Nonassociative Number Theory

Trevor Evans

The American Mathematical Monthly, Vol. 64, No. 5. (May, 1957), pp. 299-309.

NONASSOCIATIVE NUMBER THEORY

TREVOR EVANS, Emory University

Introduction. In several papers I. M. H. Etherington has studied the algebra of exponents of the general element in a nonassociative linear algebra and he has called these systems *logarithmetics*. If the linear algebra does not satisfy any identities the corresponding logarithmetic bears a close resemblance to the natural numbers. In fact, in [3] Etherington has shown that the elements of this particular logarithmetic can be defined in terms of partitioned classes in complete analogy to the Frege-Russell definition of the natural numbers as classes of classes. It is not too surprising then that we can also characterize this logarithmetic by a set of postulates analogous to the Peano postulates for the natural numbers. We do this in Section 1 and develop the basic properties of the logarithmetic in a manner paralleling the usual development of the natural numbers.*

We proceed to study the number theory of this logarithmetic. Several of the theorems in Section 1 and 2 including the "fundamental theorem of arithmetic" have been obtained by Etherington, although our derivations are in general quite different. Some of the standard theorems and conjectures of ordinary number theory have trivial analogues in this new number theory but a little more effort is needed to prove Fermat's Last Theorem.

By analogy with the extension of the natural numbers to the ring of positive and negative integers, we extend the logarithmetic to a system in which subtraction is always possible. The system so obtained is the left neoring of Bruck's recent paper [2]. The fundamental theorem of arithmetic has to be proved anew, since there are many more primes than just the original primes and their associates. In this new system we are also able to introduce the analogues of finite arithmetics and congruence by using some of the results of [6].

We conclude by mentioning a few problems and possible directions for further work.

1. Peano-like postulates for the nonassociative natural numbers. Peano's postulates characterize the natural numbers as a set closed under a unary operation and satisfying certain other conditions. If we replace the unary operation by a binary operation and make the corresponding changes in the postulates we obtain the following system.

Undefined terms: The set of nonassociative natural numbers, the elements of which we will just call numbers;† the binary operation of addition.

* See, for example, the first few pages in [8].

† We will always use the words "positive integer" in referring to the natural numbers of ordinary arithmetic.

Postulates:

(i) 1 is a number,

(ii) to every pair of numbers a, b there corresponds a third called the sum of a and b and written $a+b$,

(iii) there are no numbers a, b such that $a+b=1$,

(1) (iv) if the numbers a, b and c, d are such that $a+b=c+d$, then $a=c$ and $b=d$,

(v) if a set of numbers contains 1, and if whenever it contains numbers a, b then it contains $a+b$, then the set contains all numbers. (The principle of nonassociative induction.)

Thus our numbers are $1, 1+1, 1+(1+1), (1+1)+1, 1+(1+(1+1)), \cdots$. By postulate (v), every number except 1 can be expressed as the sum of two other numbers and postulate (iv) implies that this can be done in only one way. Also, by postulate (iv), addition is in general noncommutative since $a+b=b+a$ implies $a=b$. Following Etherington, we will denote $1+1$ by 2, $1+(1+1)$ by 3, $1+(1+(1+1))$ by $4, \cdots$.

As an example of nonassociative induction we prove:

THEOREM 1. *For all numbers a, b, $a\neq a+b$.*

Proof. Let S be the set of all values of a such that $a\neq a+b$ for any b. S contains 1 by postulate (iii). Let m, $n\in S$. If there exists a number b such that $m+n=(m+n)+b$, then $m=m+n$ by postulate (iv), in contradiction to the assumption that $m\in S$. Thus $m+n\in S$ and so by the principle of nonassociative induction, S contains all numbers.

