My Own Private World of Non-Ordinary Associative Arithmetics

Marion D. Cohen
Drexel University

Follow this and additional works at: https://scholarship.claremont.edu/jhm

Part of the Arts and Humanities Commons, and the Mathematics Commons

Recommended Citation
Marion D. Cohen, "My Own Private World of Non-Ordinary Associative Arithmetics," Journal of Humanistic Mathematics, Volume 14 Issue 2 (July 2024), pages 60-106. Available at: https://scholarship.claremont.edu/jhm/vol14/iss2/5

©2024 by the authors. This work is licensed under a Creative Commons License. JHM is an open access bi-annual journal sponsored by the Claremont Center for the Mathematical Sciences and published by the Claremont Colleges Library | ISSN 2159-8118 | http://scholarship.claremont.edu/jhm/

The editorial staff of JHM works hard to make sure the scholarship disseminated in JHM is accurate and upholds professional ethical guidelines. However the views and opinions expressed in each published manuscript belong exclusively to the individual contributor(s). The publisher and the editors do not endorse or accept responsibility for them. See https://scholarship.claremont.edu/jhm/policies.html for more information.
Abstract

A binary operation # on \( \mathbb{Z}^+ \) is said to be an associative arithmetic if both # and its iteration — the binary operation \( * \) defined recursively by: \( x*1 = x \) and \( x*y = [x*(y-1)]#x \) — are associative. E. Rosinger [6] showed that under reasonable conditions an associative arithmetic must be ordinary addition. However, in the general case, there are associative arithmetics that are not ordinary addition. This paper gives examples of these as well as results towards a structure theorem for associative arithmetics. The paper also describes the role that this particular math problem has played in my mathematical life.

Keywords. arithmetic, associative, addition, multiplication, iteration, modular.

1. Introduction

Right now nobody else even knows what an associative arithmetic is! (If I write the plural “arithmetics” Google puts a red line under it.) Well, I have told a few mathematical friends and colleagues, but still nobody else knows the details like Theorem 9, which gives necessary conditions that a binary operation be the iteration of an associative arithmetic. It’s nice to have this private world. It’s not that much of an ego thing; it’s more like I’m a kid in a hideout. Or a kid that’s fallen into some mystery and becomes a kid detective perhaps solving or preventing a murder. Or like I’m the first one to know a wonderful secret.

If my associative arithmetics wind up getting published, they’ll still be in some respects private. And even if the research turns out to be incorrect or
not original, it's still been a private world for a while and in some respects will continue to be. Is that how other mathematicians feel about their research?

Math itself is kind of a private world since it has such interesting press. When you tell people you're a mathematician, they often get intrigued and curious, perhaps a tad jealous or the opposite of jealous. For me, math was definitely a private world back in high school when I was the only “girl in math” nicknamed “Mathbrain” by the other students. I liked being unique and mysterious, even though it meant being alone in some ways. And math meant so much to me that it was hard for me to talk about it. It was, yes, a private world, perhaps too private, more private than it is now that I'm all grown up.

I've been thinking of the following question for mathematicians and perhaps also for non-mathematicians: What was your first math? The first math you knew about? Do you remember how you became aware that there's such a thing as math?

I know how I would answer that question. Probably as for many or most others, my first math was shapes. But after that, and possibly more salient, came counting. And my second math was arithmetic — “the big four”: addition, subtraction, multiplication, division. Later came exponentiation, roots, and logs. It was a while before I knew on a conscious level that there was such a thing as math and then decided that this math was the thing for me (what I would be going to college for, what I would do when I grew up). But it was around fourth or fifth grade that I was curious about math-things — more curious than about history or geography things (“social studies”). One math-thing I was curious about was “Mr. Magic 9” which our teacher had told us about. (The magic is: a number is divisible by 9 if and only if the sum of its digits is.) I was curious about whether there was some form of “Mr. Magic 8” or 7 or 6. I'd sit in geography class and work out times tables and digit-sums. I saw patterns but none, to my dismay, as short and cool as “Mr. Magic 9”.

Another math-thing I was curious about was the “invert and multiply” rule. I wanted to convince myself and therefore believe that it worked. For a child, believing is often enough; I didn't need a proof or even an official reason. I made diagrams (during geography class) to convince myself that, for example, 86/57 truly did fit into (I didn’t yet know the word “gozinta”) 39/62 the quantity \(\{(86/57) \times \frac{62}{39}\}\) times. I remember using unlikely high
numbers like 57 and 86. I remember that in order to convince myself of the invert and multiply rule I needed to think about what a fractional number of “times” would mean. For example, 6 fits into 3 half a time.

I think it was around third grade that we learned how multiplication is repeated addition. (We didn’t say “iterated” or “iteration” then as I do now.) It took a few years to realize how enamored I was with this repetition thing. I was also enamored with commutativity and associativity. Over my early-adolescent years I wondered several things about those “big three”: iteration, commutativity, and associativity. At first I felt puzzled that exponentiation is neither commutative nor associative. It had seemed to me that multiplication is commutative and associative because it’s the iteration of the commutative associative addition and that therefore exponentiation, being the iteration of multiplication, should also be commutative and associative. But then I came to realize that things were different from how I’d thought; the commutativity and associativity of addition were not the reasons for the commutativity and associativity of multiplication. Geometry would provide good proofs for the commutativity and associativity of both addition and multiplication — and there’s no such geometry for exponentiation. (Of course, I didn’t in those days know about things like Peano’s axioms and Cantor’s theories.)

Was it in eighth or ninth grade that taking algebra made me conscious that math was a big passion? (I didn’t use the word “passion” then.) Somehow, even though I’m “good” at childhood and adolescent memories, I don’t remember which grade I was in. I do remember that algebra and my fascination with arithmetic made me decide to use algebra to find out which pairs of numbers had the same products as sums. It was interesting to me that (2, 2) and (0, 0) were the only pairs consisting of two integers and I liked writing down examples of non-integer pairs.

In early high school, I wondered about the iteration of exponentiation. Every binary operation has to have an iteration so exponentiation does too. And then you could talk about the iteration of that. There could be a whole hierarchy of processes each the iteration of the preceding. I wondered whether there might be some binary process, some kind of “alternative addition”, all of whose “higher iterations” were both commutative and associative. Or maybe only commutative or only associative?

I also marveled at the idea that not only was $2 \times 2$ equal to $2 + 2$ and $2^2$ also equal to 4 but 2 with 2 in all the “higher processes” — meaning the
higher iterations — was also equal to 4. Why did 2 have this property? (I
later became fascinated with the number 2, its various unique, often obvious
properties. In my college freshman year, I made a list of them and recently
wrote a long poem about the lower positive integers from 1 to 4.)

Back to high school, early and later: I was a newbie. The lemmas and
theorems I came up with about commutativity, associativity, and iteration
were few, far between, and not interesting enough for me. But I believed that
there was a lot to eventually discover about these “big three”. And I enjoyed
calculating various iterations (besides multiplication and exponentiation).
For example, the iteration of \(xy + x + y\) (which is commutative and associiative)
is \((x + 1)^y - 1\) (not commutative or associiative). And the iteration of \(x + 1\)
(a constant function of \(y\) not commutative or associiative) is \(x + y - 1\).

I wrote all this down in a special notebook which (in my adolescent Angst)
I titled “My Very Own System”. Just now writing this paper (in old age
Angst?) I call it “my private world” the titular phrase of this paper. I
brought the notebook with me to my college dorm and in my freshman
year amidst calculus and lesser-liked classes like “Western Civ” I became
somewhat more math-sophisticated. My new idea was the opposite problem
from finding iterations of given binary operations. I thought about starting
with a possible iteration (what I thought of as “generalized multiplication”)
and asking what “generalized addition” that might be the iteration of.

I soon realized that not all binary processes could be iterations; an iteration
* has to satisfy \(x * 1 = x\) for all \(x\). Soon after that I identified the other
more extensive requirement for an iteration: if * is the iteration of some #,
we must have for all \(x\) and all positive integers \(k\) the recursion

\[
x * k = (x * (k - 1))#x.
\]

This “formula” gave me an idea. Once we’re given *, we have \(x * 1 = x\) for all
\(x\). And that gives us \((x * 1)#x = x * 2\). Which gives us \((x * 2)#x = x * 3\). In
general \((x * (k - 1))#x = x * k\). Thus to find \(y#x\) for all \(y\), if we can express
\(y\) in the form \(x * (k - 1)\) for some \(x\) and some \(k\), that gives us \(y#x = x * k\).
And I reminded myself we know *, so we know \(y#x\). Therefore if given \(y\)
and \(x\), we can solve the equation \(y = x * (k - 1)\) for \(k - 1\), and therefore
for \(k\), we have \(y#x = x * k\), where \(k - 1\) is the solution \(z\) to the equation
\(y = x * z\). After playing with variables — for example changing the \(z = k - 1\)
to \(z + 1 = k\) — my “college freshman formula” becomes:
Given an iteration \(*\), a “compatible” (as I much later termed what \(*\) could be the iteration of) \(\#\) can be given by:

\[ y\#x = x\ast(z+1) \text{ where } z \text{ is the solution to the equation } y = x\ast z. \]

(And if to be consistent with the notation in the problem of finding a \(\#\) compatible with \(\ast\) we want to interchange \(x\) and \(y\) we’d have:

\[ x\#y = y\ast(z+1) \text{ where } z \text{ is the solution to the equation } x = y\ast z. \]

There are a number of possible iterations — that is, binary operations \(\ast\) which satisfy \(x\ast1 = x\) for all \(x\). Thus there are a number of binary processes for which Equation 1 might be solved.

But I knew that my formula was not quite a theorem; it wasn’t completely rigorous. One trouble is that the solution(s) to Equation 1 might not be a positive integer. And my theory then and now is about positive integers.\(^1\) However, “the college freshman formula” does often work, meaning that for a number of possible iterations — meaning binary operations \(\ast\) for which 1 is a right identity — the formula finds what \(\ast\) is an iteration of. Also as we’ll see, this formula is what gave me the idea for the important Theorem 11 in Section 4 which leads to several classes of associative arithmetics.

Here are four examples of finding given \(\ast\) a compatible \(\#\):

**Example 1.** \(x + y\) is NOT a possible iteration since \(x + 1\) does not (ever) equal \(x\). However, if we modify it by setting \(x\ast y = x + y - 1\), then the college freshman formula goes as follows in two steps:

First, for every \(x\) and \(y\), solve the equation for \(z\): \(x = y \ast z\). That is \(x = y + z - 1\). So we get \(z = x - y + 1\).

Then calculate \(x\#y = y\ast(z+1) = y+(z+1)-1 = y+z = y+x-y+1 = x+1\).

