ARITHMETIC: MORE OF THE STORY

Abstract

A binary operation # on Z+ is said to be an ASSOCIATIVE ARITHMETIC if both #, and the binary operation * defined by:

$$x * y = x \# x \# x \# \ldots \quad y\ x\text{'s}$$

are associative. This paper gives a structure theorem for associative arithmetics, and in particular shows that there are other associative arithmetics besides addition.

ARITHMETIC: MORE OF THE STORY

Why are addition and multiplication commutative and associative, but not exponentiation? Suppose humankind had defined a different kind of addition? It could then define, as it does now, multiplication as "repeated addition" and exponentiation as "repeated multiplication". If the new addition were stategically chosen, could the resulting multiplication (which would mean repeating this new kind of addition) and exponentiation (which would mean, in turn, repeating the new multiplication) perhaps be both commutative and associative? And could we then, perhaps, go on to define "higher" binary operations -- repeated exponentiation, repeated repeated exponentiation, and so on? If we had "started" with just the right kind of "alternative addition", could they all be both commutative and associative?

These are questions with which I was preoccupied during my high school years. I would start with various binary operations as the new addition, and then calculate which binary processes, instead of multiplication, would result from their iteration. For example, starting with x+1 as addition gives rise to x+y-1 as multiplication, xy + x + y gves rise to (x+1)^y - 1, and xy / x+y gives rise to x / y.

I had fun with all this, proving a few easy lemmas (I called them theorems...), for any pair o binary processes # (called "generalized addition") and * (called 'generalized multiplication") such that, for all positive integers x and y, we have x * y = x # x # . . . y x's (that is, such that * is iterated #).:

Lemma 1: Any "generalized multiplication" * must satisfy: x * 1 = x, for all positive integers x.

Lemma 2: For all positive integers x and y, we have x * (y+1) = (x * y) # x

Lemma 3: For all positive integers x, y, and z, we have x * (y+z) = (x * y) # x # x . . . z x's.

Lemma 4: (a generalized distributive law)) If the "generalized addition" # is associative, then # and its "compatible" generalized multiplication * must satisfy:

For all positive integers x, y, and z, (x * y) # (x * z) = x * (y+z).

In college I got slightly more sophisticated and asked, the other way around, whether every binary operation can be considered a "multiplication" -- that is, does every "generalized multiplication" have its corresponding "generalized addition".. More preciselyly, given a binary operation *, does there exist another binary operation # such that, for all positive integers x and y, we have x # x # . . . y x's = x * y. During my freshman year, that question was answered in the affirmative (given reasonable conditions on *), in the following:

Theorem 1 (This one really IS a theorem. . .): Let * be any binary operation such that x * 1 = x for all positive integers x, and such that * can be extended to all of the reals in such a way that, for all real x and y, the equation y * z = x has a unique solution z. Then there is a binary operation # which is "compatible" with *, in the sense that, for all integers x and y, x # x # . . . y x's = x * y.

Proof: Given such a *, define # by:

For all positive integers x and y, let $x \# y = y * (1 + x \setminus y)$, where $x \setminus y$ denotes the unique z such that $y * z = x$.

To show that # and * are compatible, we use induction on n to show that, for all n, we have: x # x # . . . n x's = x * n. By hypothesis this is true for n = 1, since we have x * 1 = x = x. . 1 x.

Now, assume that it's true for n = k. Then, using the inductive hypothesis, we have:

x # x # . . . k+1 x's = ((x * k) # x, by Lemma 2

= x * (1 + (x*k) \ x) , by the definition of #

= x * (1+k), by the definition of \

Thus the statement is true for all n, and the theorem is proven.

All this provided a refreshing break from Calculus! Decades later (after getting my PhD, doing research in Schwartz distribution theory and abstract algebra, making a small career as a poet and writer, and a large career as a mother of four), I again got back to that original high school question: Can we have a hierarchy of processes, each the iteration of the previous, such that they're all both commutative and associative. I must have acquired some more sophistication, or perhaps just getting away from it for a long while helped. Or else life had taught me that some things are impos -sible, and that this is not always bad. At any rate, it was easy, both mathematically and emotionally, to replace my youthful "quest" with the following non-existence theorem:

Theorem 2: Let # be a "generalized addition" and let * be its compatible "generalized multiplication". Then, if # is associative and if, for all integers x, we have 1 * x = x, then # must be "regular addition" and * must be "regular multiplcation" -- that is, # and * together constitute "regular arithmetic".