An immediate consequence of this theorem is that there are no numbers a, b, c such that $a+(b+c)=(a+b)+c$. That is, addition is completely nonassociative. Because of the lack of commutativity and associativity in addition, introducing an order or partial order into the system does not seem to be very fruitful. One fairly reasonable definition is as follows. We first define "well-formed part" of a number by (i) the only well-formed part of 1 is 1 itself, (ii) if $a=b+c$, the well-formed parts of a are a itself and the well-formed parts of b and c. Now we define $x\leq y$ if x occurs as a well-formed part of y, and $x<y$ if $x\leq y$ but $x\neq y$. With these definitions we get a partial ordering* between numbers but unfortunately $x<y$ does not imply $x+z<y+z$ or $z+x<z+y$. However, with the definition of multiplication given below, $x<y$ does imply $z\cdot x<z\cdot y$.

We introduce multiplication $a\cdot b$ (or ab) into our number system by

* The partial order for N can be extended to a complete ordering as was pointed out to me recently in conversation by R. H. Bruck and D. R. Hughes. Define $a<b$ in N if (i) $|a|<|b|$; (ii) $|a|=|b|$ but $a_1<b_1$, where $a=a_1+a_2$, $b=b_1+b_2$; (iii) $|a|=|b|$ and $a_1=b_1$, but $a_2<b_2$. Unlike the partial ordering given above, this ordering has all the usual properties. Another complete ordering of N is obtained by interchanging a_1 and a_2, b_1 and b_2 in (ii), (iii).

$$\text{(2)} \qquad \text{(i) } a\cdot 1 = a, \qquad \text{(ii) } a\cdot(b+c) = a\cdot b + a\cdot c.$$

Clearly this defines a product between every pair of numbers. We leave to the reader the proof of the next two theorems. Nonassociative induction is used on a in the first and c in the second.

THEOREM 2. *$1\cdot a = a$ for all numbers a.*

THEOREM 3. *$(ab)c = a(bc)$ for all numbers a, b, c.*

Some examples of calculation in our system are

$$2\cdot 2 = 2+2, \qquad 3\cdot 2 = 3+3 = (1+(1+1))+(1+(1+1)),$$
$$2\cdot 3 = 2+(2+2) = (1+1)+((1+1)+(1+1)),$$
$$((3+2)+(3+2))+(3+2) = ((1+2)+2)\cdot(2+1).$$

As an immediate consequence of the definition of multiplication the left-distributive law is satisfied. The cancellation properties of multiplication are given in the following theorems.

THEOREM 4. *If $xa = ya$, then $x = y$.*

Proof. This is true for $a = 1$. Assume that it is true for $a = m$ and $a = n$. Now, if $x(m+n) = y(m+n)$, expanding each side we get $xm+xn = ym+yn$. By postulate (iv), $xm = ym$, and so by our inductive hypothesis, $x = y$. Thus the theorem is true for $a = m+n$, and so for all values of a by nonassociative induction.

In order to prove the other cancellation law it is useful to introduce the concept of length of a number n. We mean by this the positive integer obtained from n by regarding $+$ in the expression for n as the addition of ordinary arithmetic. We will denote the length of n by $|n|$. The following relations hold.

$$\text{(3)} \qquad |m+n| = |m| + |n|, \qquad |m\cdot n| = |m|\cdot|n|,$$

i.e., $m \to |m|$ is a homomorphism onto the positive integers.

THEOREM 5. *If $ax = ay$, then $x = y$.*

Proof. We use induction on x. When x is 1, consideration of the lengths of the two sides of the equation $a = ay$ shows that $y = 1$. Consider the equation $a(m+n) = ay$. By the preceding sentence y cannot be 1 and so $y = s+t$ for some numbers s, t. Then $a(m+n) = a(s+t)$ or $am+an = as+at$. By postulate (iv), $am = as$ and $an = at$.

Hence, if $am = as$ implies $m = s$, and $an = at$ implies $n = t$, then $a(m+n) = ay$ implies $m+n = y$. The theorem follows by nonassociative induction.