If we want, we can check to see that \(x+1\) does indeed have the iteration \(x + y - 1\).

\(^1\) Someday I’ll restate the “formula” more precisely, make it into a theorem; perhaps I can add to the hypothesis that \(\#\) can be extended from \(\mathbb{Z}^+ \times \mathbb{Z}^+\) to \(\mathbb{R}^+ \times \mathbb{R}^+\) or just hypothesize that \(\#\) is a binary process on \(\mathbb{R}^+ \times \mathbb{R}^+\). That hasn’t been something I feel like doing nor have I felt necessary to do, or not yet.
Example 2. If we denote: \( x*y = x - y + 1 \), we can use our formula (Equation 1) since 1 is a right identity for \(*\). First, for every \( x \) and \( y \), solve the equation for \( z \): \( x = y*z \). That is, \( x = y - z + 1 \). Algebra gives us \( z = y - x + 1 \). Then calculate

\[
x\#y = y*(z+1)
\]
\[
= y*[y-x+1-1]
\]
\[
= y - (y - x + 1 - 1 + 1)
\]
\[
= y - (y - x + 1) = x - 1.
\]

Example 3. Let \( x*y = x/y \) (so 1 is a right identity for \(*\)). First, for every \( x \) and \( y \), solve the equation for \( z \): \( x = y*z \), that is, \( x = y/z \). Thus \( z = y/x \). Finally, calculate

\[
x\#y = y*(z+1)
\]
\[
= y*(y/x + 1)
\]
\[
= y/(y/x + 1) = xy/x + y.
\]

Example 4. Let \( x*y = xy + y - 1 \) (Again 1 is a right identity for \(*\)). First, for every \( x \) and \( y \), solve the equation for \( z \): \( x = y*z \). Thus: \( x = yz + z - 1 = (y + 1)z - 1 \), so algebra gives us \( z = (x + 1)/(y + 1) \). Then we calculate:

\[
x\#z = y*(z+1)
\]
\[
= y*[(x + 1)/(y + 1) + 1]
\]
\[
= y*[(y + x + 2)/(y + 1)]
\]
\[
= y[[y + x + 2]/(y + 1)] + [(y + x + 2)/(y + 1)]
\]
\[
= [(y^2) + xy + 2y + y + x + 2 - y - 1]/(y + 1)
\]
\[
= [(y^2) + xy + 2y + x + 1]/(y + 1)
\]
\[
= x + y + 1.
\]

Over the years and decades I have engaged with mathematics in a variety of ways. My Master’s thesis was on Schwartz distribution theory and included an original theorem, and my Ph.D. dissertation was on an idea coming from a generalization of that theorem. (Schwartz himself was my advisor in absentia.) I have just a few published math papers; one is an offshoot of distribution theory, another is a generalization of a generalization of the ratio test. And over the years and decades, I taught math, mostly adjuncted.
Math continued to be a passion, and when I became a poet, “math poetry” was possibly my forte in both my math and my poetry careers. My poetry book *Crossing the Equal Sign* [3] describes what math research feels like, at least to me. (But other mathematicians as well as physicists have related to that book.)

But I didn’t forget what I called “alternative arithmetics”. I thought of new and better questions and wrote up more and more lemmas and theorems. I knew that it probably wasn’t what other mathematicians were “doing” but I didn’t care. My years and decades as a mathematician and math professor gave me some further mathematical sophistication, and I easily proved for example that there could not be a “generalized addition” whose infinite sequence of iterates were all commutative and associative. I proved other stronger theorems of that ilk (for example, if a binary process is associative and its iteration is commutative, that process must be addition) and soon stopped “worrying” about any “third or higher process” — at least as of this writing...

I concentrated on associativity. My main question, the topic of this paper, has been: Are there binary processes other than addition which are associative and which have associative iterations? And if so, what must these binary processes look like? I did realize that there are indeed what some might call “trivial” binary processes other than addition which fit that bill. $x \# y = \max(x, y)$ is one of them. Min would work, too. But I wanted more information and more examples, especially those that were less trivial-seeming.

It wasn’t all that long ago that I decided to be more practical and get googling. I don’t always care whether what I’m working on has already been done, but now I was becoming curious. Had other mathematicians worked on this kind of thing? Had they gone other routes, asked further questions, found other results?

There wasn’t a whole lot on google. There was something about the higher orders (in particular the fourth and the fifth) of iterations of addition.² The only other mathematician I could find who worked on such things was

---

Elemer Rosinger. His work didn’t answer all my questions. But he proved theorems which contained the phrase “right regular” and I needed to know what “right regular” meant so I could if need be (and as you’ll see need eventually did be…) use his theorems. I found his email address and wrote him and was surprised when he wrote back in particular to tell me that “right regular” was his term for one-to-one in the second variable. He and I corresponded for a while, and in fact, I’m going to brag a tad because he said something that meant a lot to me and to my perceptions about my mathematical life. He told me that he had worked on “regular things,” in particular some pretty hefty physics stuff, but that he also had this interest in and high regard for what I had called “alternative arithmetics”. And he complimented me, writing “You’re not just ANY mathematician”.

I haven’t always been certain that I’m any mathematician at all. I’m not very much of a problem solver; if anything, I’m a theory creator. I don’t qualify as a tenure-track professor though I’ve had a couple of full-time math prof positions. Mostly, as I said, I’ve adjuncted while living a lot of my other passions such as writing poetry and sometimes memoir, having babies and rearing children, and my less serious passion for thrift-shopping. Until rather recently, I haven’t really thought of myself as a “real” mathematician; I knew only that math was my most serious passion (except for family), and that being a theory creator, I was also a problem creator, so I was always working on some problem or other and usually not getting publishable solutions. So to be called “not just ANY mathematician” by a “real’ mathematician” meant a lot to me, and it solidified and affirmed what math has meant to me.

I’ve written a lot about what math has meant to me. It’s in my poetry book *Crossing the Equal Sign* [3] and is scattered throughout my other poetry books as well as unpublished writings. But there’s a lot more. One could say that I like easy math. Or math that’s easy to me. Or at any rate, math that seems easy (to all). I like math that goes back to fundamental stuff, to what I called first math at the beginning of Section 1. I like conjectures that are easy to state but hard to prove. But since I’m not a problem solver, I can’t prove them. So theory creator that I often am, I think of definitions. And then I explore them.

About definitions and back to “my own private world”: I’m the only one who made those particular definitions. And then I’m the only one who thought of those lemmas and theorems, trivial though they might turn out to be.
Even if somebody else thought of those concepts, they probably didn’t call them by the same names. Again, it’s like I’m a kid making up a secret code.

I’ve written elsewhere (in my review [4] of Mathematicians on Creativity [2]) that in striving for mathematical creativity I like to go back to childhood, maybe even babyhood, real or perceived. And so arithmetic was, along with shapes, my “first math,” and now it’s become my latest. It’s also been, as we’ve seen, recurrently and persistently in the middle.

2. Other Associative Arithmetics

Here’s another way to phrase my high school questions: Suppose humankind had defined addition differently and then iterated this “new addition” to get a “new multiplication”? What exotic arithmetic might result? Any binary operation # on $\mathbb{Z}^+$ could be thought of as a “generalized addition” and iteration of # as a “generalized multiplication” *. The example given in Section 1 is $x\# y = xy + x + y$ restricted to $\mathbb{Z}^+ \times \mathbb{Z}^+$ as “addition”, which gives rise via iteration to $x \ast y$ as “multiplication”. In this example, “addition” is associative, but “multiplication” is not. In Section 1, I also talked about how I came to concentrate on binary operations # on $\mathbb{Z}^+$ that are associative and whose iterations $\ast$ are also associative; in this section we will see more details as to how. When that happens, we say that # is an associative arithmetic; if # is ordinary addition (and thus $\ast$ ordinary multiplication) we say that the arithmetic is ordinary.

As we know, both addition and multiplication are associative so ordinary arithmetic is associative. Are there non-ordinary arithmetics which are associative? Rosinger [6] answered that question in the negative but only under certain conditions. What about in general? Are there non-ordinary binary operations # on $\mathbb{Z}^+$ such that both # and its iteration $\ast$ are associative? If so, can we characterize such #? What follows describes some headway in answering these questions. Let’s first consolidate definitions.

**Definition 1.** Let # be a binary operation on $\mathbb{Z}^+$. Then its iteration $\ast$ is defined inductively by:

$$x \ast 1 = x \quad \text{for all } x \in \mathbb{Z}^+$$

$$x \ast y = (x \ast (y - 1)) \# x \quad \text{for all } x, y \in \mathbb{Z}^+$$

**Definition 2.** Let # and $\ast$ be two binary operations on $\mathbb{Z}^+$. We say that # is compatible with $\ast$ if $\ast$ is the iteration of #.
We define an arithmetic to be a binary operation $\#$ on $\mathbb{Z}^+$, keeping in mind that any such $\#$ gives rise to its iteration $\ast$ and thus to a pair $(\# , \ast)$. We call a binary operation $\#$ on $\mathbb{Z}^+$ an associative arithmetic if both $\#$ and its iteration $\ast$ are associative. Finally, if $\#$ is ordinary addition, we say that $\#$ is ordinary.

Here are three perhaps uninteresting examples of non-ordinary associative arithmetics:

\[
\begin{align*}
  x \# y &= \max(x, y) \\
  x \# y &= \min(x, y) \\
  x \# y &= x
\end{align*}
\]

All three of these have iterations $x \ast y = x$. Later we will give more interesting examples. However uninteresting as these examples might be, they provide answers to two questions: (1) Must an associative arithmetic be commutative? The third example is clearly not. (2) Can distinct associative arithmetics have the same iteration? All three of these examples do.

Now, let’s get more information about the relationship between an associative binary operation on $\mathbb{Z}^+$ and its iteration; most of what follows is motivated by what happens with ordinary arithmetic:

**Lemma 3.** If a binary operation $\#$ is associative then $\#$ and its iteration $\ast$ must satisfy for all $x, y,$ and $z$ in $\mathbb{Z}^+$:

(A) \((x \ast y)\#(x \ast z) = x \ast (y + z)\). (This is a generalized distributive law.)

(B) \((x \ast y) \ast z = x \ast yz\). (This generalizes \((x^y)^z = x^{yz}\) and \((xy)z = x(yz)\).)

(C) \(x \ast j = y \ast i\) implies that for all \(K \in \mathbb{Z}^+\), \(x \ast Kj = y \ast Ki\).

Note that (A), (B), and (C) hold whether or not the iteration $\ast$ is associative but they hold in particular when $\ast$ is the (associative) iteration of an associative arithmetic.

