Questioning Articles of Faith

A re-creation of the history and theology of arithmetic

David Isles[1]

> Inasmuch as many have taken in hand to set in order a narrative of those things which are most surely believed among us, . . . , it seemed good to me also . . . to write to you an orderly account.
>
> Luke 1:1,3 Bible (New King James Version)

There are three parts to this article. The first is a very brief sketch of the historical development of numerical notations and arithmetic operations on them. Like many such sketches it reinterprets many features of this development and omits most of them. It corresponds to the sort of folk history that St. Luke may have depended on as he tried to write a seamless biography of an individual whose living memory was even then being lost.

Second is an equally brief sketch of an ideological reworking of this historical material into a coherent intellectual narration. St. Luke did not simply write a biography, he wrote a story which gained coherence because of its theology.

Finally, some of the assumptions of this ideology are criticized and alternative approaches suggested.

A re-creation of the history

People counted, people tallied. Over time civilizations developed many notational systems to record these counts using a variety of media: knots on string, pictographs on stone, marks on paper, beads on an abacus, electric charges in computers. Among the simplest of these notational systems were the numerals: | , || , ||| , ... Simultaneously a variety of computations using these notations evolved. At first they were carried out with stones, boards, beads, etc. but later (especially after the invention of positional notation) done directly with the notations themselves.[2] Eventually these computations were done on paper and involved notations similar to the following set.

Definition 1 The *exponential numerical terms* consist of the collection of terms built from |, + (addition), $*$ (multiplication), and ^ (exponentiation) together with left and right parentheses.

---

[1] Submitted to the Forum by Richard L. Epstein. Refereed and accepted for publication by Richard L. Epstein and Walter A. Carnielli.

[2] The Mayans had positional notation together with a zero (see Ifrah, 1985, pp. 397-428). I have not been able to learn whether they developed algorithms for manipulating these notations analogous to our paper based algorithms for addition and multiplication.

Bulletin of Advanced Reasoning and Knowledge 2 (2004) 51–59.

Examples of this definition include: $||$, $(|| + |||)$, $(|| + |||) * (|||)$, $((||\,\hat{}\,|||) + (||)) * (|| + |)$.

Many algorithms for doing addition, multiplication, and exponentiation were developed over time. A contemporary version of these is the following set of rewriting rules.

Definition 2 Let A, B, C, and D be exponential numerical terms.

a. We define a notion $A \sim B$, read as A *immediately reduces* to B:

a1. $A \sim A$

a2. If $A \sim C$ and $B \sim D$, then $A| \sim C|$, and $(A + B) \sim (C + D)$, and $(A * B) \sim (C * D)$, and $(A\,\hat{}\,B) \sim (C\,\hat{}\,D)$.

a3. If $A \sim C$ and $B \sim D$, then

$$(A + |) \sim (C|) \qquad (A + (B|)) \sim ((C + D)|)$$
$$(A * |) \sim C \qquad A * (B|) \sim (C * D) + C$$
$$(A\,\hat{}\,|) \sim C \qquad (A\,\hat{}\,(B|)) \sim (C\,\hat{}\,D) * C$$

b. We define $A > B$, read as A *reduces* to B, as the transitive closure of $\sim$.

Whether one uses these rules or other algorithms, it sometimes happens that two superficially different exponential numerical terms reduce to a common term.

Example $(||\,\hat{}\,||) > (|| + ||)$ and $|| * || > || + ||$.

Analysis

$$\frac{||>|| \qquad |>|}{(||\,\hat{}\,||) > (||\,\hat{}\,|) * ||} \; > \; \frac{\dfrac{||>||}{(||\,\hat{}\,|) > ||} \quad ||>||}{(||\,\hat{}\,|) * || > || * ||} \qquad \frac{||>|| \qquad |>|}{|| * || > (|| * |) + ||} \; > \; \frac{\dfrac{||>||}{(|| * |) > ||} \quad ||>|}{(|| * |) + || > || + ||}$$

In such a case it seems natural to consider such terms as equivalent. In contemporary terminology we have the following definition.

Definition 3 If A and B are exponential numerical terms then $A = B$ means that there is a term S (not necessarily a numeral) such that $A > S$ and $B > S$.