We now have a fairly complete picture of our nonassociative number system. Every number in it can be obtained from 1 by a finite number of nonassociative additions. Multiplication, $u(1)\cdot v(1)$, of two of these numbers satisfies $u(1)\cdot v(1) = v(u(1))$, in complete analogy with multiplication in ordinary arithmetic. Addition satisfies the uniqueness law, $a+b=c+d$ implies $a=c$ and $b=d$. Multiplication is associative, has 1 as an identity, is connected with addition by the left-distributive law, and satisfies the usual cancellation laws. In the language of modern algebra, this system can be described as additively the free groupoid generated by 1 with a multiplication introduced by $a\cdot b=b\phi_a$ where ϕ_a is the endomorphism of the groupoid determined by mapping 1 into a.

From now on, we will denote this system by N and call it *nonassociative arithmetic.*

2. **Number theory.** We can now proceed with the development of the number theory of N. In view of the noncommutativity of multiplication we need the concepts of *left-factor* and *right-factor.* If $a=b\cdot c$, then b is called a left-factor of a and c is called a right factor of a. If b, c are not equal to 1 or a, we call them *proper* left- or right-factors. A number, other than 1, having no proper left-factors is called a *prime number.* Clearly, a prime number has no proper right-factors either. A striking property of factors in nonassociative arithmetic is given in the next theorem.

THEOREM 6. *If p is a proper left-factor of a, and $a=b+c$, then p is a left-factor of b and a left-factor of c.*

Proof. Since $pq=a$ for some q and $p\neq a$, then $q\neq 1$. Thus $q=m+n$ for some m, n. Then $p(m+n)=a$ and so $pm+pn=b+c$. By postulate (iv), $pm=b$, $pn=c$. That is, p is a left-factor of both b and c. We note that this theorem is not true if we consider right-factors instead of left-factors.

In ordinary arithmetic we have the theorem that if a prime is a factor of a product it is a factor of one of the numbers. The following theorem is similar.

THEOREM 7. *If the prime p is a left-factor of the product $a\cdot b$, where a is not* 1, *then it is a left-factor of a.*

Proof. We use nonassociative induction on b. For $b=1$ the theorem is certainly true. Now if it is true for m, n and if $b=m+n$, then p is a left-factor of $a(m+n)=am+an$. But $p\neq a(m+n)$ since p is prime and so by Theorem 6, p is a left-factor of am. Hence p is a left-factor of a by our inductive hypothesis.

The corresponding result for right factors is also true, but it is most easily obtained as a consequence of the following theorem.

THEOREM 8. (*The fundamental theorem of nonassociative arithmetic.*) *There is only one way in which a number can be written as a product of primes.*

Proof. Let $p_{|1|}p_{|2|}\cdots p_{|s|}$, $q_{|1|}q_{|2|}\cdots q_{|t|}$ be two products of primes such that $p_{|1|}p_{|2|}\cdots p_{|s|}=q_{|1|}q_{|2|}\cdots q_{|t|}$. By Theorem 7, $p_{|1|}$ is a left-factor of $q_{|1|}$ and since $q_{|1|}$ is prime, $p_{|1|}=q_{|1|}$. Then, by Theorem 5, $p_{|2|}\cdots p_{|s|}=q_{|2|}\cdots q_{|t|}$. Continuing this, we get $p_{|2|}=q_{|2|}$, $p_{|3|}=q_{|3|}$, $\cdots$. There must be the same number of factors in each product since otherwise we would eventually have 1 expressed as a product.

COROLLARY. *If the prime p is a right factor of the product $a\cdot b$, where b is not* 1, *then it is a right-factor of b.*

For $a\cdot b$ when written as a product of primes must end with p by the theorem, and since this product of primes can be obtained by writing a and b separately as products of primes, p must be the last factor in the expression of b as a product of primes.

