsistency must have at least one wff with length greater than 5, so p > 2 ^ (2 ^ 5)) > 2 ^ (3 ^ 3).

That is, **F** can prove that it is Godel consistent to assume the existence of 1 and 2 (when arities are less than 3). Clearly this is not the best possible result, and more research should be able to determine one. Remark that, given any n, **F.n/k** has a model where the number of possible entities is less than some large bound. It would then appear possible to construct a proof where one uses multiple variables to represent interpretations. In its extreme form, one could use a second-order variable I_i to represent the *ith* possible interpretation. That is, $I_i n,x$ would mean that in the *n*th element of a sequence, the variable represented by x is mapped to the *i*th interpretation. One would, of course, need many, many I_i, and it would quickly become questionable whether one could actually write such a proof down.

Ideally, one would like **F** to be able to prove, $\forall n \forall k$ *GCon*(**F.n/k**).

One can make the problem of showing the Godel consistency of **F.n/k** much easier by choosing a different coding. That is, once one has accepted the idea of using numbers to code sequences and thus proofs, then it would seem one must also be willing to accept Godel codings which use different rules and indeed rules involving much larger numbers. One could, for instance, multiply each code by some fixed (huge) constant and still have a well-defined coding scheme. Or one could use a coding based on the Ackermann function,which would create very huge numbers very quickly. With such codings it would be straight-foward to bound the number of second-order entities of **F.n/k** by the number used to code any possible proof of ¬ 0 = 0, and thus, by the usual reasoning, one could show **F.n/k**'s Godel consistency, modulo the coding.

11E. Intensionally Correct?

Return now to the question of the intensional correctness of *GCon*(**F**). What *GCon*(**F**) *really* says, is that there does not exist a number representing, under a Godel coding scheme, a proof which ends in contradiction. But this would not be the same thing as consistency itself. Indeed, it would seem conceivable that there is a proof of a contradiction, but that there are just no numbers big enough to represent the proof. So the proof that there is no such number cannot be taken to mean there is no proof of an inconsistency; maybe it's that, but maybe it's just because the number is too big.

That is, ¬ *GCon*(**F**) asserts *more* than **F**'s inconsistency, since it also asserts the existence of certain very big numbers. So *GCon*(**F**) asserts *less* than **F**'s consistency. Godel consistency is a weaker assertion than consistency.

11F. Wffs and Proofs as Sequences

With intensional correctness in mind, let us remove as much coding as possible. Some coding is necessary, because symbols need to be expressed in the system of **F** in a way that **F** can reason about them. Since **F** has been built to reason about numbers, symbols need to be coded as numbers. But other than that, there need be no coding. A proof is a sequence of wffs, and wffs are themselves sequences of symbols. So a proof will be defined to be a sequence of sequences of symbols. To emphasize this point: a sequence of sequences is not a code for the proof; it *is* the proof. In this way, the formulation of consistency will be intenstionally correct, or at least, as intensionally correct as is possible given the initial conditions.

It is straight-foward to recast the argument in the previous section without Godel coding, beyond that necessary to represent the symbols of the language in terms of numbers. First, one maintains the codings

(	0
)	1
$\Rightarrow$	2
$\neg$	3
$\forall$	4
,	5
=	6
0	7
σ	8
M	9
N	10

and the definitions *Term1*(n) as

$$seven(n) \vee \exists y \exists z\ ((y + y) = n \ \&\ eleven(z) \ \&\ n \geq z)$$

and *Term2*(n) as

$$\exists z\ (eleven(z) \ \&\ n \geq z \ \&\ \neg \exists y\ (y + y) = n).$$

After that, one does not need to use codings at all; sequences suffice. So one says that R is an atomic wff and writes *AtomicWff*(R) if