The notation "=" is used for this relation because a variant of the proof of the Church-Rosser Theorem for lambda terms guarantees that if $A = B$ and $B = C$ (that is, there are terms T and S so that both $A > T$ and $B > T$ and also $B > S$ and $C > S$) then $A = C$ (that is, there is a term V so that $A > V$ and $C > V$).[3]

Such considerations probably led people to regard the numerals as the basic numerical notations, while taking the elaboration to exponential numerical terms as just a notational convenience. Moreover, this belief was strengthened by the fact that every time the complete reduction of a term was achieved, the result was

[3] The Church-Rosser argument establishes the "diamond property": If $B > T$ and $B > S$ then there is a term V so that $T > V$ and $S > V$ (from which it follows that $A > T > V$ and $C > S > V$). The diamond property for the relation $>$ follows from that for the relation $\sim$, and the diamond property for $\sim$ is established by induction on the sum of the depths of the derivation trees of $B > T$ and $B > S$. This proof was due to Tait and Martin-Löf; see Barendregt, 1977, p. 1102.

seen to be a numeral. When mathematical sophistication had reached a point where people started asking questions about the underlying structures involved in doing arithmetic, this attitude led to a revised view of what one was actually dealing with.

An orderly account

The Creed The basic entities are the numerals (or, perhaps, abstract quantities, "natural numbers", which are generated in a manner parallel to the numerals) plus (total) functions on these numerals.

From this standpoint, therefore, the exponential numerical terms are merely names indicating the application of these functions (addition, multiplication, and exponentiation) to the numerals. In order to develop the consequences of this Creed in a systematic way, in particular in order to establish the existence of these functions, a logical narrative was devised. This was framed using classical logic within a first-order system that included as predicates $x = y$, $\mathrm{A}(x, y, z)$, $\mathrm{M}(x, y, z)$ and $\mathrm{P}(x, y, z)$ (which could be interpreted over the exponential numerical terms as $x = y$, $x + y = z$, $x * y = z$, and $x \wedge y = z$.) The narrative took the form of proofs of statements about these relations from the following assumptions:

E1 $(x)\,(x = x)$

E2 $(x)\,(y)\,(x = y \rightarrow y = x)$

E3 $(x)\,(y)\,(z)\,(x = y \;\&\; y = z \rightarrow x = z)$

E4 $(x)\,(y)\,(x = y \rightarrow x| = y|)$

E5 $(x) \sim (x| = |)$

E6 If Q stands for any of the three predicates A, M, or P:
$(x)\,(y)\,(z)\,(w)\,(x = y \rightarrow (\,(\mathrm{Q}(x, z, w) \rightarrow \mathrm{Q}(y, z, w))\;\&$
$(\mathrm{Q}(z, x, w) \rightarrow \mathrm{Q}(z, y, w))\;\&\;(\mathrm{Q}(z, w, x) \rightarrow \mathrm{Q}(z, w, y))\,)\,)$

F1 $(x)\,(y)\,(\,x| = y| \rightarrow x = y)$

F2 If Q stands for any of the three predicates A, M, or P:
$(x)\,(y)\,(z)\,(w)\,(\mathrm{Q}(z, w, x)\;\&\;\mathrm{Q}(z, w, y) \rightarrow x = y)$

R1 $(x)\,\mathrm{A}(x, |, x|)$

R2 $(x)\,(y)\,(z)\,(\mathrm{A}(x, y, z) \rightarrow \mathrm{A}(x, y|, z|))$

R3 $(x)\,\mathrm{M}(x, |\,, x)$

R4 $(x)\,(y)\,(z)\,(w)\,(\,\mathrm{M}(x, y, z)\;\&\;\mathrm{A}(z, x, w) \rightarrow \mathrm{M}(x, y|, w))$

R5 $(x)\,\mathrm{P}(x, |\,, x)$

R6 $(x)\,(y)\,(z)\,(w)\,(\mathrm{P}(x, y, z)\;\&\;\mathrm{M}(z, x, w) \rightarrow \mathrm{P}(x, y\,|, w))$

Observe that all of these axioms when interpreted as described earlier are true of the numerals (but are also true of the exponential numerical notations).