The concept of factor can be extended by defining m to be a *factor* of a if $a=smt$. The concept of mutually prime in ordinary arithmetic has several analogues in nonassociative arithmetic. Two numbers, a, b are *mutually left-prime* if they have no common proper left-factor, *mutually right-prime* if they have no common proper right-factor, *mutually prime* if one is not a factor of the other, and no proper right-factor of one is a left-factor of the other. It is easy to verify the following generalizations of Theorems 6, 7:

(i) If m is a proper factor of a, not a right-factor, and $a=b+c$, then m is a factor of b and of c, (ii) let m be a factor of $a\cdot b$; if m, b are mutually prime, then m is a factor of a, or if a, m are mutually prime, then m is a factor of b.

If a, b are two mutually left-prime numbers then a, $a+b$, $(a+b)+b$, $((a+b)+b)+b$, $\cdots$ have no nontrivial left-factors by Theorem 6, and so are all prime. Hence there are an infinite number of primes. An example of such an infinite sequence of primes is 2, 3, 4, $\cdots$. The twin primes conjecture of ordinary arithmetic has a trivial generalization for, if k is any number, there exists an infinite number of pairs of primes of the form n, $n+k$. The analogue of Goldbach's conjecture fails to hold by virtue of postulate (iv). However, another famous conjecture of ordinary arithmetic is provable in nonassociative arithmetic. In fact, an even stronger result than the original is true.

THEOREM 9. (*Fermat's Last Theorem*). *There are no numbers x, y, z such that $x^{|n|}+y^{|n|}=z^{|n|}$ for any positive integral $|n|$ greater than $|1|$.*

Proof. We obtain a proof by contradiction. Let x, y, z be numbers such that $x^{|n|}+y^{|n|}=z^{|n|}$, where $|n|$ is a positive integer greater than $|1|$. We note that (i) neither x nor y can be 1 since this would imply that $x^{|n|}+y^{|n|}$ is a prime, (ii) $|x|^{|n|}+|y|^{|n|}=|z|^{|n|}$.

Since $|n|$ is greater than $|1|$, $z^{|n|}$ has z as a left-factor and so by Theorem 6, both $x^{|n|}$ and $y^{|n|}$ have z as a left-factor. Let x and z be expressed as a product of primes in the form $x=p_{|1|}p_{|2|}\cdots p_{|s|}$, $z=q_{|1|}q_{|2|}\cdots q_{|t|}$. Then, since $zu=x^{|n|}$ for some number u, we have $q_{|1|}q_{|2|}\cdots q_{|t|}u=p_{|1|}p_{|2|}\cdots p_{|s|}v$, where $v=x^{|n-1|}$.

By Theorem 7, $q_{|1|}=p_{|1|}$, $q_{|2|}=p_{|2|}$, $\cdots$. Now $|s|<|t|$, for otherwise $|z|\leq|x|$, in contradiction to $|x|^{|n|}+|y|^{|n|}=|z|^{|n|}$. Hence, $z=xa$ for some a and, similarly, $z=yb$ for some b.

We have then $|z|=|x|\cdot|a|$, $|z|=|y|\cdot|b|$. Substituting in $|x|^{|n|}+|y|^{|n|}=|z|^{|n|}$ for $|x|$ and $|y|$, we get $|1|/|a|^{|n|}+|1|/|b|^{|n|}=1$. This is a contradiction since for $|n|>|1|$, no positive integers $|a|$, $|b|$ satisfy such a condition.

3. Introduction of "negative integers." In ordinary arithmetic, zero and the negative integers are introduced in order that subtraction always be possible. The same problem arises naturally in nonassociative arithmetic also. In N, subtraction can be defined between some pairs of numbers as follows. If $m=p+n$ we can introduce the operation of right-subtraction $m-n$ between m and n and write $m-n=p$. If $m=n+q$, we can introduce the operation of left-subtraction* $-n+m$ between m and n and write $-n+m=q$. With these definitions we get the following properties

$$(4)\qquad \begin{aligned} (m+n)-n&=m, \qquad & n+(-n+m)&=m,\\ (m-n)+n&=m, \qquad & -n+(n+m)&=m. \end{aligned}$$