Proof: Let x and y be positive integers. Then we have:

x * y = (1 * x) * y, by the hypothesis

= (1 # 1 # . . . x 1's) * y , since # and * are compatible

= (1 # 1 # . . . x 1's) # (1 # 1 # . . . x 1's) # . y of these

= 1 # 1 # . . . xy 1's, since # is associative

= 1 * xy

= xy, again by hypothesis.

Thus * is regular multiplication. To show that # must be regular addition:

x # y = (1 * x) # (1 * y), by hypothesis

= 1 * (x+y), by Theorem 1, since # is associative

= x + y, by hypothesis

and the theorem is proven. This, then, characterizes all arithmetics with associative "addition" such that the identity 1 * x = x is satisfied (that is, "multiplication" possessing left identity 1).

Corollary: If # is associative and * is commutative, then # and * constitute regular arithmetic.

Proof: If * is commutative, then for all positive integers x, we have 1 * x = x * 1 = x, and the theorem just proven applies.

The hypothesis 1 * x = x of the theorem seems a natural property for a "generalized multiplication", but suppose we remove it? That is, what if we merely hypothesize that # is associative?

This by itself leads us nowhere. After all, without any stipulations on * , ANY #, associative or not, gives rise via iteration to SOME "multiplication" *. However, what happens if we hypothesize BOTH # AND * associative?

At this point we need to consolidate our terms: We will call a binary operation # an ASSOCIATIVE ARITHMETIC if both # and its compatible * are associative. Also, if # is ordinary addition, then we will call the resulting arithmetic REGULAR. Our question, then, is: Must any associative arithmetic be regular? And if not, how is # (and therefore *) constrained? What, that is, can we say about associative arithmetics? Can we characterize them?

An associative, non-regular arithmetic could not, by the proof of the above Corollary, satisfy the identiy 1 * x = x. So as a first step, I decided to look for properties equivalent to 1 * x = x being an identity, but whose negations might be easier and more promising to work with. I had also begun to wonder whether or not # and/or * must necessarily be monotone (strictly or not), as are in regular arithmetic. These two endeavors would up connecting in the following:

Lemma 5: Let # be an associative arithmetic. Then the following statements are pairwise equivalent:

(A) 1 * x = x, for all x, where * is the "multiplication" compatlble with #

(B) For all m and n, 1 * n = 1 * m implies n = m.

(C) # is regular.

Proof that A implies B: Assume we have A but not B. Then there exist distinct n and m such that 1 * n = 1 * m. Thus by A, we have 1 * n = n and 1 * m = m, and therefore n = m, contrary to our assumption that n and m are distinct.

Proof that B implies A: Assume that A is not true. Then there exists m such that $1 * m = m$. Now, let M denote $1 * m$. Then $M = m$ and $1 * M = 1 * (1 * m) = (1 * 1) * m$ (by associativity of *), which equals $1 * m$, contradictory to B. This completes the proof of the lemma.

That A implies C has already been shown in Theorem 2, and the converse is easily seen via considering the 1 times table. The proof of Lemma 5 is thus complete.

Property B is the beginning of a structure theorem for the generalized "1 times table" of all non-regular associative arithmetics:

Theorem 3: Let # be an associative arithmetic which is not regular.

Then there exist integers n and m such that $n > m$ and $1 * n = 1 * m$.

Further structure is provided by:

Theorem 4: Let # be an associative arithmetic which is not regular. Then:

(A) There exists a SMALLEST ordered pair (m, n) (That is, (m, n) is the smallest in the sense of ordered pairs, meaning that if (m', n') is such an ordered pair, then m is smaller than or equal to m, and n is smaller than or equal to n.)

(B) For all positive integers i, we have $1 * (n+i) = 1 * (m+i)$

(C) The function $1 * i$ (of i) has period n-m "beginning with m" -- that is, for all positive integers j greater than or equal to m, we have $1 * (j+n-m) = 1 * j$.

(D) If $i < m$, then $1 * i = i$.

(E) For all integers i, we have $1 * i = i \bmod (n-m)$

(F) If $1 * i = 1 * j$, then we must have $i = j \bmod (n-m)$, and i and j greater than or equal to m.

(G) In particular, n-m is the SMALLEST "period beginning with m".

Proof: To prove (A), first work with m; there ALWAYS exists a smallest positive integer satisfying ANY property, so there exists a smallest m such that there exists n not equal to m such that $1 * n = 1 * m$. In turn, once we have that smallest m, choose the smallest such n.

(B) happens because of the compatibility of # and *; thus we have $1 * (n+i) = (1 * n) \# 1 \# 1 \# \ldots$ i 1's $= (1*m) \# 1 \# 1 \# \ldots$ i 1's $= 1 * (m+i)$

(C) is just another way of stating (B).