$$\begin{aligned}
&\exists 1 \exists 2 \exists 3\ (\ one(1) \ \&\ two(2) \ \&\ three(3) \\
&\qquad (\ (Seq(R,2) \ \&\ Term1(R_0) \ \&\ six(R_1) \ \&\ Term1(R_2)) \\
&\qquad \vee (Seq(R,1) \ \&\ ten(R_0) \ \&\ Term1(R_1)) \\
&\qquad \vee (Seq(R,3) \ \&\ eight(R_0) \ \&\ Term1(R_1) \ \&\ five(R_2) \ \&\ Term1(R_3)) \\
&\qquad \vee (Seq(R,3) \ \&\ nine(R_0) \ \&\ Term1(R_1) \ \&\ five(R_2) \ \&\ Term2(R_3))\ )\ ) \\
&\ \vee \exists k\ (\ Seq(R,k) \ \&\ Term2(R_0) \ \&\ Term1(R_k) \ \& \\
&\qquad \forall i\ (\ 0 < i \leq k \ \&\ \exists y\ (y + y) = i \Rightarrow five(R_i)) \ \& \\
&\qquad \forall i\ (\ 0 < i \leq k \ \&\ \neg \exists y\ (y + y) = i \Rightarrow Term1(R_i))\ ).
\end{aligned}$$

And one defines *Wff*(R) as

$$\begin{aligned}
&\exists W \exists u\ (\ SeqOfSeq(W,u) \ \&\ R \equiv W_u \ \&\ \forall i\ (i \leq u \Rightarrow (AtomicWff(W_i) \\
&\vee \exists j \exists k\ (j < i \ \&\ k < i \ \&\ (Impl(W_j,W_k,W_i) \vee Negat(W_j,W_i) \vee ForAll(W_j,W_i)))))),
\end{aligned}$$

where the definitions of *Impl*, *Negat*, and *ForAll* have been changed appropriately. And finally one defines $Proof_{\mathbf{F}}(P,R)$ as

$$\begin{aligned}
&\exists u\ (\ SeqOfSeq(P,u) \ \&\ R \equiv P_u \ \&\ \forall i\ (i \leq u \Rightarrow (Axiom_{\mathbf{F}}(P_i) \\
&\vee \exists j \exists k\ (j < i \ \&\ k < i \ \&\ (ModusPonens(P_j,P_k,P_i) \vee Generalization(P_j,P_i))))),
\end{aligned}$$

where again $Axiom_{\mathbf{F}}$, *ModusPonens*, and *Generalization* have been defined appropriately.

It is now possible to exhibit a formula which says there is no sequence which is a proof of $\neg\, 0 = 0$. Formally, *Con*(**F**) if and only if

$$\neg\, \exists P \exists R \exists 3\ (\ \mathit{Proof}_{\mathbf{F}}(P,R)\ \&\ \mathit{three}(3)\\ \&\ \mathit{Seq}(R,3)\ \&\ \mathit{three}(R_0)\ \&\ \mathit{seven}(R_1)\ \&\ \mathit{six}(R_2)\ \&\ \mathit{seven}(R_3)\ ).$$

Whereas the negation of Godel consistency asserts the existence of a huge number (the Godel coding of a sequence of Godel codings, that is an exponential of an exponential), the negation of *Con*(**F**) asserts the existence of numbers only as large as the length of the proof and the lengths of the wffs in the proof. The proof of *Con*(**F**) cannot go through as the proof of Godel consistency did, because of the need for numbers as large as 2 ^ (length of a wff) to define satisfaction. Nonetheless, **N** *does* show *Con*(**N**) because it has a model with only one second-order, as well as only one first-order, entity. This means there are no branchings needed for big-letter quantified formula in the definition of satisfaction, and so the number of nodes in the tree can be shown to be less than or equal to the length of the *wff*. The rest of the proof goes through exactly in the same way as the proof of *GCon*(**F**). Thus **N** proves *Con*(**N**).