**Proof of part (A):** We use induction on $z$. For $z = 1$ (A) is certainly true since \((x \ast y)\#(x \ast 1) = (x \ast y)\#x\) by the definition of iteration and thus \((x \ast y)\#(x \ast 1) = x \ast (y + 1)\), also by the definition of iteration. Now suppose (A) is true for $z = k$. Then we have:
(x * y)#(x * (k + 1)) = (x * y)#(x * (1 + k))
= (x * y)#[(x * 1)#(x * k)] by the inductive hypothesis
= [(x * y)#(x * 1)]#(x * k) by associativity of #
= [(x * (y + 1))#(x * k)] by the definition of iteration
= x * (y + 1 + k) by the inductive hypothesis
= x * [y + (k + 1)].

Thus (A) holds for z = k + 1 and therefore for all z.

**Proof of part (B):** We use induction on z. Certainly for z = 1 (B) is true by the definition of iteration. Now suppose (B) holds for z = k. Then we have:

(x * y) * (k + 1) = [(x * y) * k]#(x * y) by definition of iteration
= (x * ky)#(x * y) by the inductive hypothesis
= x * (ky + y) by (A)
= x * (k + 1)y.

Thus (B) holds for z = k + 1 and therefore for all z.

**Proof of part (C):** Suppose x * j = y * i. Then by (B) applied twice, we have for all K: x * K j = (x * j) * K = (y * i) * K = y * Ki and Lemma 3 is proven.

**Lemma 4.** If # is associative and if its iteration * satisfies 1 * x = x for all x ∈ Z^+, then # must be ordinary arithmetic.

**Proof:** Let x and y be in Z^+. Then:

x#y = (1 * x)#(1 * y) by hypothesis
= 1 * (x + y) by Lemma 3A since # is associative
= x + y by hypothesis.

It follows that * is multiplication and the lemma is proven.

This then characterizes all arithmetics with associative addition such that for all x, 1 * x = x (that is * possesses left identity 1); namely they must be ordinary:

**Corollary 5.** If # is associative and its iteration * is commutative, then # must be ordinary arithmetic.
Proof: If $*$ is commutative, then for all $x$, we have $1 * x = x * 1 = x$, and Lemma 4 applies.

This corollary was also proven by Rosinger [6].

It is perhaps worth mentioning two apparent counterexamples. First, consider addition and multiplication mod $N$ for any positive integer $N$. These are both commutative and associative and thus might seem to contradict Corollary 5. However, iterated addition mod $N$ is not the same as multiplication mod $N$ because $(N \times 1) \mod N = 0 \mod N$. The second apparent counterexample is “carryless arithmetic”, where addition and multiplication of two positive integers are calculated without “carrying”; see, for example, [1] for details. “Carryless arithmetic” might seem to contradict Corollary 5. However, “carryless multiplication” is not iterated “carryless addition.” For example, carryless multiplication of 10 and 1 yields 10, whereas iterated carryless addition — ten 1’s added “carrylessly” (carelessly?!...) — yields 0.

Rosinger [6] defines right-regularity of any binary operation on $\mathbb{Z}^+$ to mean being one-to-one in the second variable, and he studies arithmetics $#$ which are right-regular. But before knowing that, I had decided to consider instead right-regularity of possible iterations $*$. Here is a lemma which gives a good head-start towards investigating necessary conditions on any binary operation $*$ on $\mathbb{Z}^+$ for it to be the iteration of an associative arithmetic.

**Lemma 6.** Let $#$ be an associative arithmetic with iteration $*$. Then the following statements are equivalent:

1. $#$ is ordinary.
2. $*$ is right-regular (1-to-1 in the second variable). That is, for all $x, y, z \in \mathbb{Z}^+$, $x * y = x * z$ implies $y = z$.
3. For all $i$, $1 * i = i$.

Proof: That (1) implies (2) is clear. Now suppose (2); that is, assume that $*$ is right-regular, and let $i \in \mathbb{Z}^+$. Then letting $x = 1$ we have $1 * (1 * i) = (1 * 1) * i$ by associativity of $*$, so $1 * (1 * i) = 1 * i$ by the definition of iteration. Thus by right-regularity of $*$, $1 * i = i$, so (2) implies (3). Finally, that (3) implies (1) is the statement of Lemma 4. \qed
3. Investigating Necessary Conditions on Associative Arithmetics

According to Lemma 6, if \# is to be a non-ordinary associative arithmetic, its iteration * must not be right-regular. So consider the negation of the assertion that * is right-regular. That would mean that there exist, for some \( x \in \mathbb{Z}^+ \), two integers \( i, j \) (say \( i < j \)) such that \( x \cdot i = x \cdot j \). (Note that neither \( i \) nor \( j \) is necessarily unique.) We might then visualize what I at first called “the generalized \( x \)-times table,” and zero in on the row (technically the sequence):

\[ x, x \cdot 2, x \cdot 3, \ldots \]

We will call this the \( x \)-row. This could be made more visual, emphasizing the \( i \) and \( j \) mentioned above:

\[ x, x \cdot 2, x \cdot 3, \ldots, x \cdot i, x \cdot (i+1), x \cdot (i+2), \ldots, x \cdot j, x \cdot (j+1), x \cdot (j+2), \ldots \]

which becomes, by the negation of right-regularity, the following (where we “change” the \( x \cdot j \) to \( x \cdot i \)):

\[ x, x \cdot 2, x \cdot 3, \ldots, x \cdot i, x \cdot (i+1), x \cdot (i+2), \ldots, x \cdot i, x \cdot (j+1), x \cdot (j+2), \ldots \]

Further, we may change all the \( j \)’s to \( i \)’s because:

\[
x \cdot (j + 1) = (x \cdot j) \# x \quad \text{since } * \text{ is the iteration of } \#
\]

\[
= (x \cdot i) \# x \quad \text{since } 1 \cdot j = 1 \cdot i
\]

\[
= x \cdot (i + 1) \quad \text{again since } * \text{ is the iteration of } \#
\]

and by the same token, we have \( x \cdot (j + 2) = x \cdot (i + 2) \), and so on. So our “\( x \)-row” now looks like this (with all the \( j \)’s changed to \( i \)’s):

\[ x, x \cdot 2, x \cdot 3, \ldots, x \cdot i, x \cdot (i+1), x \cdot (i+2), \ldots, x \cdot i, x \cdot (i+1), x \cdot (i+2), \ldots \]

Do we detect an “eventual periodicity”? Indeed we do! Thus if * is to be the iteration of a non-ordinary associative arithmetic (actually any non-right-regular iteration at all), there exists an \( x \)-row which has an “eventual periodicity” of \( j - i \) starting at \( x \cdot i \). (Note that \( j - i \) is not necessarily the least periodicity.)

Further, we can now show that every “row” (not only that particular \( x \)-row) has an eventual periodicity. For this, let \( y \in \mathbb{Z}^+ \), and let \( m, n \) with \( m < n \).
be such that \((x \ast n) = (x \ast m)\). We have \(y \ast (x \ast n) = y \ast (x \ast m)\). But then by associativity of \(\ast\) and Lemma 3B, we also have:

\[ y \ast (x \ast n) = (y \ast x) \ast n = y \ast xn. \]

Similarly

\[ y \ast (x \ast m) = y \ast xn. \]

Therefore \(y \ast xn = y \ast xm\). Now since \(m < n\), we must have \(xm < xn\), so the \(y\)-row has eventual periodicity for every \(y\).

With this picture in mind, we can focus on eventual periodicity since this is the beginning of a necessary structure for any iteration \(\ast\) of any associative arithmetic. Let’s make some precise definitions:

**Definition 7.** Let \(\ast\) be the iteration of any non-ordinary associative arithmetic and let \(x \in \mathbb{Z}^+\). Then the \(x\)-row is defined to be the sequence

\[ (x \ast i : i \in \mathbb{Z}^+). \]

**Definition 8.** Let \(\ast\) be the iteration of any non-ordinary associative arithmetic and let \(x \in \mathbb{Z}^+\). Then we denote:

\[ (m_x, n_x) = \text{the smallest ordered pair } (i, j) \text{ such that } i < j \text{ and } x \ast i = x \ast j, \]

where ordered pairs of positive integers are given the lexicographic ordering:

\[ (i, j) < (i', j') \text{ if and only if either } i < i' \text{ or } i = i' \text{ and } j < j'. \]

Also, we denote \(m_1\) by just-plain \(m\) and \(n_1\) by just-plain \(n\).

Continuing to concentrate on the iteration \(\ast\) rather than on the arithmetic \#, we can look for further necessary conditions on a binary operation \(\ast\) on \(\mathbb{Z}^+\) for \(\ast\) to be the iteration of a (non-ordinary) associative arithmetic. In particular, armed with what was already mentioned about the eventual periodicity of the \(x\)-rows, we can investigate further properties of the \(x\)-rows, and thereby of \(\ast\). 1 is often a very special and useful number. Not only do we have \(x \ast 1 = x\), but using the 1-row as a kind of “base” turns out to be helpful.

**Theorem 9.** Suppose that \(\ast\) is the iteration of a non-ordinary associative arithmetic. Then \(\ast\) must have the following properties:
Property (1) There exist $i < j$ in $\mathbb{Z}^+$ such that $1 \ast i = 1 \ast j$, and therefore there exist $m, n$ such that $(m, n)$ is the smallest ordered pair $(i, j)$ with $i < j$ and $1 \ast i = 1 \ast j$, where ordered pairs of positive integers are given the lexicographic ordering:

$$(i, j) < (i', j') \text{ if and only if either } i < i' \text{ or } i = i' \text{ and } j < j'.$$

Property (2) For $i < m$, $1 \ast i = i$, and for $i \geq m$, $1 \ast i \geq m$.

Property (3) For all $x$ in $\mathbb{Z}^+$ (including $x = 1$), the $x$-row satisfies:

A) $x \ast 1 = x$.

B) $x \ast m = x \ast n$, and therefore there exist $m_x < n_x$ such that $(m_x, n_x)$ is the smallest ordered pair $(i, j)$ with $i < j$ and $x \ast i = x \ast j$. (This implies that the $x$-row, beginning with $i = m_x$, is periodic, with period $n_x - m_x$, and that this is the smallest such period.)

C) (Eventual periodicity) For $i \neq j$, we have $x \ast i = x \ast j$ if and only if $i, j \geq m_x$ and $i \equiv j \pmod{(n_x - m_x)}$. If $m = 1$, then $m_x = 1$, and this property simplifies to:

$$x \ast i = x \ast j \text{ if and only if } i \equiv j \pmod{(n_x - 1)}.$$

D) For all $x, y$ in $\mathbb{Z}^+$, we have $x \ast y \equiv xy \pmod{(n - m)}$.