In order to complete the narrative, it is only necessary to prove:

$(x)\ (y)\ (\exists z)\ \mathrm{A}(x, y, z)$

$(x)\ (y)\ (\exists z)\ \mathrm{M}(x, y, z)$

$(x)\ (y)\ (\exists z)\ \mathrm{P}(x, y, z)$

That is, we must show that the numerals are closed under these relations and that they therefore represent total functions on the numerals. With the stated interpretation, the exponential numerical notations are trivially closed under these relations. For example, if t and s are any two such terms then $t \wedge s = t \wedge s$ and so $(x)\ (y)\ (\exists z)\ \mathrm{P}(x, y, z)$. But in order to prove that the *numerals* are closed with respect to these relations another proof technique, mathematical induction, must be used. Once this is introduced, the standard proofs for closure of these relations can be argued. In the following sketches of natural deduction derivations, a, b, c, and d are free variables.

I. $(x)\ (y)\ (\exists z)\ \mathrm{A}(x, y, z)$

1. From Axiom *R1*, $\mathrm{A}(a, \mathrm{I}, a\mathrm{I})$. Hence, $(\exists z)\ \mathrm{A}(a, \mathrm{I}, z)$.
2. Assume (#1) $\mathrm{A}(a, b, c)$. From Axiom *R2* then follows $\mathrm{A}(a, b\mathrm{I}, c\mathrm{I})$ and so $(\exists z)\ \mathrm{A}(a, b\mathrm{I}, z)$.
3. Assume (#2) $(\exists z)\ \mathrm{A}(a, b, z)$ and cancel assumption (#1).
   Thus we have established $(\exists z)\ (\mathrm{A}(a, b, z) \rightarrow (\exists z)\ \mathrm{A}(a, b\mathrm{I}, z))$.
   Using induction on b, we conclude $(x)\ (y)\ (\exists z)\ \mathrm{A}(x, y, z)$.

II. $(x)\ (y)\ (\exists z)\ \mathrm{M}(x, y, z)$

1. Axiom *R3* gives $\mathrm{M}(a, \mathrm{I}, a)$. Hence, $(\exists z)\ \mathrm{M}(a, \mathrm{I}, z)$.
2. Assume (#1) $\mathrm{M}(a, b, c)$ and (#2) $\mathrm{A}(c, b, d)$. Then from Axiom *R4* we conclude $\mathrm{M}(a, b\mathrm{I}, d)$ and so $(\exists z)\ \mathrm{M}(a, b\mathrm{I}, z)$. From the conclusion to Proof I we have $(\exists z)\ \mathrm{A}(c, b, z)$ and so we can cancel assumption (#2).
3. Assume (#3) $(\exists z)\ \mathrm{M}(a, b, z)$ and cancel assumption (#1).
   Thus we have established $(\exists z)\ \mathrm{M}(a, b, z) \rightarrow (\exists z)\ \mathrm{M}(a, b\mathrm{I}, z)$.
   Using induction on b, we conclude $(x)\ (y)\ (\exists z)\ \mathrm{M}(x, y, z)$.

III. $(x)\ (y)\ (\exists z)\ \mathrm{P}(x, y, z)$

(Notice that this proof is parallel in form to Proof II.)

1. Axiom *R5* gives $\mathrm{P}(a, \mathrm{I}, a)$. Hence, $(\exists z)\ \mathrm{P}(a, \mathrm{I}, z)$.
2. Assume (#1) $\mathrm{P}(a, b, c)$ and (#2) $\mathrm{M}(c, b, d)$. Then from Axiom *R6* we conclude $\mathrm{P}(a, b\mathrm{I}, d)$ and so $(\exists z)\ \mathrm{P}(a, b\mathrm{I}, z)$. From the conclusion to Proof II we have $(\exists z)\ \mathrm{M}(c, b, z)$ and so we can cancel assumption (#2).
3. Assume (#3) $(\exists z)\ \mathrm{P}(a, b, z)$ and cancel assumption (#1).
   Thus we have established $(\exists z)\ \mathrm{P}(a, b, z) \rightarrow (\exists z)\ \mathrm{P}(a, b\mathrm{I}, z)$.
   Using induction on b, we conclude $(x)\ (y)\ (\exists z)\ \mathrm{P}(x, y, z)$.