Con(**X**) is a stronger condition than *GCon*(**X**), because $\mathit{Proof}_{\mathbf{X}}$ is a weaker condition that $\mathit{GProof}_{\mathbf{X}}$. That is, let *ReprProof(p,P)* define the relationship of a Godel code *p* of a proof which is a sequence *P*. Then

$$\mathit{GProof}_{\mathbf{X}}(p,r) \Rightarrow \exists P \exists R\ (\ \mathit{ReprProof}(p,P)\ \&\ \mathit{GSeq}(r,R)\ \&\ \mathit{Proof}_{\mathbf{X}}(P,R)),$$

but not

$$\mathit{Proof}_{\mathbf{X}}(P,R) \Rightarrow \exists p \exists r\ \ (\ \mathit{ReprProof}(p,P)\ \&\ \mathit{GSeq}(r,R)\ \&\ \mathit{GProof}_{\mathbf{X}}(P,R)),$$

the latter not holding because the Godel codes of a proof and a wff are much bigger than the length of the proof and the wff, so the existence of the Godel code cannot be inferred from the existence of the sequences *P* or *R*. This adds support to our contention that Godel consistency is actually a weaker condition than consistency itself. On the other hand, unless one wants to take a very hard line on the possible synonymy of different expressions, it would seem that $\mathit{Proof}_{\mathbf{X}}(P,R)$ is a fair way of expressing something to be a proof of a wff in system **X**, and accordingly *Con*(**X**) is a fair way of expressing the consistency of **X**.

It seems appropriate, then, to say that a system **X** is *consistent* if *Con*(**X**). So **N** proves that **N** is consistent, *really consistent*. **N** is *auto-consistent*.

Note that, even though $\exists P\ \mathit{Proof}_{\mathbf{X}}(P,R)$ seems to express well that *R* is provable in system **X**, it does not satisfy the Lob-Hilbert-Bernays conditions of provability:

(*i*) if $\vdash_{\mathbf{X}} A$, then $\vdash_{\mathbf{X}}$ *Provable*("*A*");

(*ii*) $\vdash_{\mathbf{X}}$ *Provable*("*A* ⇒ *B*") ⇒ (*Provable*("*A*") ⇒ *Provable*('*B*"));

(*iii*) $\vdash_{\mathbf{X}}$ *Provable*("*A*") ⇒ *Provable*("*Provable*("*A*")").

For, given a proof of *A*, there is no assurance that there exists a Godel code of "*A*", since this would be a much larger number than anything implicit in the proof. And so (*i*) falls down. Similarly for (*iii*). The Lob-Hilbert-Bernays conditions are too strong, and are suitable only for systems where one is sure of being able to code any syntactical object and to construct proofs of any length, which of course is not the case for **F** or **N**. That is, these conditions imply, given a proof of *A* in a system **X**, that *Provable*("*A*"), *Provable*("*Provable*("*A*")"), *Provable*("*Provable*("*Provable*("*A*")")"), etc. exist *ad infinitum*. But this is less a condition on provability than a condition of expressibility in the system.

N proves stronger systems consistent. Let (N5) be:

(N5) N1

Then **N** proves **N** + (N5) and **N** + (F6), both with full comprehension (modified to exclude the empty predicates).

12. FUTURE TOPICS

1) Show that **F** proves Fermat Last's Theorem.

2) Show that **F** proves the Prime Number Theorem.

3) Can **F** prove its own consistency? (If not possible, prove not, or prove the claim equivalent to another proposition.)

4) Can **F** prove $\forall n\ \mathit{Con}(\mathbf{F.n}/2)$? $\forall n\ \mathit{Con}(\mathbf{F.n}/3)$? $\forall n \forall k\ \mathit{Con}(\mathbf{F.n/k})$? (If not possible, prove not.)

5) Develop analysis using an agnostic philosophy.

6) The author expects that theories of physics which most closely fit with the actual world as we observe it should be based on mathematics which is agnostic about the *Successor Axiom* and which assumes of spacetime neither that it is discrete or that it is continuous. That is, the author conjectures that it is possible to develop a meaningful physical theory in which spacetime is neither assumed to be continuous or discrete.