Clearly these are properties we would like subtraction to have, and in a general nonassociative system they are the most for which we can hope. The problem now is to find a system containing N and such that left- and right-subtraction is possible between every pair of elements. More specifically, we want a system with two operations $+$, $\cdot$, and such that (i) the equations $a+x=b$, $y+a=b$ have unique solutions, (ii) multiplication is associative, (iii) the multiplicative identity 1 generates the system, (iv) the cancellation laws hold, (v) the left-distributive law holds, (vi) with respect to the operation $+$, 1 generates a subsystem isomorphic to N. Such a system is of the type discussed by Bruck in a recent paper [2] and called by him a left neoring. However, there are many left neorings satisfying the above conditions. We will choose the one which seems to be the most natural extension of N.

Let L be the free monogenic loop† generated by 1 with the operation written as addition. This is the nonassociative analogue of the additive group of integers. The mapping $1\rightarrow a$ where a is any element of L determines an endomorphism ϕ_a of L and we can introduce a multiplication into L by defining $a\cdot b=b\phi_a$. We will denote the resulting system by I and call it the left neoring of nonassociative integers. In this section "number" will refer to an element of I.

An immediate consequence of this definition of multiplication is that $a(b+c)=ab+ac$ for all a, b, c. In addition, as is shown in [2], multiplication is associative and the two cancellation laws of multiplication are satisfied. Since, additively, I is a loop, we do have the required subtraction properties, and the subsystem of I consisting of 1, $1+1$, $1+(1+1)$, $\cdots$, *etc.* is isomorphic to N. We refer the reader to [2], [6], for a discussion of the algebraic structure of I. We wish to introduce here some analogues of ordinary number theory in I. For this reason we will use another approach to the system which has the advantage of an explicit representation of its elements.

Consider all expressions which can be generated by 0 and 1 with the three

* Note that the $-$ and $+$ here do not exist independently, but are each part of the notation for the binary operation of left-subtraction.

† For a discussion of free loops see [1], [4], [5].

binary operations of addition $a+b$, left subtraction $-a+b$, and right subtraction $a-b$. We call such expressions *numerical expressions*. An example is $(4+(0-1))-((1+1)+(1+(-2+1)))$, where 2, 4 have the usual meaning as abbreviations.

Two numerical expressions are equal if and only if their equality follows from the following

$$\begin{array}{lll}
\text{(i)} & a+0=0+a=a, & \\
\text{(ii)} & a-a=-a+a=0, & \\
\text{(iii)} & a-0=-0+a=a, & \\
\text{(iv)} & (a+b)-b=a, & -b+(b+a)=a, \\
\text{(v)} & (a-b)+b=a, & b+(-b+a)=a, \\
\text{(vi)} & a-(-b+a)=b, & -(a-b)+a=b,
\end{array}\tag{5}$$

where a, b are numerical expressions.

Clearly (i), (ii), (iii) are properties we wish 0 to have, (iv) and (v) are the properties of subtraction we already have in N. Equations (vi) are actually consequences of the preceding equations and we list them merely for their usefulness in computation. We remark that $(-a+b)$ is the unique solution of $a+x=b$ and $b-a$ is the unique solution of $y+a=b$.

Our nonassociative integers are now defined as the classes of equal numerical expressions. A multiplication is introduced into the system by $u(1)\cdot v(1)=v(u(1))$ where u, v are numerical expressions.

That this system is I is a consequence of the results of [4], [5]. Another result from [4, Theorem 2.2], shows that in each class of equal numerical expressions there is a unique expression of shortest length (here "length" refers to the number of 0's and 1's in the expression). Such a shortest numerical expression is characterized by the property that there is no application of equations (5) to the expression which will shorten it. We will call this the normal form of the class of equal numerical expressions and refer the reader to [4], [5] for a full discussion of these ideas.