To prove (D), assume that we have $i < m$ and $1 * i$ does not equal i. Then, since $1 * (1 * m) = (1 * 1) * m = 1 * m$, therefore by the choice of m (according to A), we must have both i and $1 * i$ greater than or equal to m, which contradicts the hypothesis that $i < m$.

The proof of (E) uses “periodicity beginning with m”, and the fact that n-m is the SMALLEST such period. We need only note that, for i greater than or equal to m, we have 1 * (1 * i) = 1 * i (as already observed in the proof of #), so that 1 * i and i must differ by a multiple of n-m, from which follows (E). For i < m, we have (D), which of course implies (E).

To prove (F), let i and j be such that 1 * j = 1 * i, with i < j. Then certainly i and j are both greater than or equal to m; otherwise this would contradict the definition of m. Now, assume that i and j are NOT equal mod (n-m). Then, by periodicity after m, we can assume without loss of generality that j - i < n-m, and that i and j are both less than n. But then we could “bring i up to n” (that is, we could take i = n) -- via the same method as in the proof of (B) -- and finally we could, via periodicity after m, “bring both i and j down to me” (that is, we could take i + m); j wold then be less than n, and the definition of n would be contradicted.

(G) follows directly from the proof of the first statement of the theorem, which completes the proof of the entire theorem.

Let us make this “1 times table” more visual. Again, Theorem 4 says that, for any given non-regular associative arithmetic, the 1 times table must take a particular form. Here is an example of a 1-times table which takes that form:

m = 4, n = 7, n-m = 3 -- Note that for i < 4 we have 1 * i = i, and that 1 * i and i are always congruent mod 3, and that beginning with i = 4, the top line is periodic with period 3 (and that 3 is the SMALLEST such period).

1 * i	1	2	3	10	8	6	10	8	6	10	8	6	. . .
i	1	2	3	4	5	6	7	8	9	10	11	12	. . .

But of course, besides the 1 times table, we still have the OTHER times tables to concern ourselves with. We need some properties of those. .Our next theorem takes us a step further; it tells us the 1 * j times table, for any 1 * j -- I call this the 1 times times table.

Theorem 5: let # be a non-regular associative arithmetic, with multiplication *. Then, for all positive integers i and j, we must have:

$$(1 * j) * i = 1 * ji$$

As in previous proofs, this follows from the compatibility of # and *.

Thus the 1 times times table must take a particular form; in fact, it’s DETERMINED by the 1 times table. An visual example follows (which includes the above “picture” of the 1 times table):

Again, m = 4, n = 7, n-m = 3

Note that, visually, for all j, the 1 * j times table is obtained by taking every jth number from the 1 times table.

(Next is 10 * i again, and it keeps repeating, so we don't need to put them in.)

6*i = (1*6)*i = 1*6i	6	6	6	6	6	6	6	6	6	6	6	6	. . .
8*i = (1*5)*i = 1*5i	8	10	6	8	10	6	8	10	6	8	10	6	. . .
10*i = (1*4)*i = 1*4i	10	8	6	10	8	6	10	8	6	10	8	6	. . .
3*i = (1*3)*i = 1*3i	3	6	6	6	6	6	6	6	6	6	6	6	. . .
2*i = (1*2)*i = 1*2i	2	10	6	8	10	6	8	10	6	8	10	6	. . .
1*i	1	2	3	10	8	6	10	8	6	10	8	6	. . .
i	1	2	3	4	5	6	7	8	9	10	11	12	. . .

As we can see, however, this still hasn't told us anything about, for example, the 4 times table, or the 5 times table, and so on. What must these "others" look like, in order to be an associative arithmetic? Let us, then, concern ourselves with the other times tables. Our next definition takes us "one step beyond".

Definition: Let # be a non-regular associative arithmetic, with multiplication *. Then since, as we've seen, not all of the integers are in the one-times table , there is a LEAST integer which is NOT in the 1 times table. Denote that integer by x_2 and call it the BASE OF THE SECOND LEVEL (the first level being the 1 times times table).

The next theorem describes, for every non-regular associative arithmetic, what the second level must look like. (As we'll see, it has many things in common with the first level, but not all.)

Theorem 6: Let # be a non-regular associative arithmetic, with multiplication *. Then the x_2 times table must satisfy the following properties:

(A) x_2 * n = x_2 * m (where m and n are the same m and n that we have been dealing with for the FIRST level.). Note, however, that (m, n) might not be the SMALLEST such ordered pair (as they were for the first level).

(B) For all positive integers j greater than or equal to m, we have x_2 * (j+n-m) = _2 * j. (That is, the function x2 * i of i has period n-m "biginning with m".) NOTE: n-m might not be the SMALLEST such period.)