Property (4) If both $x \ast j = y \ast i$ and $x \ast j' = y \ast i'$, then we must have

$$x \ast (j + j') = y \ast (i + i').$$

Property (5) $x \ast y < m$ if and only if $y \ast x < m$.

Proof: Property (1) is the result of our previous discussion.

To prove Property (2), first let $i < m$, and assume that $1 \ast i \neq i$. Now,

$$1 \ast (1 \ast i) = (1 \ast 1) \ast i,$$

by associativity of $\ast$, so

$$1 \ast (1 \ast i) = 1 \ast i.$$

But since $i < m$ and $1 \ast i \neq i$, this contradicts the construction of $m$. 

Next, let \( i \geq m \), and assume \( 1 \ast i < m \). But

\[
1 \ast (1 \ast i) = (1 \ast 1) \ast i,
\]

by associativity of \(*\), so

\[
1 \ast (1 \ast i) = 1 \ast i.
\]

But \( i \geq m \) so we must have \( 1 \ast i \neq i \). This contradicts the construction of \( m \), so our assumption cannot hold. Thus \( 1 \ast i \geq m \).

Property (3A) follows directly from the definition of iteration.

Proving (3B) involves a short calculation:

\[
x \ast m = (x \ast 1) \ast m
= x \ast (1 \ast m), \text{ by associativity of } *
= x \ast (1 \ast n), \text{ by (1)}
= (x \ast 1) \ast n, \text{ again by associativity}
= x \ast n, \text{ from the definition of iteration.}
\]

To prove Property (3C), in the “only if” direction, let \( x, i < j \in \mathbb{Z}^+ \) satisfy \( x \ast i = x \ast j \). We’ll show \( i \geq m_x \). Assume \( i < m_x \). Then by definition of \( m_x \), \( j = i \), contrary to hypothesis so

\[
i \geq m.
\]

We also have to show \( i \equiv j \mod (n_x - m_x) \). Assume not. Without loss of generality, by periodicity after \( m_x \), we can assume \( m_x < i, j < n_x \), so \( j - i < n_x - m_x \). We also have \( i, j \geq m_x \). Since \( x \ast i = x \ast j \), we must have

\[
x \ast (i + 1) = (x \ast i) \# x = (x \ast j) \# x = x \ast (j + 1),
\]

and thus, similarly,

\[
x \ast (i + 2) = x \ast (j + 2),
\]

and so on, up to

\[
x \ast (i + N) = x \ast (j + N),
\]

where \( i + N = n_x \). By periodicity after \( m_x \) of the \( x \)-row, we have

\[
x \ast n_x = x \ast (i + (j - i) + N) = x \ast (i + N + (j - i)) = x \ast (n_x + (j - i)).
\]
Thus we have, by periodicity after $m_x$,
\[ x \cdot m_x = x \cdot n_x = x \cdot (m_x + (j - i)). \]

But since $j - i < n_x - m_x$, this contradicts the definitions of $m_x$ and $n_x$. Thus we must have
\[ i \equiv j \pmod{(n_x - m_x)}. \]

To prove Property (3C) in the “if” direction, suppose
\[ i \equiv j \pmod{(n_x - m_x)}, \]
with $i, j > m_x$. It follows from the definitions of $m_x$ and $n_x$ that $x \cdot i = x \cdot j$.

To prove Property (3D), note that
\[ 1 \cdot (x \cdot y) = (1 \cdot x) \cdot y, \]
by associativity so
\[ 1 \cdot (x \cdot y) = 1 \cdot x \cdot y, \]
by Lemma 3B. We prove this property in two cases:

Case I: $xy < m_x$. Then $1 \cdot x \cdot y = xy < m_x$, by Property (2). Also, $x, y < m_x$ and
\[ x \cdot y = (1 \cdot x) \cdot y \text{ by (2)}, \]
\[ = 1 \cdot x \cdot y \text{ by the above}, \]
\[ = xy \text{ by (2)}. \]

Thus certainly $x \cdot y \equiv xy \mod (n_x - m_x)$.

Case II: $xy \geq m_x$. Then by Property (2), $1 \cdot x \cdot y \geq m_x$, so by the above, we have $1 \cdot (x \cdot y) \geq m_x$. Again by (2), $x \cdot y \geq m_x$. Thus we have $xy, x \cdot y \geq m_x$, and $1 \cdot xy = 1 \cdot (x \cdot y)$, so by Property (3C), $x \cdot y \equiv xy \mod (n - m)$, which concludes the proof of Property (3D).

To prove Property (4), suppose $x \cdot j = y \cdot i$ and $x \cdot j' = y \cdot i'$. Then we have:
\[ x \cdot (j + j') = (x \cdot j) \# (x \cdot j'), \text{ by Lemma 3A} \]
\[ = (y \cdot i) \# (y \cdot i'), \text{ by hypothesis} \]
\[ = y \cdot (i + i'), \text{ again by Lemma 3A}, \]
so Property (4) is proven.
To prove Property (5), suppose \( x \ast y < m \). Then by the first statement of Property (2), \( 1 \ast (x \ast y) < m \), so by associativity \( (1 \ast x) \ast y = 1 \ast (x \ast y) < m \). Thus by Lemma 3B, \( 1 \ast xy = (1 \ast x) \ast y < m \). Again by Lemma 3B, \( (1 \ast y) \ast x = 1 \ast xy < m \), so by associativity
\[
1 \ast (y \ast x) = (1 \ast y) \ast x < m.
\]

Finally, by the second statement of Property (2), we have \( y \ast x < m \), which completes the proof of Theorem 9. \( \Box \)

4. Sufficient Conditions

Theorem 9 above says that in order for a binary operation \( \ast \) to be the iteration of an associative arithmetic, it must satisfy certain properties. But are these properties also sufficient conditions? Do those properties even guarantee associativity of \( \ast \)? The answer to the second question is yes, as the last item in the next theorem states:

**Theorem 10.** Let \( \ast \) be a binary operation on \( \mathbb{Z}^+ \) which satisfies the properties of Theorem 9. Then:

(A) For all \( x, y, z \in \mathbb{Z}^+ \), we have \( (x \ast y) \ast z = x \ast yz \).

(B) For all \( x, y, i, j \in \mathbb{Z}^+ \) such that \( x \ast j = y \ast i \), we have \( j \geq m \) if and only if \( i \geq m \), and therefore \( j < m \) if and only if \( i < m \).

(C) For all \( x, y \in \mathbb{Z}^+ \), \( xy < m \) implies \( x \ast y < m \) and \( y \ast x < m \), and in that case \( x \ast y = y \ast x = xy \).

(D) For all \( x, y \in \mathbb{Z}^+ \), \( x \ast y < m \) implies \( y < m \).

(E) If \( x \geq m \), then for all \( i \), \( x \ast i \geq m \) and \( i \ast x \geq m \).

(F) For all \( x, y \in \mathbb{Z}^+ \), we have \( x \ast y < m \) if and only if \( xy < m \), and in that case \( x \ast y = y \ast x = xy \).

(G) \( \ast \) is associative.

**Proof.** To prove part (A), use induction on \( z \). By Property (1) of Theorem 9, the statement holds for \( z = 1 \). Now, suppose it holds for \( z = k \). That is, our inductive hypothesis is:
\[
(x \ast y) \ast k = x \ast ky.
\]
But by Property (1) of Theorem 9, we also have:

\[(x \ast y) \ast 1 = x \ast y.\]

Thus, by Property (4) of Theorem 9,

\[(x \ast y) \ast (k + 1) = x \ast (ky + y) = x \ast (k + 1)y,
\]

which is the statement for \(z = k + 1\), so our statement holds for all \(z\).

To prove part (B), suppose \(x \ast j = y \ast i\), and \(j \geq m_x\). Then, by definition of \(m_x\), there exists \(k > 0\) such that \(x \ast j = x \ast (j + k)\). Thus we have:

\[
y \ast (i + ki) = y \ast (k + 1)i \\
= (y \ast i) \ast (k + 1), \text{ by part (A)} \\
= (x \ast j) \ast (k + 1), \text{ by hypothesis} \\
= [x \ast (j + k)] \ast (k + 1), \text{ by hypothesis} \\
= x \ast (j + k)(k + 1), \text{ by (A)} \\
= x \ast (jk + j + k^2 + k) \\
= x \ast (j + (j + k + 1)k) \\
= x \ast j, \text{ by Property (3C) of Theorem 9, since } j \geq m_x \\
= y \ast i, \text{ by hypothesis.}
\]

Thus, by definition of \(m_y\), we have \(i \geq m_y\) and by symmetry, \(i \geq m_y\) implies \(j \geq m_x\).

To prove part (C), first note that if \(xy < m\), then \(x < m\) so \(x = 1 \ast x\), by Property (2) of Theorem 9. Thus

\[x \ast y = (1 \ast x) \ast y = 1 \ast xy,
\]

by part (A). But since \(xy < m\), we have \(1 \ast xy < m\), again by Property (2) of Theorem 9. Thus \(x \ast y = xy < m\). Symmetrically, \(y \ast x < m\), proving part (C).

To prove part (D), suppose \(x \ast y < m\). Then \(1 \ast (x \ast y) < m\), by Property (2) of Theorem 9. But also, since \(x \ast y < m\), we have \(x \ast y = 1 \ast (x \ast y)\). Thus by part (B), we have \(y < m\).

To prove part (E), suppose \(x \geq m\) and assume \(i \ast x < m\). Then by part (D), \(x < m\) so \(x < m\), by Property (3B) of Theorem 9. This contradicts
our hypothesis, and thus $i \ast x \geq m$. By Property (5) of Theorem 9, we must also have $x \ast i \geq m$.

To prove part (F), first note that the “if” part of (F) is (B). To prove the “only if” part, suppose $x \ast y < m$. Then, by Property (5) of Theorem 9, $y \ast x < m$. But by part (D) proven above, $x < m_y$, so by Property (3B) of Theorem 9, $x < m$, which gives us $x = 1 \ast x$. Therefore we have

\[
1 \ast xy = (1 \ast x) \ast y, \quad \text{by part (A)}
\]
\[
= x \ast y, \quad \text{since } x = 1 \ast x
\]
\[
< m.
\]

Finally, by Property (2) of Theorem 9, we get $xy < m$, which completes the proof of part (F).

To prove part (G), let $x, y, z$ be in $\mathbb{Z}^+$. By part (F), either $yz$ and $y \ast z$ are both less than $m$, or neither is less than $m$. We study these two cases separately.