The following examples illustrate the rules of computation in I and some specific computations.

$$\begin{array}{l}
\left.\begin{array}{ll}
\text{(i)} & a\cdot 1=1\cdot a=a,\\
\text{(ii)} & a\cdot(m+n)=a\cdot m+a\cdot n,\\
\text{(iii)} & a\cdot(m-n)=a\cdot m-a\cdot n,\\
\text{(iv)} & a\cdot(-m+n)=-a\cdot m+a\cdot n,
\end{array}\right\}\text{by the definition of multiplication,}\\
\begin{array}{ll}
\text{(v)} & a\cdot 0=a(1-1)=a-a=0,\\
\text{(vi)} & 0\cdot a=0, \text{ by induction on the length of } a,\\
\text{(vii)} & a\cdot(0-1)=0-a, \qquad a\cdot(-1+0)=-a+0,
\end{array}
\end{array}\tag{6}$$

$$\text{(viii)}\quad (0-1)\cdot(-1+0) = -(0-1)+(0-1)\cdot 0 = -(0-1)+0 = 1,$$

$$\text{(ix)}\quad (1-2)\cdot((0-1)+2) = (1-2)\cdot(0-1)+(1-2)\cdot(1+1)$$
$$= (0-(1-2))+((1-2)+(1-2)).$$

The discussion of the number theory of I is complicated by the existence of units. As usual we define a unit to be an element possessing a multiplicative inverse. In the ring of integers of ordinary arithmetic there are only two units but the left neoring I contains an infinite number.

We will call the elements $0-1$, $0-(0-1)$, $0-(0-(0-1))$, $\cdots$ the first, second, third, $\cdots$ right negatives of 1 and similarly, $-1+0$, $-(-1+0)+0$, $-(-(-1+0)+0$, $\cdots$ the first, second, third, $\cdots$ left negatives of 1. It is easily verified from equations (5) and (6) that the product of the nth left negative and nth right negative is 1.

It is not quite so easy to show that these are the only units in I. We recall that the product of two elements $u(1)$, $v(1)$ of I is defined by $u(1)\cdot v(1)=v(u(1))$. Hence we have to show that the left- and right-negatives of 1 are the only elements of I which satisfy $v(u(1))=1$. This is an immediate consequence of Lemma 2 in [5].

Since $(0-1)^2=0-(0-1)$, $(0-1)^3=0-(0-(0-1))$, $\cdots$ and $(-1+0)^2=-(-1+0)+0$, $(-1+0)^3=-(-(-1+0)+0)+0$, $\cdots$, the units of I are exactly the powers of $0-1$.

We collect these results as a theorem.

THEOREM 10. *The multiplicative group of units of I is the infinite cyclic group generated by* $0-1$.

As before b will be called a *left-factor* of a if there exists an element c of I such that $b\cdot c=a$. If neither b nor c is a unit and $a\neq 0$, we say that b is a *proper left-factor* of a. In the same way we define *right-factor* and *proper right-factor*. We note that any number is a factor of 0. Two numbers a, b in I will be called *associates* if $xay=b$ where x, y are units.

LEMMA 1. *If a, b are left- (right-) factors of each other, then they are associates.*

Proof. If $ax=b$, $by=a$, then $axy=a$ or $xy=1$. Hence x, y are units. The proof for right-factors is similar.

If a is a left- (right-) factor of b and b is a right- (left-) factor of a, then $a=b$ unless both a and b are units. A proof of this leans heavily on the results of [4], [5], and so we omit it.

In ordinary arithmetic, the primes in the ring of integers are simply the original primes in the set of natural numbers multiplied by the units. This situation does not carry over to nonassociative arithmetic. In fact, a rather complicated situation exists in I. We define, in the usual way, a *prime number* of I to be a number without proper factors. Then all the primes of N are primes in I.