(C) Let (m_2, n_2) denote the SMALLEST ordered pair such that n_2 > m_2 and x_2 * n = x_2 * m. Then n_2 - m_2 is the smallest period beginning with m_2 of the function x_2 * i (of i) and is therefore a divisor of n-m. Moreover, (n-m) / (n_2 - m_2) divides x_2.

(D) m_2 is less than or equal to m, and n_2 is less than or equal to n.

(E) If m_2 < m, then n_2 < n.

(F) The x_2 * i, for i < m_2, are all distinct.

(G) If x_2 * i = x_2 * j, then i and j are congruent mod (n_2 - m_2), and i and j are both greater than or equal to m_2.

(H) x_2 * i and x_2 x i (meaning ordinary multiplication) are congruent mod (n-m).

(I) For all positive integers i and j, we have (x_2 * i) * j = x_2 * ij. (That is, as with the 1 times times table in Theorem 5, the _2 times table determines the x_2 times times table.)

Since the ideas involved in the proof of Theorem 6 are similar to those of Theorem 4 we will omit that proof. Instead, let us first give the picture (below) -- a continuation of the previous example (with the second layer added on) and then move on to ALL levels, by defining them inductively, just as we moved from the first to the second level.

m = 4, n = 7, n-m = 3, x2 = 4 Note that, throughout this "multiplication table", each x * y is congruent mod (n-m) to xy (the ordinary product of x and y). Again, for all j from 1 to 6 (n-1), the 4 * j times table consists of every jth number in the 4 t times table.

18*i = (4*6)*i = 4*6i	18	18	18	18	18	18	18	18	18	18	18	18
29*i = (4*5)*i = 4*5i	29	13	18	29	13	18	29	13	18	29	13	18
13*i = (4*4)*i = 4*4i	13	29	18	13	29	18	13	29	18	13	29	18
9*i = (4*3)*i = 4*3i	9	18	18	18	18	18	18	18	18	18	18	18
11*i = (4*2)*i = 4*2i	11	13	18	29	13	18	29	13	18	29	13	18
4*i x_2 =	4	11	9	13	29	18	13	29	18	13	29	18
6*i	6	6	6	6	6	6	6	6	6	6	6	
8*i	8	10	6	8	10	6	8	10	6	8	10	
10*i	10	8	6	10	8	6	10	8	6	10	8	
3*i	3	6	6	6	6	6	6	6	6	6	6	
2*i	2	10	6	8	10	6	8	10	6	8	10	
1*i	1	2	3	10	8	6	10	8	6	10	8	
i	1	2	3	4	5	6	7	8	9	10	11	

Of course, once again, this doesn't give ALL the multiplication tables, and thus does not completely describe the multiplication *. Once again, however, we can move on to the THIRD level, and then the fourth, and so on. here is the theorem which say just that. (It "looks" very much like the previous theorem and, again, the ideas in the proof have already been explained.)

Theorem 7: Let # be a non-regular arithmetic, with multiplication *. Let x1 = 1, and assume that levels x have been defined, for s < r. Then we can define inductively level r as follows:

Set x_r = the least positive integer which is not in any of the "previous" times tables (that is, not equal to x_s * j, for any s < r and any positive integer j).

Then this x_r times table must satisfy:

A) x_r * n = x_r * m, where m and n are as they have been (first introduced in Theorem 5A).

B) For all positive integers j >= m, we have x_r * (j+n-m) = x_r * j. (That is, the function x_r * i has period n-m befinning with m. n-m might not be the SMALLEST such period.)

C) Let (m_r, n_r) denote the smallest ordered pair such that n_r > m_r and x_r * n_r = x_r * m_r. Then n_r - m_r is the smallest period beginning with m_r of the function x_r * i (of i), and is therefore a divisor of n-m. Moreover, (n-m) / (n_r - m_r) divides x_r.

D) m_r <= m and n_r <= n

E) If m_r < m, then n_r < n.

F) The x_r * i, for i < m_r, are all distinct.

G) if x_r * i = x_r * j, then i and j are congruent mod (n_r - m_r), and i and j are both >= m_r. Further, the x_r times table (and thus the x_r times times table) must take the form, (x_r * i) * j = x_r * ji.

H) x_r * i and (x_r)i (ordinary product of x_r and i) are congruent mod (n-m).

And now let's return to our original question: Can we characterize associative arithmetics? That is, having just found a structure that associative arithmetics MUST take, does the converse hold: do ALl binary operations which are constructed according to properties A through H of the last theorem turn out to be assocaitvie arithmetics? More precisely: IF we define a binary operation * by constructing, first, the 1 times table satisfying properties A through H in Theorem 4, then the 1 times times table, and inductively from that a hierarchy of times times tables satisfying properties A through H in Theorem 7,, then will * give rise to an associative arithmetic?