Case I: Both are less than $m$. That is, $yz < m$, and $y \ast z < m$. Thus $y \ast z < m$. Therefore we have

\[
x \ast (y \ast z) = x \ast yz = (x \ast y) \ast z, \quad \text{by part (A)}.
\]

Case II: Neither is less than $m$.

Then both have to be greater than or equal to $m$. By Property (3D) of Theorem 9, we have $y \ast z \equiv yz \mod (n - m)$. Thus by Property (3C) of Theorem 9 and part (A) above, we have

\[
x \ast (y \ast z) = x \ast yz = (x \ast y) \ast z.
\]

So associativity holds in either case, and the proof of Theorem 10 is done. □

So we now know that the properties of Theorem 9 ensure associativity. However, what about the first question; namely, do those properties ensure an associative arithmetic? That is, does there then exist an associative $\#$ which is compatible with $\ast$? This so far seems not an easy question to answer, and
I have not yet answered it. However, in certain cases, when $\ast$ satisfies additional properties, we can get information about the existence of associative $\#$ compatible with $\ast$. Here is one such result, which was motivated by my “college freshman theorem” mentioned in Section 1.

**Theorem 11.** Let $\ast$ be a binary operation on $\mathbb{Z}^+$ which satisfies the properties of Theorem 9 with $m = 1$ and which has the additional property that for any $x$ in $\mathbb{Z}^+$, there exists a unique $a$ in $\mathbb{Z}^+$ such that $x$ is in the $a$-row and $a \equiv 1 \mod (n-1)$. Then:

1. The binary operation $\#$ defined on all $x, y$ in $\mathbb{Z}^+$ by:
   \[
   x \# y = a \ast (x + i), \quad \text{where } y = a \ast i \text{ with } a \equiv 1 \mod (n-1)
   \]
   is associative, compatible with $\ast$, and thus an associative arithmetic with iteration $\ast$.

2. This associative arithmetic is not commutative.

Now let me say a bit about where this theorem came from.

Recall that the college freshman formula (Equation 1) can be written as:

\[
x \# y = y \ast (z + 1), \quad \text{where } z \text{ satisfies } y \ast z = x.
\]

But such a $z$ doesn’t always exist, for the general possible iteration $\ast$ satisfying the properties of Theorem 9. However, one day while taking a break from a flea market in a great Mexican restaurant — so I sometimes think of the following as “the flea market formula”, even though as we’ll see it had to be modified, to get to Theorem 11, I thought, “well, how about, instead of using $z$ — or $x/y$ as in the case when $\ast$ is ordinary multiplication — we try $x$ times $[y\text{-inverse mod } (n - 1)]$?” If $n - 1$ is prime, such an inverse does exist, unless $y$ is a multiple of $n - 1$. So the “flea market formula” would be:

\[
x \# y = y \ast (x[y\text{-inverse mod } (n - 1)]).
\]

That formula works — when $y$-inverse mod $(n - 1)$ exists. That is, $\#$ does indeed turn out to be both associative and compatible with $\ast$ (again, when the inverse exists).

Okay, so how can we get around those pesky little “rare” multiplies of $n - 1$? After a few months I did come up with something, something that works...
under a particular condition. Who knows, sometimes, how a mathematician comes up with anything? One of my poems in *Crossing the Equal Sign* [3] begins: “After a while making a proof is like making a calculation.” A mathematician sometimes just knows what the next step of a proof might be — perhaps similarly to how, if you know the music of, say, Mozart, you sort of know what the next note might be (not as much with Beethoven, though...). At any rate, I thought, “What if we hypothesize, in addition to the properties of Theorem 9, that $y$ can be expressed in the form, $y = a \cdot i$ for some $i$ in $Z^+$ and some unique $a$ congruent to $1$ mod $(n - 1)$?” That leads, in that case, to a usable formula for any $x \# y$ (given, again, the iteration $\ast$). Then we can define:

$$x \# y = (a \cdot i) \ast (x[y\text{-inverse}] + 1)$$

$$= a \cdot i(x[y\text{-inverse}] + 1), \text{ by Theorem 10}$$

$$= a \ast (i(x[y\text{-inverse}] + i)).$$

But $ix[y\text{-inverse}]$ is congruent to $y$ mod $(n - 1)$, since $i$ is congruent to $y$ mod $(n - 1)$ and since $a$ is congruent to $1$ mod $(n - 1)$.

So we can set $x \# y = a \ast (x + i)$, where $y = a \ast i$ — as is done in Theorem 11. Note that this definition of $\#$ avoids mention of inverses.

That was the motivation; the proof is probably reminiscent of it.

**Proof.** To prove part (1), we first prove compatibility of $\#$ with $\ast$. For all $x, k \in Z^+$ we have:

$$(x \ast k) \# x = a \ast [(x \ast k) + i], \text{ where } x = a \ast i$$

$$= a \ast [kx + i], \text{ since } x \ast k \equiv kx \text{ mod } (n - 1) \text{ and } m = 1$$

$$= a \ast (ki + i), \text{ since } x \equiv i \text{ mod } (n - 1) \text{ and } m = 1$$

$$= a \ast i(k + 1) = (a \ast i) \ast (k + 1), \text{ by Theorem 10A}$$

$$= x \ast (k + 1), \text{ since } a \ast i = x,$$

so compatibility holds.

We next prove the associativity of $\#$. By definition of $\#$ we have, for all $x, y, z$ in $Z^+$:

$$(x \# y) \# z = [a \ast (x + i)] \# z, \text{ where } y = a \ast i \text{ and } a \equiv 1 \text{ mod } (n - 1)$$

$$= b \ast [(a \ast (x + i)] + j), \text{ where } z = b \ast j \text{ and } b \equiv 1 \text{ mod } (n - 1)$$
and
\[ x\#(y\#z) = x\#[b \ast (y + j)], \text{ where } z = b \ast j \text{ and } b \equiv 1 \mod (n - 1) \]
\[ = b \ast [x + (y + j)], \text{ where } y = a \ast i \text{ and } a \equiv 1 \mod (n - 1), \]
where we are using the same \(a, b, i, j\) as above. Note that these latter expressions both begin with “\(b \ast\)”. Let’s now compare their “endings”.
\[ a \ast [(x + i) + j] \equiv [a(x + i) + aj] \mod (n - 1) \text{ by Property 3D of Theorem 9} \]
\[ = (ax + ai + aj) \mod (n - 1) \]
\[ \equiv [x + (a \ast i) + j] \mod (n - 1) \text{ since } a \equiv 1 \mod (n - 1) \]
\[ \text{and } ai \equiv (a \ast i) \mod (n - 1) \]
\[ = (x + y + j) \mod (n - 1) \text{ since } y = a \ast i \]

Thus, by Property (3C) of Theorem 9, we have
\[ b \ast (x + y + j) = b \ast \{[a \ast (x + i)] + j\} \]
since \(m = 1\), so \(x\#(y\#z) = (x\#y)\#z\), and associativity holds.

To prove part (2), let \(a \neq a'\), but \(a \equiv a' \equiv 1 \mod (n - 1)\). (For example, \(a = 1, a' = n\).) Then \(a \# a'\), by its definition, is in the \(a'\)-row, whereas \(a' \# a\) is in the \(a\)-row. Now assume \(a \# a' = a' \# a\). Then by the uniqueness in the theorem hypothesis, \(a = a'\), which contradicts our assumption, thus proving (2), completing the proof of the theorem. \(\square\)

5. Two Theorems towards Examples of Non-Ordinary Associative Arithmetics

The next theorem inspires and motivates a further theorem that will help provide more examples of non-ordinary associative arithmetics. It gives information, when \(m = 1\) and \(n - 1\) is prime, about the structure of the rows of binary operations which satisfy the properties of Theorem 9.

**Theorem 12.** Let \(\ast\) be a binary operation on \(\mathbb{Z}^+\) which satisfies the properties of Theorem 9, with \(m = 1\) and \(n - 1\) prime. Then the rows of \(\ast\) must satisfy:

1. All rows have period either \(n - 1\) or 1. The rows with period 1 are constant (as sequences) and, unless \(n = 2\), that constant is congruent to 0 \(\mod (n - 1)\).
For all \(a \equiv 1 \mod (n - 1)\) and \(i \in \mathbb{Z}^+\), we have \(a \ast i \equiv i \mod (n - 1)\).

For all \(x \equiv 0 \mod (n - 1)\), all \(x\)-row entries are congruent to 0 mod \((n - 1)\).

Suppose the \(x\)-row and the \(x'\)-row have distinct ranges. Then the two row ranges are “almost disjoint” in the sense that any common element must be \(x \ast (n - 1) = x' \ast (n - 1)\).

Every \(x\) not congruent to 0 mod \(n - 1\) is in the range of an \(a\)-row for some unique \(a\) that is congruent to 1 mod \((n - 1)\).

Proof: By Property (3B) of Theorem 9, \(n_x - 1\) divides \(n - 1\), so since \(n - 1\) is prime, the first assertion of part (1) follows. To prove the second half of (1), let \(x\) by such that the \(x\)-row is constant and assume that \(x\) is not congruent to 0 mod \((n - 1)\). Then, for example, \(x \ast 1 = x \ast 2\). Then \(x = x \ast 2\), so by Property (3D) of Theorem 9, we have \(x \equiv 2x \mod (n - 1)\), and therefore, since \(x\) does not equal 0 mod \((n - 1)\), 1 \(\equiv 2 \mod (n - 1)\). Therefore \(n\) must equal 2, contrary to hypothesis.

To prove part (2), let \(a\) be given such that \(a \equiv 1 \mod (n - 1)\). Then, by Property (3D) of Theorem 9, \(a \ast i \equiv ai \mod (n - 1)\), and thus by our assumption that \(a \equiv 1 \mod (n - 1)\), \(a \ast i \equiv i \mod (n - 1)\).

Now, let \(x\) be given such that \(x \equiv 0 \mod (n - 1)\). Then, again by Property (3D) of Theorem 9, for all \(i\) we have \(x \ast i \equiv xi \mod (n - 1) \equiv 0 \mod (n - 1)\), which follows from our assumption that \(x \equiv 0 \mod (n - 1)\).

To prove part (3), assume we have \(x \ast i = x' \ast j\), with \(i\) not congruent to 0 mod \((n - 1)\). Thus, since \(n - 1\) is prime, the inverse \(i^{-1}\) exists mod \((n - 1)\), so we have \((x \ast i) \ast i^{-1} = (x' \ast j) \ast i^{-1}\). By Theorem 10A, we then have \(x \ast i \ast i^{-1} = x' \ast ji^{-1}\) and thus \(x = x \ast 1 = x \ast i \ast i^{-1}\), since \(i \ast i^{-1} \equiv 1 \mod (n - 1)\) and since \(m = 1\), so \(i \ast i^{-1} \geq m\) and \(1 \geq m\). Thus we have \(x = x' \ast ji^{-1}\).