So our proofs have justified our faith:

> We can restrict notations to the numerals (except for "practical" calculations) and recover addition, multiplication, and exponentiation as functions on numerals.[4]

Being logical locally

Anyone who criticizes the preceding claim faces the challenge of explaining where any or all of arguments I, II, and III fail, given that the axioms are admitted to hold of the numerals and the inference rules preserve truth. The critique which follows focuses on two issues: first, the role of mathematical induction, and second, and more basic, the semantics which are being used.

Even if one grants that the logical rules preserve truth, it seems to me that we are entitled to some evidence that the same is always true of induction. After all, mathematical induction is the first inference rule which involves a potentially infinite number of steps. The usual justification—indeed, to my knowledge, the only justification offered—is to visualize this inference as if it were a potentially infinite number of *modus ponens* steps. This is not much of a clarification. I am not alone in my skepticism. Various people including Edward Nelson, *1986*, p. 1 have argued that unrestricted use of induction can produce false results. In my opinion, one need not go far to find such a result: the belief that, for example, $2\textasciicircum n$ is equal to a numeral for any numeral n forces thinkers about mathematical philosophy to go into contortions to make sense out of what seems to be false.[5]

One way to justify mathematical induction is to provide independent evidence that the results it produces are correct. This seems impossible in the case of Proofs I, II, and III as long as we assume that the reference range of the variables involved is the numerals. That is because then to verify the conclusions of these derivations we would have to know that the numerals are closed, respectively, under addition, multiplication, and exponentiation and this is just the knowledge that the putative "proofs" are supposed to supply.

Need we make this assumption? These proofs are carried out in first-order logic using certain inference rules. What is of logical importance about these rules (I believe) is that they preserve truth, i.e., they are sound. But in order to preserve truth as one passes from the premise of an inference to its conclusion, you do not need to assume that the ranges of all the variables are the same; you need only assume that the ranges are related appropriately. The assumption that the variables all have the same range is a semantic assumption, not a logical one.

[4] Although other more set theoretic proofs of the closures of these relations exist, the first-order ones presented here are essentially the arguments used to convince mathematicians of the fact.

[5] Certainly it is "false" if one considers the time and space required to evaluate to a numeral for an (abbreviated) expression like 2^65536. Underlying my skepticism is a (rather ill-defined) belief that computations such as those represented by the exponential numerical notations plus the reduction rules (Definition 2) are more similar to, say, a gear system than to a mathematically defined object. And although one might have a mathematical theory which is descriptive of the gear system, it could not be constitutive of it. The same holds true of the computation: At best one can hope to find a mathematical model of it, and any model is bound to have its flaws.

For example, suppose we are working in a natural deduction system and have an occurrence of Universal Elimination:

$$\frac{(x)\ A(x)}{A(t)}$$

One need only assume that the value(s) of the term t are a subset of the values assumed by the variable x.

Or suppose one wants to ensure that Implication Elimination preserves truth:

$$\frac{A_1 \quad A_2 \rightarrow B}{B}$$ where A1, A2 differ perhaps only in the naming of their bound variables

Then it is sufficient to demand that the ranges of corresponding variables be the same. Of course this means that the range of a particular occurrence of a variable may change as the proof of which it is a part enlarges and that the interpretation of the formulas in a proof may depend on the form of that proof. This is unconventional in logic, but surely not in other forms of narration where the reference of a pronoun may change as the narrative unfolds.[6]