BIBLIOGRAPHY

Bernays, Paul. *On Platonism in Mathematics*. In: Paul Benacerraf & Hilary Putnam (eds.), ***Philosophy of Mathematics***. Prentice-Hall, 1964.

Boolos, George. ***Logic, Logic, and Logic***. Harvard University Press, 1998.

Boolos, George, and Jeffrey, Richard. ***Computability and Logic***. Cambridge University Press, 1974.

Boucher, Andrew. *Systems for a Foundation of Arithmmetic*, 2001. On web site, www.andrewboucher.com/papers.

Boucher, Andrew. *"True" Arithmetic can Prove its Own Consistency*, 2002. On web site, www.andrewboucher.com/papers.

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

Boucher, Andrew. *Equivalence of* ***F*** *with a Sub-Theory of Peano Arithmetic*, 2005. On web site, www.andrewboucher.com/papers.

Boucher, Andrew. *The Existence of Numbers (Or: What is the Status of Arithmetic?)*, 2001. On web site, www.andrewboucher.com/papers.

Burgess, John. ***Fixing Frege***. Princeton University Press, 2005.

Burton, David. **Elementary Number Theory**. Allyn and Bacon, Inc., 1976.

Buss, Samuel. *Nelson's Work on Logic and Foundations and Other Reflections on Foundations of Mathematics*, to appear. On web site, http://www.math.ucsd.edu/~sbuss/ResearchWeb/nelson/index.html.

Feferman, Solomon. *Arithmetization of metamathematics in a general setting,* ***Fundamenta Mathematicae***, vol. 49 (1960), pp. 35-92.

Ferreira, Fernando, *Amending Frege's Grundgesetze der Arithmetik*, **Synthese** Vol.147 (2005), pp. 3-19.

Field, Hartry. *The Conceptual Contingency of Mathematical Objects*. ***Mind***. Vol 102 (1993), pp. 285-299.

Frege, Gottlob. ***The Foundations of Arithmetic***, trans. by J.L. Austin. Northwestern University Press, 1953.

Frege, Gottlob. ***Grundgesetze der Arithmetik***. Georg Olms Verlagsbuchhandlung, 1966.

Gandy, R.O. *Limitations to Mathematical Knowledge*. In: D. van Dalen, D. Lascar, J. Smiley (eds.), ***Logic Colloquium '80***. North-Holland Publishing Company, 1982.

Gauthier, Yvon. ***Internal Logic: Foundations of Mathematics from Kronecker to Hilbert.*** Synthese Library, Vol. 310. Kluwer Academic Publishers, 2002.

Gauthier, Yvon. *The Internal Consistency of Arithmetic With Infinite Descent*. ***Modern Logic***, Vol. 8 no 1/2 (Jan 1998-Apr 2000), pp. 47-86.

Godel, Kurt. *Uber formal unentscheidbare Satze der Principia Mathematica und verwandter Systeme I.* ***Monatshefte fur Mathematik und Physic***. Vol. 38, pp. 173-98. Translated as *On formally undeciable propositions of the Principia Mathematica*. In: J. van Heijenoort (ed.), ***From Frege to Godel***. Harvard University Press, 1967.

Hardy, G.H. & Wright, E.M. ***An Introduction to the Theory of Numbers***. Clarendon Press, 1938.

Heck, Richard. *Finitude and Hume's Principle*. ***Journal of Philosophical Logic***, Vol. 26 (1997), pp. 589-617.

Heck, Richard. *The Finite and the Infinite in Frege's Grundgesetze der Arithmetik*. In: M. Schirn (ed.), ***The Philosophy of Mathematics Today***. Clarendon Press, 1998, pp. 429-66.

Heck, Richard. *Cardinality, Counting, and Equinumerosity*. ***Notre Dame Journal of Formal Logic***. Vol. 41 (2000), pp. 187-209.

Hilbert, David. *On the Infinite*. In: Paul Benacerraf & Hilary Putnam (eds.), ***Philosophy of Mathematics***. Prentice-Hall, 1964.