So \(x\) is in the range of the \(x'\)-row, and thus the entire range of the \(x\)-row is in the range of the \(x'\)-row. Symmetrically, the entire range of the \(x'\)-row is in the range of the \(x\)-row. So the two row-ranges are not distinct, which contradicts the hypothesis. So \(i \equiv 0 \mod (n - 1)\) and, symmetrically, \(j \equiv 0 \mod (n - 1)\). Thus \(x \ast i = x \ast (n - 1)\) and \(x' \ast j = x' \ast (n - 1)\).

\(^3\) Rows are sequences, not sets, so we need to use the term “range”.
To prove part (4), let \( x \in \mathbb{Z}^+ \) not be congruent to 0 mod \((n - 1)\). Then, since \( n - 1 \) is prime, we have an inverse, \( x^{-1} \), of \( x \). Taking \( a = x \ast x^{-1} \) proves the existence part of (4). As for the uniqueness of \( a \), non-uniqueness would contradict part (3). This completes the proof of Theorem 12.

This last conclusion says that, in the case when \( m = 1 \) and \( n - 1 \) is prime, if any \( z \) congruent to 0 mod \( p \) is in some unique \( a \)-row, with \( a \equiv 1 \) mod \((n - 1)\), then by Theorem 11, \( \ast \) is the iteration of an associative arithmetic. A quick example (which will be explained less “quickly” as our first example in Section 6) is given by setting \( x \ast y = x + y - 1 \), for \( y \) between 1 and 4, and for larger \( y \), extending the \( x \)-row periodically.

The next theorem is motivated by the following: A binary operation which satisfies the properties of Theorem 9 is determined by its “row segments”, meaning the first \( n - 1 \) entries in each of its rows. This is because the subsequent entries in each row are determined by “eventual periodicity” — periodicity beginning with the \( m \)th entry. Thus, in applying Theorem 11 to give examples of associative arithmetics, as we will in the next section after proving the following theorem, it is convenient to think in terms of their “row segments”. In fact, we need not give all the row segments, since some rows are contained in others. Our just-proven Theorem 12 says things about the structure of the rows for any \( \ast \) satisfying the properties of Theorem 9 with \( m = 1 \) and \( n - 1 \) prime. Here we start with “row segments” or rather, as we’ll see, \( p \)-tuples and end up with a binary operation satisfying the properties of Theorem 9 (\( m \) will be 1 and \( p \) will be \( n - 1 \) for this operation), and which, in each of the examples following the next theorem, is the iteration of an associative arithmetic.

A quick remark might be helpful here. A variation on the division algorithm is necessary, since 0 is not in \( \mathbb{Z}^+ \) and therefore not “in the running”. Instead, we note that, given \( M, N \) in \( \mathbb{Z}^+ \), \( N \) can always be uniquely expressed as \( N = KM + r \), where the “remainder” \( r \) is one of the \( M \) integers 1, 2, \ldots, \( M \) (rather than, as in the division algorithm, 0 through \( M - 1 \)). (The proof of this uses the “usual” division algorithm.)

In the following, whenever \( z \) is the beginning entry of an ordered \( p \)-tuple in \( \mathbb{Z}^+ \), \((z, i)\) will denote the \( i \)th entry in that \( p \)-tuple. In particular \((z, 1) = z\).

**Theorem 13.** Let \( p \) be in \( \mathbb{Z}^+ \), and let \( S \) be a set of ordered \( p \)-tuples in \( \mathbb{Z}^+ \), such that \( S \) satisfies the following conditions:
(1) Any \( p \)-tuple in \( S \) either is constant or its range consists of precisely \( p \) distinct entries, with first entry equal to \( 1 \mod p \). The constant in any constant \( p \)-tuple is congruent to \( 0 \mod p \), and conversely, any \( x \)-row where \( x \) is congruent to \( 0 \mod p \) is constant.

(2) For all \( a \) congruent to \( 1 \mod p \), there exists a unique \( p \)-tuple in \( S \) beginning with \( a \), and for all \( i = 1, 2, \cdots, p \), \( (a, i) \equiv ai \mod p \).

For all \( z \) congruent to \( 0 \mod p \) such that \( z \) is the beginning entry of some \( p \)-tuple in \( S \), we have \( (z, i) \equiv 0 \mod p \), for all \( i = 1, 2, \cdots, p \).

(3) The ranges of two distinct \( p \)-tuples in \( S \), beginning with \( z \) and \( z' \) respectively, are “almost disjoint” in the sense that they intersect, if at all, only at \( (z, p) = (z', p) \).

(4) For all \( x \) there exists a \( p \)-tuple in \( S \) of which \( x \) is an entry. If \( x \) is not congruent to \( 0 \mod p \), then that \( p \)-tuple is unique, and its beginning entry \( z \) is congruent to \( 1 \mod p \).

Then \( S \) induces a binary operation \( \ast \) (with the \( p \)-tuples serving as row-segments of \( \ast \)) which satisfies the properties in Theorem 9 with \( m = 1 \) and \( n = p-1 \). This \( \ast \) is given, for all \( x \) and \( y \) in \( \mathbb{Z}^+ \), by the following process:

By Condition (4), there exists a \( p \)-tuple with \( x \) as one its entries. Let \( z \) be the beginning entry in that \( p \)-tuple.\(^4\) Define \( x \ast y = (z, r) \), where \( x = (z, i) \), and \( i = 1, 2, \cdots, p \), and \( r \equiv iy \mod p, r = 1, 2, \cdots, p \) (according to the remark appearing just before this theorem).

Proof: We first show that \( \ast \) is well-defined. Suppose we have \( x = (z, i) = (z', j) \). By Condition (3), we have \( i = j = p \). Thus \( x = (z, p) = (z', p) \), for two possibly distinct beginning entries \( z \neq z' \). We now use the given definition of \( \ast \) to find \( x \ast y \), according to each expression for \( x \), and to show that the two give the same value.

Since \( x = (z, p) \), we have \( x \ast y = (z, r) \), where \( r \equiv py \mod p, r = 1, 2, \cdots, p \).

Thus \( r = p \) so \( x \ast y = (z, p) \). Similarly, using \( x = (z', p) \), we have \( x \ast y = (z', p) \).

---

\(^4\) This \( p \)-tuple is not always unique, but as we show in the beginning of the proof of Theorem 13, the definition we give here for \( x \ast y \) is independent of which \( p \)-tuple is used.
But \((z', p) = (z, p)\) so \(x \ast y = (z, p)\), same as above. Thus the definition of \(x \ast y\) is independent of how we express \(x\), and \(\ast\) is indeed well-defined.

We now show that \(\ast\) satisfies the properties of Theorem 9.

To prove Property (1) of Theorem 9, we have to show that \(1 \ast 1 = 1 \ast (p+1)\), and that \(p+1\) is the smallest \(j \neq 1\) such that \(1 \ast 1 = 1 \ast j\). We will thus show that \(m = 1\) and \(n = p+1\).

First, note that \(1 = (1, 1)\), so when we take \(1 = (z, i)\) as in the definition of \(\ast\), we have \(z = i = 1\). Thus \(1 \ast 1 = (1, r)\), where \(r \equiv 1 \mod p, r = 1, 2, \ldots, p\). Thus \(r = 1\), so \(1 \ast 1 = (1, 1) = 1\).

And \(1 \ast (p+1) = (1, r')\), where \(r' \equiv p + 1 \mod p, r' = 1, 2, \ldots, p\). Thus \(r' = 1\) and therefore \(1 \ast (p+1) = (1, 1) = 1 \ast 1\), which proves the first part of Property (1).

Next, suppose that \(1 \ast 1 = 1 \ast j, j < p+1\). We’ll show \(j = 1\).

As above, we have \(1 \ast 1 = 1\). Now, \(1 \ast j = (1, r)\), where \(j\) is congruent to \(r, r = 1, 2, \ldots, p\). We have two cases to consider:

Case I: \(j = p\). Then \(r = p\), so \(1 \ast j = (1, p)\). Thus \((1, p) \equiv 1 \ast 1 = 1\). But by Condition (2) that we assumed in our theorem, \((1, p) \equiv p \mod p\), so \(1\) is congruent to \(p \mod p\). But \(1 \equiv (p+1) \mod p\), so Case I can’t happen.

Case II: \(j < p\). Again, \(1 \ast 1 = 1\) so \(1 \ast j = (1, r)\), where \(r \equiv j \mod p, r = 1, 2, \ldots, p\). Thus since \(j < p, r = j < p\). Thus \(1 = (1, r) = (1, j)\), which is congruent to \(j \mod p\), by Condition (2) of Theorem 13. Since \(i < p\), we must have \(j = 1\), which proves Property (1) of Theorem 9.

As for Property (2) of Theorem 9, we have to prove that for all \(j < m, 1 \ast j = j\). But this is vacuously true, since \(m = 1\).

To prove Property (3A) of Theorem 9, we note that for all \(x\), we have \(x \ast 1 = (z, r)\), where \(x = (z, i)\) and \(r \equiv i \mod p, r = 1, 2, \ldots, p\). Thus \(r = i\) and \(x \ast 1 = (z, i) = x\).

To prove Property (3B) of Theorem 9, we need to show that for all \(x\) (not only \(x = 1\), as in property (1)), we have \(x \ast 1 = x \ast (p+1)\). From Property (3A) directly above, we have \(x \ast 1 = x\). Now, \(x \ast (p+1) = (z, r)\), where \(x = (z, i), i = 1, 2, \ldots, p,\) and \(r \equiv i(p+1) \mod p, r = 1, 2, \ldots, p\). That is, \(r \equiv i \mod p, so r = i\) and \(x \ast (p+1) = (z, i) = x\). Therefore \(x \ast 1 = x \ast (p+1)\).
To prove Property (3C), note first that if $i'$ is congruent to $j'$ mod $p$, then $x \ast i' = x \ast j'$. (I'm using $i'$ and $j'$ rather than $i$ and $j$, in order to avoid confusion of notation.) Now, suppose we have $x \ast i' = x \ast j'$. By the definition in the theorem:

\[
x \ast i' = (z, r), \text{ where } x = (z, i), i = 1, 2, \ldots \text{ or } p \text{ and } r \equiv i' \mod p
\]

\[
x \ast j' = (z, r'), \text{ where } x = (z, i), i = 1, 2, \ldots \text{ or } p \text{ and } r' \equiv j' \mod p.
\]

Thus we have: $x \ast i' = x \ast j'$ if and only if $r$ and $r'$ are congruent mod $p$, which happens if and only if $i'I$ and $j'I$ are congruent mod $p$. We have two cases to consider.