We also have primes such as $0-(1+1)$ consisting of the product of the prime $(1+1)$ in N and the unit $0-1$. But other primes such as $1-(1+1)$ exist in I, not the product of a unit and a prime of N. In addition, there is a special subclass of the primes of I with the property that no prime in this subclass can be written as a product of two numbers of shorter length. For want of a better name, we will call these *special primes*. The number $(0-(1+1))$ is a prime but it is not a special prime since $0-(1+1)=(1+1)\cdot(0-1)$. However, $(1+1)$ is a special prime and, more generally, all the primes of N are special primes in I. Examples of other special primes are $(1-2)$, $(1-3)$, $(1-4)$, $\cdots$.

We now state some theorems, giving only brief outlines of the proofs, which are basic in the further development of the number theory of I.

THEOREM 11. *Let a be an element of I represented by a numerical expression in normal form so that a has one of the forms $m+n$, $m-n$, $-m+n$ where m, n are numerical expressions. Then any proper left-factor of a is a left-factor of m and n.*

Proof. This corresponds to Theorem 6 for N. The proof proceeds by ordinary induction on the length of a, coupled with the fact that the representation of a number as a numerical expression in normal form is unique.

THEOREM 12. *If the prime p is a left-factor of the product ab, where $a\neq 1$, $b\neq 0$, then p is a left-factor of a.*

Proof. By induction on the length of b, and by the previous theorem.

THEOREM 13. *If a number a can be written as a product of primes in two ways, say, $a=p_{|1|}\cdots p_{|s|}$ and $a=q_{|1|}\cdots q_{|t|}$, then $|s|=|t|$ and $p_{|i|}$, $q_{|i|}$ are associates $(|i|=|1|, \cdots, |s|)$.*

Proof. By Lemma 1, Theorem 12, and the left-cancellation law for I.

We conclude our discussion of I by introducing the concept of congruence in it. In ordinary arithmetic, a homomorphic image of the ring of integers is obtained by adding the relation $|m|=|0|$ to the ring. Then two integers are congruent mod $|m|$ if they map onto the same element under this homomorphism. It is shown in [6] that if $m(=u(1))$ is an element of I, then adding the relation $u(1)=0$ to I determines a left neoring which is a homomorphic image of I. We define two numbers in I to be congruent mod m if they map onto the same element under this homomorphism. Alternatively, we can define two numbers in I to be congruent mod m if their difference lies in the fully invariant normal subloop, generated by m, of the additive loop of I. The relation between these two points of view is discussed briefly in [6] and can be studied in detail using the techniques of [4], [5]. The homomorphic images of I described above are the nonassociative analogues of finite arithmetics.

With the above definition of congruence in I, some of the elementary properties of congruence in ordinary arithmetic carry over without difficulty (see, *e.g.*, Chapter 1 in [8]). The author does not know whether the same is true of some of the deeper theorems involving congruence.

4. Further developments. The ideas introduced in this paper can be developed in several directions. There are many problems for the arithmetic N, *e.g.*, obtaining an analogue of the prime number theorem. This seems quite feasible since estimates of the number of nonassociative natural numbers of given length are available.

In some of our proofs of properties of N we used properties of ordinary arithmetic including induction. Can this be avoided completely and all properties of N obtained from the postulates for N given in Section 3? One way to do this is to develop ordinary arithmetic within N. Define nonassociative powers of numbers in N by $a^1=a$, $a^{m+n}=a^m\cdot a^n$ where $m, n\in N$. An equivalence relation, $\equiv$, between numbers in N can be defined by $m\equiv n$ if $a^m=a^n$ for all $a\in N$. We now show that the set of these equivalence classes satisfies Peano's postulates for the ordinary natural numbers. This is a consequence of the Peano-like postulates which N satisfies. The length of a number n in N is defined as the equivalence class containing n. In this way all of ordinary arithmetic and in particular those parts which we have used in discussing N can be developed inside N. It follows that if we set up N as a formal system, there will be a Gödel incompleteness theorem for the system. We leave to the interested reader the detailed carrying out of the above ideas. A related topic which may be interesting is the theory of recursive functions of nonassociative natural numbers.