Isles, David. *What Evidence is There That 2^65536 is a Natural Number?* ***Notre Dame Journal of FormalLogic,*** Vol. 33 nr. 4 (1992), pp. 465-480.

Isles, David. *A Finite Analog to the Löwenheim-Skolem Theorem*. ***Studia Logica***, Vol. 53 (1994), pp. 503-532.

Jeroslow, R. *Consistency statements in formal mathematics*, ***Fundamenta Mathematicae***, vol. 72 (1971), pp. 17-40.

Lavine, Shaughan. ***Understanding the Infinite***. Harvard University Press, 1994.

Linnebo, Oystein. *Predicative Fragments of Frege Arithmetic*. ***Bulletin of Symbolic Logic***. Vol 10, Issue 2 (2004), pp. 153-174.

Mycielski, *Analysis Without Actual Infinity*. ***Journal of Symbolic Logic***, Vol. 46 (Sep 1981), pp. 625-633.

Nelson, Edward. ***Predicative Arithmetic***. Princeton University Press, 1986.

Parikh, Rohit. *Existence and Feasibility in Arithmetic*. ***Journal of Symbolic Logic***, Vol. 36, Issue 3 (Sep. 1971), pp. 494-508.

Parsons, Charles. *Frege's Theory of Number*. In: Max Black (ed.), ***Philosophy in America***, Cornell University Press (1965), pp. 180-203.

Parsons, Charles. *Developing Arithmetic in Set Theory without Infinity: Some Historical Remarks*. ***History and Philosophy of Logic***, Vol. 8 (1987), pp. 201-213.

Raatikainen, Panu. *The Concept of Truth in a Finite Universe*. ***Journal of Philosophical Logic***, Vol. 29 (2000), pp. 617-633.

Robinson, R.M. *An Essentially Undecidable Axiom System*, ***Proc. Int. Cong. Math.***, Vol. 1 (1950), pp. 729-730.

Rotman, Brian. ***Ad Infinitum - The Ghost in Turing's Machine: Taking God out of Mathematics and Putting the Body Back in : An Essay in Corporeal Semiotics***. Stanford

University Press, 1993.

Shapiro, Stewart. ***Foundations without Foundationalism: A Case for Second-Order Logic***. Clarendon Press, 1991.

Tait, William W. *Finitism*. ***Journal of Philosophy***, Vol 78 (1981), pp 524-546.

Tennant, Neil. ***Anti-Realism and Logic: Truth as Eternal***, especially Chapter 25 (pp. 275-300). Clarendon Press, 1987.

Tennant, Neil. *On the Necessary Existence of Numbers*. ***Noûs***. Vol. 31 (1997), pp. 307-336.

Willard, Dan. *Self-verifying Axiom Systems, The Incompleteness Theorem and Related Reflection Principles*. ***Journal of Symbolic Logic***, Vol. 66 (2001), pp. 536-596.

Wright, Crispin. ***Frege's Conception of Numbers as Objects***. Aberdeen University Press, 1983.

Yessenin-Volpin, A.S. *Le programme ultra-intuitioniste des fondements des mathématiques*. In: ***Infinitistic Methods, Proceedings of the Symposium on Foundations of Mathematics. Warsaw, 2-9 Sept 1959***. Pergamon Press, Oxford, 1961, pp. 201-223.

Yessenin-Volpin, A.S. *The ultra-intuitionistic criticism and the antitraditional program for foundations of mathematics*. In: Kino, Myhill, and Vesley (eds.), ***Intuitionism & proof theory: Proceedings of the Summer Conference at Buffalo, N.Y. 1968***. North-Holland Publishing Company, 1970, pp. 3-45.

Yessenin-Volpin, A.S. *About infinity, finiteness and finitization*. In Richman, F. (ed.), ***Constructive Mathematics (Proceedings of the Conference at Las Cruces, New Mexico, August 1980) Lecture Notes in Mathematics 873***. Springer-Verlag, (1981), pp. 274-313.