In any case, suppose we look at Proofs I, II, and III as being arguments about the exponential numerical notations and not just about numerals. After all, the axioms are true of these notations and induction should also be a truth-preserving method of inference as long as the variable of induction is presumed to range over the numerals. Looking at Proofs I, II, and III in this way, we see something curious. Tracing the variable identifications and substitutions in Proof I of $(x_1)\ (y_1)\ (\exists z_1)\ A(x_1, y_1, z_1)$, it turns out that the ranges of variables x_1 and z_1 can be exponential numerical terms although the range of the induction variable y_1 must be restricted to numerals. Because of substitutions that occur in Proof II, the range of x_2 (as well as the range of the induction variable y_2) in the formula $(x_2)\ (y_2)\ (\exists z_2)\ M(x_2, y_2, z_2)$ must be restricted to the numerals whereas z_2 can range over the exponential numerical terms. In addition, although Proof II uses the conclusion $(x_1)\ (y_1)\ (\exists z_1)\ A(x_1, y_1, z_1)$ of Proof I, the range of the variable z_1 (and x_1) remains the same. Because the range of z_1 and z_2 can be notations, the conclusions of Proofs I and II are obviously true. So we obtain justification for the use of mathematical induction in these cases. But when we repeat the argument a third time in Proof III, matters change. Here when the

---

6 This was certainly my experience as I read the description of soirees in *War and Peace* and frequently found that the individual that I'd assumed was being referred to by "he" or "she" in fact, as the paragraph developed, turned out to be another. Such reference shifts either by the reader or by characters in the story occur all the time in mysteries. For example, at the end of the Sherlock Holmes story "Silver Blaze", Dr. Watson and Colonel Ross are made to realize that the murderer they'd been seeking was not a man but, as Holmes pointed out, a horse. In such cases there is a complete shift of the referent. In the case of the word "electors" as used in Article 1, Section 1 of the U.S. Constitution, the reference range has expanded from the collection of propertied, free-born white males in 1787 to its contemporary wider inclusiveness. In Proofs I, II, and III there is a narrowing of the range of reference of certain variables. Finally, the referent of the term "rogue state" as used by the present United States administration changes so frequently that it is difficult to determine it at all.

conclusion $(x_2)\,(y_2)\,(\exists z_2)\,\mathrm{M}(x_2, y_2, z_2)$ of Proof II is used, the substitutions and identifications occurring force the range of z_2 (as well as the ranges of x_2, y_2 and x_1, z_1) to be numerals. That is, Proof III requires as an assumption that the numerals be closed under multiplication (and addition). However, this is not what Proof II (or I) has established. So it seems that Proof III uses unjustified assumptions to derive $(x_3)\,(y_3)\,(\exists z_3)\,\mathrm{P}(x_3, y_3, z_3)$ (where also the ranges of x_3, y_3, z_3 must be numerals.)[7] Because of the proof's structure, the only interpretation for the variables in Proof III is the numerals, and these we do not know *a priori* to be closed under exponentiation. Thus, we have no independent justification for the use of induction here.

As another example consider the theorem:

$$(x)\,(\,(x = |)\ \vee\ (\exists y)\,(x = y|)\,)$$

This can be proved by induction on x whose range therefore is the numerals. Then if one derived $(x)\,(y)\,(\exists z)\,(\,\mathrm{M}(x, y, z)\ \&\ ((z = 1)\ \vee\ (\exists w)\,(z = w|)))$ from the theorem $(x)\,(y)\,(\exists z)\,\mathrm{M}(x, y, z)$, the range of z is also forced to be the numerals.

A slightly different version of the same phenomenon occurs in the proof, given in Kleene, 1971 that exponentiation is numeralwise expressible in elementary number theory. The essential step is the proof by induction on y of the formula $(y)\,(\exists x)\,\mathrm{F}(y, x)$ which expresses the existence of the common multiple x of the numbers in the sequence $1, 2, 3, \ldots, y$.[8] Due to substitutions which occur during its proof, the range of x must contain arbitrarily large multiples of multiplicative numerical terms (for example, $(\ldots(((|| * ||) * ||) * \ldots * ||))$ and, simultaneously, the range of x is a subset of the numerals. That is, the numerals must be closed under exponentiation.[9]

Conclusion

Although we can agree that the logical inference rules preserve truth, mathematical induction (at least in the contexts illustrated) seems to be something different: It introduces an extralogical element by limiting the possible range of the induction variable. And this semantic restriction can then propagate through the derivation. This is illustrated in the Proof of III where the third use of induction results in a derivation from assumptions which have not been proved but which must, apparently, be taken on faith. But if one is of little faith, as I tend to be, then *the conclusion that the numerals are closed under exponentiation does not follow*.[10]

---

[7] For a more detailed exposition of this argument, see Isles, 1992. Some consequences of the idea of derivation-determined interpretations are spelled out in Isles, 1994.