Case I: $I$ is not congruent to 0 mod $p$. Then $i' \equiv j'$ mod $p$.

Case II: $i \equiv 0 \mod p$. Then $x = (z, p)$. That is, $x \equiv 0 \mod p$. Therefore, by the last statement in Property (1) of the theorem, the $x$-row is constant. Thus $m_x = 1$, and so $n_x - m_x = 1$, and therefore clearly $I' \equiv j'$ mod $(n_x - m_x)$.

This completes the proof of Property (3C).

To prove Property (3D) of Theorem 9, we have to show that, for all $x, y$ in $\mathbb{Z}^+$, we have $x \ast y \equiv xy \mod p$. By definition of $\ast$, $x \ast y = (z, r)$, where $x = (z, i)$, $r$ is congruent to $iy$ mod $p$, with $i, r = 1, 2, \ldots, p$. Thus we have:

\[
x \ast y \equiv zr \mod p \text{ by Condition (2)}
\]

\[
\equiv z(iy) \mod p \text{ since } r \equiv iy \mod p
\]

\[
\equiv (zi)y \mod p
\]

\[
\equiv (z, i) \mod p \text{ since } (z, i) \equiv zi \mod p \text{ by Condition (2)}
\]

\[
\equiv xy \mod p \text{ since } x = (z, i).
\]

Now, to prove Property (4) of Theorem 9, suppose $x \ast j = y \ast i$ and $x \ast j' = y \ast i'$. We have to show that $x \ast (j + j') = y \ast (i + i')$.

We have $x = (z, k)$ and $y = (w, l)$ by Condition (4), where $x$ and $w$ are beginning entries and $k$ and $l$ are between 1 and $p$, inclusive. Thus $x \ast j = (z, r)$, where $r$ is congruent to $kj$ mod $p$ and $y \ast j = (w, s)$, where $x$ is congruent to $li$ mod $p$.

Since $x \ast j = y \ast i$, we have $w = z$ and $s = r$. Similarly, $x \ast j' = (z, r')$, where $r'$ is congruent to $kj'$ mod $p$ and $y \ast j' = (w, s')$, where $s'$ is congruent to $li'$ mod $p$, and since $x \ast j' = y \ast i'$, we have $s' = r'$ (and, as before, $w = z$).
Also, \( x \ast (j + j') = (z, r) \), where \( r \) is congruent to \( k(j + j') \mod p \), where \( r \) is between 1 and \( p \), and \( y \ast (i + i') = (w, s) \), where \( s \) is congruent to \( l(i + i') \mod p \), where \( s \) is between 1 and \( p \).

To show that these “last two” are equal, we need to show that \( w = z \) and \( s = r \). But we’ve already shown that \( w = z \), so we need only show \( s = r \).

\( s \) is congruent to \( l(i + i') \mod p \), and \( l(i + i') \) equals \( li + li' \), which is congruent to \( (s + s') \mod p \). Similarly, \( r \) is congruent mod \( p \) to \( s + s' \). But we’ve shown that \( s = r \) and \( s' = r' \). Therefore \( s + s' \) is certainly congruent mod \( p \) to \( r + r' \), so \( s \) is congruent mod \( p \) to \( r \). Finally, since \( r \) and \( s \) are both between 1 and \( p \), we have \( s = r \), which completes the proof of Property (4) of Theorem 9.

Property (5) of Theorem 9 is vacuously true, since \( m = 1 \) so \( x \ast y < m \) never happens. This completes the proof of Theorem 13.

6. Examples of Other Associative Arithmetics

When all the \( p \)-tuples in Theorem 13 have beginning entries congruent to 1 mod \( p \), the induced \( \ast \) satisfies the hypothesis of Theorem 11, so we can now give examples of non-ordinary associative arithmetics found by application of Theorem 11 and our just-proven Theorem 13. What follows is a typical example.

**Example 14.** Let, for all \( x, y \in \mathbb{Z}^+ \), \( x \ast y = x + y - 1 \). This is the example mentioned after the proof of Theorem 12. In “row-segment language”, according to Theorem 13, \( \ast \) is induced by letting \( p = 5 \) and the set \( S \) of 5-tuples as appears below.

\[
\{(1, 2, 3, 4, 5), (6, 7, 8, 9, 10), (11, 12, 13, 14, 15), \cdots \}
\]

Or if we write the 5-tuples as rows of a table:

\[
\begin{array}{ccccc}
1 & 2 & 3 & 4 & 5 \\
6 & 7 & 8 & 9 & 10 \\
11 & 12 & 13 & 14 & 15 \\
\vdots
\end{array}
\]

\( S \) satisfies the conditions in Theorem 13 (all the 5-tuples in \( S \) have beginning entries congruent to 1 mod \( p \)), so \( S \) induces a binary operation \( \ast \) on \( \mathbb{Z}^+ \) that
satisfies the properties of Theorem 11. In particular, for all $x$ there is an $a$ which is congruent to 1 mod 5 such that $x$ is in the 5-tuple beginning with $a$, so $\ast$ satisfies the hypotheses of Theorem 11. So there is a $\#$, given by Theorem 11, such that $\#$ is an associative arithmetic with iteration $\ast$. Let us do a couple of calculations for $\#$:

$9 = 6 \ast 4$ so $3 \# 9 = 6 \ast (3 + 4) = 6 \ast 7 = 6 \ast 2 = 7$.

$3 = 1 \ast 3$ so $9 \# 3 = 1 \ast (9 + 3) = 1 \ast 12 = 1 \ast 2 = 2$.

We see that $3 \# 9 \neq 9 \# 3$, which is not surprising since Theorem 11 says that $\#$ is not commutative. In fact, this $\#$ is, in some sense, the least commutative that an associative arithmetic can be. For in every associative arithmetic, two numbers in the same row commute with respect to $\#$, and for this $\#$, any two numbers not in the same row do not commute.

**Remark 15.** On the other hand, let the set $S$ of 5-tuples be as appears directly below.

```
1  2  3  4  5
6  7  8  9  5
11 12 13 14 10
16 17 18 19 15
...
```

$S$ differs from the previous $S$ in that 5 appears in both of the first two rows. $S$ does satisfy the conditions of Theorem 13 and thus induces a binary operation $\ast$ on $\mathbb{Z}^+$ which satisfies the properties of Theorem 9. However, since $5 = 1 \ast 5 = 6 \ast 5$, there are two distinct $a$’s which are congruent to 1 mod 5 whose row-ranges both contain 5, so an associative arithmetic $\#$ compatible with $\ast$ cannot be defined using Theorem 11.

Note also that there might, however, be another way to define an associative arithmetic $\#$ that is compatible with $\ast$. If not, that would be an example of an operation satisfying the properties of Theorem 9 but which is not the iteration of any associative arithmetic. So that would show that the Theorem 9 properties are not sufficient to give us all the iterations of associative arithmetics.

Let us look at two more examples.
Example 16. Let $S$ be as appears below:

\[
\begin{array}{cccc}
1 & 2 & 3 & 4 & 5 \\
6 & 7 & 8 & 9 & 15 \\
11 & 12 & 13 & 14 & 20 \\
16 & 17 & 18 & 19 & 25 \\
\vdots \\
10 & 10 & 10 & 10 & 10
\end{array}
\]

What happens here is that 10 is “missing” from the rows with beginning entries congruent to 1 mod 5, but 10 is the only such number. This $S$ satisfies the conditions of Theorem 13, so it induces a $*$ that satisfies the properties of Theorem 9. However, because of the missing 10, $*$ does not satisfy the hypotheses of Theorem 11.

There still does exist an associative binary operation $\#$ on $\mathbb{Z}^+$ compatible with $*$. $\#$ can be defined as follows:

For all $x, y$ in $\mathbb{Z}^+$ such that $y \neq 10$, we define $x\#y$ as given in Theorem 11. Then we set $x\#10 = x$. It is not hard to check that $\#$ is indeed an associative arithmetic compatible with $*$.

Example 17. Let the set $S$ of 5-tuples be as appears below:

\[
\begin{array}{cccc}
1 & 2 & 3 & 4 & 5 \\
6 & 7 & 8 & 9 & 15 \\
11 & 12 & 13 & 14 & 25 \\
\vdots \\
10 & 20 & 30 & 40 & 50 \\
60 & 70 & 80 & 90 & 150 \\
110 & 120 & 130 & 140 & 250 \\
\vdots \\
100 & 200 & 300 & 400 & 500 \\
600 & 700 & 800 & 900 & 1500 \\
1100 & 1200 & 1300 & 1400 & 2500 \\
\vdots 
\end{array}
\]

It helps to further describe $S$. $S$ is divided into an infinite number of “levels”. The first level omits all multiples of 10. The second level is, entry for entry,
10 times the first level, and consists of all multiples of 10 which are not multiples of 100. The third is 100 times the first and consists of all multiples of 100 which are not multiples of 1000. And so on.

This $S$ satisfies the conditions of Theorem 13, but the induced $\ast$ does not satisfy the hypotheses of Theorem 11 (not all positive integers are entries in 5-tuples of $S$ beginning with something congruent to 1 mod 5). There is, however, at least one associative $\#$ compatible with $\ast$, which can be defined as follows:

For $x, y$ in the first level, we define $x \# y$ as given in Theorem 11. For $x, y$ both in any other level, say the $K$th, we have $k, l$ such that $x = 10h$ and $y = 10l$, so we can define $x \# y = 10(h \# l)$, where $\#$ is as given in Theorem 11. For $x$ and $y$ in different levels, set $x \# y$ equal to whichever of $x$ and $y$ is within the lower level.

Note that all three examples we have here can be generalized to any prime $p$, not only 5.

7. Further Explorations

I am far from having reached the termination of this “private world” of mine. We still have the questions, how can non-ordinary associative arithmetics be characterized? and are there non-ordinary associative arithmetics other than those arising from Theorems 11 and 13? Below are some partial results:

(1) Here is another class of examples of non-ordinary associative arithmetics. This class shows that, for any $N > M > 1$, there exist associative arithmetics with $m = M$ and $n = N$. So let $N > M > 1$. First, define the 1-row, in any way at all, as long as the following properties hold:

A) For $y < M$, $1 \ast y = y$;
B) For all $y$, $1 \ast y \equiv y \mod (N - M)$;
C) The 1-row is periodic with period $N - M$, starting with $y = M$.