There are many concepts involving congruence in ordinary arithmetic which should have interesting analogues in the arithmetic I. In particular we can ask such questions as the following. For what congruences does the quotient arithmetic (i) satisfy the cancellation law, (ii) allow division, (iii) allow unique division, (iv) satisfy the commutative laws of addition and multiplication? Other problems are (i) what is the structure of the multiplicative semigroup of I, (ii) can I be embedded in a system with division?

If we add to N the identical relation $(a+b)+(c+d)=(a+c)+(b+d)$ we get an arithmetic S with many interesting properties. In this system, which is the free symmetric groupoid generated by 1 (see [7]), we define multiplication as usual by $u(1)\cdot v(1)=v(u(1))$. Then multiplication is commutative and so both distributive laws hold. This arithmetic is extremely close to ordinary arithmetic, differing only in the replacing of the associative and commutative laws by the single law $(a+b)+(c+d)=(a+c)+(b+d)$. A study of the number theory of S should lead to some interesting problems. Another problem which presents itself is the obtaining of a set of Peano-like postulates which characterize S.

References

1. Grace Bates, Free loops and nets and their generalizations, Amer. J. Math., vol. 69, 1947, pp. 499–550.

2. R. H. Bruck, Analogues of the ring of rational integers, Proc. Amer. Math. Soc., vol. 6, 1955, pp. 50–57.

3. I. M. H. Etherington, Non-associative arithmetics, Proc. Roy. Soc. Edinburgh, vol. 62, 1949, pp. 442–453.

4. Trevor Evans, On multiplicative systems defined by generators and relations, I. Normal form theorems, Proc. Cambridge Philos. Soc., vol. 47, 1951, pp. 637–649.

5. ———, On multiplicative systems defined by generators and relations, II. Monogenic loops, Proc. Cambridge Philos. Soc., vol. 49, 1953, pp. 579–589.

6. ———, Some remarks on a paper by R. H. Bruck, Proc. Amer. Math. Soc., vol. 7, 1956, pp. 211–220.

7. Orrin Frink, Symmetric and self-distributive systems, this MONTHLY, vol. 62, 1955, pp. 697–707.

8. C. C. MacDuffee, An Introduction to Abstract Algebra, New York, 1940.

MAINTAINING COMMUNICATION*

E. J. McSHANE, University of Virginia

Some twenty years ago a professor of philosophy spoke to the mathematics club at the University of Virginia. The speech was followed by a warm discussion of the paradoxes of Zeno. Some regarded the mathematical explanation of the paradoxes as completely adequate, others disagreed, and needless to say, each disputant emerged triumphantly bearing the opinion he had carried in. But one remark of a professor of physics has stayed with me ever since. He said that he could easily conceive that someone could arrive in his own mind at a perfect solution of the paradoxes and still be unable to convey the explanation to anyone else.

Let us at least temporarily suspend disbelief in this philosopher with the incommunicable thoughts, and not boggle over reasons for acceding to him a belief that we deny to Fermat and his celebrated proof that was too long for the book's margin. There remains the fact that to the body of philosophy he remains exactly as useless as though he had never existed. Perhaps he has derived intense personal satisfaction from his brilliant reasoning, but the rest of the world may as well ignore him.

In recent years I have been troubled by a suspicion that this image of the uncommunicative philosopher may be a parable of an approaching state of mathematics. Fortunately, rather than a parable it is an overdrawn caricature, but as in all caricatures some features are recognizable. For in mathematics, as in the sciences, the communication of ideas becomes steadily more difficult. This is a matter that concerns all of us, and each of us should try to help in keeping the lines of communication open.

To begin with, there are the mechanical and financial difficulties involved

* Retiring Presidential Address, delivered at the Fortieth Annual Meeting, December 29, 1956, Rochester, N. Y.