[8] Kleene, 1971, formal theorem 157, p. 192.

[9] See Isles, 1992, p. 475 for details.

[10] Although my skepticism on this point is uncommon, similar opinions have been expressed by other authors; see, for example, Bernays, 1983, Van Dantzig, 1956, and Nelson, 1986.

Note added in proof

The argument above suggests that the usual understanding of arithmetic as "natural numbers" + "arithmetic functions" may be misleading. We are dealing with a certain set of notations plus rewriting rules (modeled, for example, by Definitions 1, 2, and 3): These are the basic entities we use when dealing with or thinking about "natural numbers". These terms and operations are natural phenomena to be investigated using whatever tools we have at our disposal: experimental or theoretical.

For example, can we show that every (~)-reduction sequence of a term terminated (necessarily in a numeral) by using induction on the depth of a term (considered as a tree)? To do this it seems that we must establish (via induction, how else?) that every term of the form $(n + m)$, $(n * m)$, or $(n \wedge m)$, where n and m are numerals, reduces to a numeral. This would mean showing that the number of steps in a (~)-reduction sequence is a numeral, i.e., that there are procedures $\mathrm{A}(n, m)$, $\mathrm{M}(n, m)$, and $\mathrm{P}(n, m)$ that, given numerals n and m, produce *exponential numeral terms* that: (i) equal a numeral and (ii) bound the number of steps in the relevant (~)-reduction sequence. Simple calculations show that for terms of the form $(n + m)$, $(n * m)$, and $(n \wedge m)$ where n and m are numerals, such algorithms are:

$$\begin{aligned} \mathrm{A}(n, m) &= m \\ \mathrm{M}(n, m) &= n * (m - 1) + m \\ \mathrm{P}(n, m) &= (n \wedge m) + (n * (m - 2))) + m \end{aligned}$$

Here $m-1$ and $m-2$ are abbreviations. Now because $\mathrm{A}(n, m) < (n + m)$ and $\mathrm{M}(n, m) < (n * m)$, where $m < n$, if $\mathrm{A}(n, m)$ and $\mathrm{M}(n, m)$ have been shown to be numerals, then we have some assurance that $(n + m)$ and $(n * m)$ will reduce to numerals. Perhaps one could describe this as saying that $+$ and $*$ are "predicative" operations. But we have no assurance in the case of $(n \wedge m)$ because $(n \wedge m) < \mathrm{P}(n, m)$. Whether one can find a different bounding function $\mathrm{P}(n, m)$ such that $\mathrm{P}(n, m) < (n \wedge m)$ is unknown to me.

Bibliography

Barendregt, Henk

1977 The type free lambda calculus
Handbook of Mathematical Logic, ed. Jon Barwise,
North-Holland Publishing Co., pp. 1091–1132.

Bernays, Paul

1983 On platonism in mathematics
Translated from the French by C. D. Parson from *L'enseignement mathématique*, 1st ser. vol. 34, 1935, pp. 52–69, in *Philosophy of Mathematics*, 2nd ed., ed. P. Benacerraf and H. Putnam,
Cambridge University Press, pp. 258–271.

Ifrah, Georges

1985 *From One to Zero*: *A Universal History of Numbers*
Translated from the French by Lowell Blair.
Viking Penguin Inc.

Isles, David

1992 What evidence is there that 2^65536 is a natural number?
Notre Dame Journal of Formal Logic, vol. 3, pp. 465–480.

1994 A finite analog to the Löwenheim-Skolem theorem
Studia Logica, vol. 53, pp. 503–532.

Kleene, Stephen Cole
1952 *Introduction to Metamathematics*
1st edition, D. Van Nostrand.

Nelson, Edward
1986 *Predicative Arithmetic*
Mathematical Notes 32, Princeton University Press.

VanDantzig, D.
1956 Is $10^{10^{10}}$ a finite number?
Dialectica, vol.19, pp. 273–277.