The answer to that question is unfortunately complex. There are two sources of trouble. First, although * is relatively easily proven to be associative (and this will be done below), this is so only if * is DEFINED. The reason that * is not necessarily defined is: In defining each of the x_r times times table (from the x_r times table),

we define $(x_r * j) * k$ to be $x_r * jk$. However, suppose there is some other s not equal to r such that $x_r * j = x_s * i$? Then the same quantity $(x_s * i) * k$ would have to also be defined as $x_r * ik$, and this, in general, could lead to contraductions (and bedlam. . .) In other words, we need the following to hold:

$x_r * j = x_s * i$ implies that, for all K, we have $x_r * jk = x_s * ik$.

True, we might consider trying to circumvent this by DEFINING, as incorporated into the inductive definition, the xr times times table by:

$(x_r * j) * k = x_s * ik$ whenever we have $x_r * j = x_s * i$, $s < r$.

However, there would then be the possibility of the existence of MORE THAN ONE such s (and its accompanying i), and we would need to insure that all such s's (and i's) give rise to the SAME value of $x_s * ik$.

The second source of trouble is: recall that an arithmetic necessitates, not only a generalized multiplication *, but also a generalized addition #., and that the two have to be compatible. True, Theorem 1 (the "college freshman theorem") concerns finding, given *, a compatible #, but only for those * which admit solutions z to the equation $x * z = y$. (What this amounts to, in the case of the *'s defined and described here, is a defintion for $x \# y$ only when x and y are on the same "level".)

In other words, at this point, I haven't figured out how to construct ALL associative arithmetics -- in particular, all NON-REGULAR associative arithmetics. However, it CAN be shown that there DO EXIST non-regular associative arithmetics. I will briefly describe how:

It turns out that, if we construct "times times tables" satisfying the properties in Theorems 4 and 7, thus defining a binary operation *, and such that the 'levels" -- meaning the x_r times tables -- are pairwise disjoint, then this circumvents BOTH difficulties. (It is possible to do this, since each x_r times table is eventually periodic and thus contains only a FINITE number of numbers; in constructing each level from all the previous, there are always an infinite number of OTHER numbers to choose from -- even considering the requirement that $x * y = xy \bmod (n-m)$; in the Example on page 8, this was done up to the second level.) Thus it can be shown that if, in constructing each level, we simply avoid using numbers which have already been used (in constructing the previous levels), then we wind up with a non-regular associative arithmetic.

The proof would be long and (mostly) straightforward. It would proceed via several lemmas, which are presented without proof below (all under the hypothesis that the "times tables" are constructed inductively to satisfy the conclusions of Theorem 7):

Lemma 6: Every integer is contained in one and only one level. (And thus x*y is always uniquely defined.)

Lemma 7: For all integers x and y, x*y is congruent mod (n-m) to xy (the ordinary product).

Lemma 8: * is associative.

Lemma 9: Define a binary operation # on all pairs of positive integers by:

Case I: If x and y are in the same level, then we have, for some integer r, $x = x_r * i$ and $y = x_r * j$. We then define:

$$x \# y = x_r * (i+j)$$

Case II: if x and y are in different levels, then we define $x \# y$ to be whichever of x and y is in the higher level.

Defined in this way, # is associative and compatible with *. (This last is straighforward to check. In fact, Case I of the definition is DETERMINED by this compatibility requirement -- in particular, from my "high school Lemma 4 at the beginning of this paper.)

A couple of weeks ago, around 2:00 A.M., the phrase "equivalence classes" suddenly jolted me awake. I meant equivalence classes of times tables. Given an associative arithmetic, two times tables are said to be equivalent if they intersect. It isn't entriely trivial that this IS an equivalence relation, but it is. Thus, if things work out right, the times tables will be organized into NEW "times tables", which are disjoint. I'm working on this now. (but 2:00 revelations are, for me, rare...). The new "extended times tables" involve an "extended multiplication" * (still denoted by *, at least while I'm working on it...), with the second variable running through a semi-group c rationals. Under reasonable conditions, "extended multiplication" is defined, and associative, if the "original multiplication" is, and associative arithmetics satisfying these conditions can, I conjecture, be characterized. I would like, of course, to remove those conditions.

I'll end with the remark that there exist non-regular COMMUTATIVE arithmetics (that is, # and * are both commutative), and that I hope to find a structure theorem characterizing ALL commutative arithmetics.