Then define the $x$-rows by:

$$
\begin{cases}
  x \ast 1 = x & \text{for all } x, \\
  x \ast y = 1 \ast xy & \text{for all } x \text{ and for all } y \neq 1 \\
  x \# y = 1 \ast (x + y) & \text{for all } x \text{ and } y.
\end{cases}
$$
Theorem 11 provides two examples of associative arithmetics compatible with binary operations satisfying certain conditions. I have asked whether there are other examples which are in some sense “between” between these two examples. In fact, there are an uncountably infinite such examples, one for every quasi-order on $\mathbb{Z}^+$. Each total order gives an associative arithmetic, which is also commutative while the non-total orders necessarily give associative arithmetics which are not commutative. The question still arises: are there yet other associative arithmetics compatible with such a given binary operation $*$ on $\mathbb{Z}^+$? In particular, is it necessarily true that arithmetics $\#$ compatible with $*$ must satisfy $x\#y \equiv x + y \mod (n - 1)$ for all $x, y$ in $\mathbb{Z}^+$?

(3) Speaking of commutativity, here is a class of examples of non-ordinary commutative arithmetics — that is, non-ordinary arithmetics which are commutative and whose iterations are also commutative. For any $k \geq -1$ set:

$$x\#y = x + y + k \min(x, y) - k \text{ and } x * y = (k + 1)xy - k(x + y) + k.$$  

$k = 0$ gives ordinary arithmetic. $k = -1$ gives $x\#y = \max(x, y) + 1$, $x * y = x + y - 1$.

This brings us to another question: Are there other non-ordinary commutative arithmetics? Can we characterize commutative arithmetics? Commutativity seems to be a trickier animal than associativity. There doesn’t seem to be much you can do with it (unless you also combine it with associativity); there are not many ways you can move the $x$’s and $y$’s around. Two quantities that commute are sort of locked inside that pair of parentheses.

Finally, I should clarify something: When I say “my own private world”, I don’t mean I want it to be exclusively mine. Certainly not forever. I’m happy to share it, and I have shared it with folks to some extent. Private communication has been a good start (in particular with Rosinger, but also with a few math colleagues, in a presentation to a cool Math Club in Madison WI, and a sprinkling in some of my reviews of math books). I said earlier that being in this private world is like being the first to know some wonderful secret. But it’s only the first that I’d want to be; I don’t need to be alone in it forever. Others are welcome to come join me — especially if they have ideas that I haven’t had towards the answer(s) to any of the above questions!
A. Limericks About the Math in This Article

In an earlier issue of JHM appeared several pages of my “math-teaching limericks” (on topics from Pre-Calc to Category Theory) [5]. In the introduction to that poetry folder, I wrote that I was thinking it might be fun to write limericks about my own math research. Well, now I’ve done that, and here they are:

ASSOC ARITH LIMERICKS

(the associative property: \((ab)c = a(bc)\)

Which goes first, \(b\) with \(a\) or with \(c\)?
If both choices always agree then, sweet as glucose it’s all assoc.
So jump up and shout out Yippee.
(the commutative property: $ab = ba$)
If ab is always ba
then we’ve hit it lucky today.
It’s all commut.
so don’t be mute
but jump up and shout out Hurray.

(some terminology)
“Operation”’s too long a word.
Fitting it in is absurd.
So I’ll just write “op”
on my desktop.
That’s what I’ve always preferred.

(reality check)
As these poems you so carefully edit
keep one thing in mind, to my credit:
I know that line one
is a bit overspun.
I tried not to be so swell-headed.

(what we’re dealing with)
Binary ops on $\mathbb{Z}$-plus
are our motif today, and thus
we’ll do no transactions
with pi, e, or fractions
and that could be nice for us.

(iterations)
Giv’n an op, we needn’t delete it.
In fact, we can dare to repeat it
to our hearts’ desire
through muck and mire
as many times as are needed.

( iterations #2)
Write down x y times, so serene
then put y-less-one ops in between.
Oh, aren’t we literate!
We’ve got that ol’ iterate.
Yep, that’s what iterates mean.
(recursive definition of iteration)
x op 1 is x – there! That's done.
But the fun has just begun.
x op y, what comes next?
Throw in one more op x
to get x op (y + 1).

(definition of an arithmetic)
Here's an easy one for us.
It's a binary op on Z+.
But don't bask in glory.
There's more to the story
much more to explore and discuss.

(terminology)
Arithmetic's quick to define
but not to fit into a line.
So I'll be forthwith
and just say "arith"
and that will be perfectly fine.

(more . . .)
All over the state and nation
each op has an iteration.
So ariths entail
to our travail
two ops in combination.

(and more . . .)
Let's say "sharp" for the very-first op.
And "star" for the second to pop.
One syllable's lighter
on this typewriter
or on anybody's laptop.

(definition of ordinary (associative) arithmetics)
This one's easy, just simple addition.
(Aren't you glad it's not long division?)
You know it well.
In it you excel.
You needn't be a mathematician.
(reality check)
That last line’s a little too long
so it comes off a little too strong.
It’s the only way
that I could say
what I meant, and at least it’s not wrong.

(definition of a non-ordinary associative arithmetic)
If an op and its iteration
are both assoc, such elation!
We’ll jump up and cheer, for
that’s what we’re here for.
But star can’t be multiplication.

In order to be convivial
let’s mention a few that are trivial.
Just-plain $x$, to begin
and max and min.
Just-plain $y$ would make for quadrivial.

That first one is kind of a beaut
‘cause it shows the op needn’t commute.
And they all, on a par
have the same cool star.
Stand up and shout root-a-toot-toot.

(lemma 3)
There are a few subtle relations
‘tween ops and their iterations.
And the laws of this lemma
with nary a tremor
have ordinary arith as motivation.

(reality check)
Uh oh, I’ve done it again.
Took too long to get to the end.
I did it, I did it.
But at least I admit it.
It happens now and then.
There’s a certain healthy condition
putting us in the sorry position
of making that op
do a belly flop
into simple boring addition.

If its iterate has the entity
1, as its left identity,
then we must report
that our op must resort
to Lem’ 4 in all its serenity.

So now we will dare to dictate:
If sharp’s assoc and its iterate
is commut, then that op
does that ol’ belly flop
and suffers the same sad fate.

Oh no, now the second line
is too long for its britches, a sign
that abbreviations
can still try our patience
no matter how genuine.

If the op’s an assoc arith
then three statements are equiv:
So check just one
and all’s said and done.
You won’t have to plead the Fifth.

One: sharp is ordinary.
Two: star’s 1-1 in the second var’y.
Three: all 1 star x
always are x
and not just temporary.
(reality check)
I seem to have second-line-itis.
Or maybe it’s just bursitis.
I apologize
for that line’s size.
It swelled maybe due to arthritis.

(definition 7)
This definition so gauche
about stars in arith’s assoc
goes: for every \( x \)
that sits on our desks
there’s an \( x \)-row that we will soon post.

(definition 7, cont.)
That \( x \)-row’s a sequence, a link
to conclusions that put us in sync
and that sequence so spry
of all \( x \) star \( i \)
will not be as long as we think.

(theorem 9)
All hail to Theorem 9!
I just love this theorem of mine.
It gives us a hook
as to how these guys look
a sort of intelligent design.

(theorem 9, cont.)
Let’s first look at ordinary
arith, how the \( x \)-rows are very
familiar; they’re merely
multiples, clearly
of \( x \), nothing terribly scary.

(theorem 9: about non-ordinary associative arithmetics)
Each \( x \)-row’s, I’m daring to say,
periodic, though not right away.
So to my delight
the rows are finite
thus easy for us to display.
(reality check)
I’m hoping you didn’t detect
that line two has a slight defect.
But four-syllables
is quite a mouthful.
Still, they’re needed, to be correct.

(theorem 9, cont.)
The eventual period \( p \)
is largest when \( x \) haps to be
the number 1.
And when all’s said and done
you’ll have no choice but to agree.

(theorem 9, cont.)
My fav’rite, in which I am fluent
is: \( x \) star \( y \)’s mod \( p \) congruent
to \( xy \), our own
product well known.
Yes, the ordinary’s kind of pursuant.

(reality check)
Darn, again I’ve committed the crime
of taking up ‘way too much time
in the very last line
but I’m not cryin’
‘cause at least I managed to rhyme.

We will soon need some further notation
for our possible iteration
and I’ll say this explicitly:
Re: periodicity
let \( m \) be the embarkation.

(reality check)
I know “embarkation”’s a word
that maybe you’ve never heard.
But it’s in RhymeZone
so please don’t groan
and I needed it for the third.
(Theorem 9, cont.)
Yep, repeating begins at \( m \)
but before \( m \) is not quite mayhem.
For Theorem 9(2)
says there’s some to-do
in the 1-row, a short apophthegm.

(Renity check)
Oh, I know that last word’s a bit tense.
But RhymeZone confirms it makes sense.
It’s “a short pithy in-
“-structive saying”, akin
to a theorem – which soon will commence.

(Theorem 9(2))
Yes, for \( i \)’s strictly less than \( m \)
here’s an interesting thing about them:
1 star \( i \) can be found
without making much sound.
It’s just little old \( i \), what a gem.

(The big question)
I fear we must now intersperse:
is there perhaps a converse?
All that Theorem 9 stuff –
is it enough?
But the question’s too long for this verse.

(Terminology)
Property’s too long a word.
‘Twould come out a little bit slurred.
So let’s just say prop.
It rhymes with op.
Then we can proceed undeterred.

(The big question, #2)
Are the Theorem 9 props enough
to conclude, on or off the cuff
that our star so vivid
has sharp to go with it?
Well, that seems a little bit tough.
(theorem 10)
So now let’s get into the mood
to seek out what we can conclude
from Theorem 9 props.
Yes, let’s test our chops
and show off our aptitude.

(theorem 10 #2)
I don’t mean to sic you a sermon
but we really do need to determine
(we can’t take this lightly):
Is star so sprightly
assoc? yes, that needs some confirm’in’.

(theorem 10A)
This theorem has many a part.
10A gives a decent jumpstart.
That part is like (B)
of Lemma 3.
It’s a regular work of art.

(theorem 10B)
Back to m, which starts periodicity.
The ippidomy of simplicity.
It’s in the next five
of the props we derive.
So get used to its multiplicity.

(theorem 10B, #2)
If i and j satisfy
x star j equals y star i.
then if one of them
is less than m
the other will have to comply.

(theorem 10C)
Star is not multiplication.
But there seems to be some relation.
x – y, star y— either
are both or neither
less than m, by my estimation.
(reality check)
That last line sure takes us by storm
since it’s longer than the norm.
But to be correct
I had to respect
content rather than form.

(theorem 10C, cont.)
“Where one goeth, goeth the other,”
both either norther or souther.
They would be a-fixin’
to cross Mason Dixon
but that’s too much of a bother.

(theorem 10D)
Here’s something that’s just a tad shorter
still having to do with order:
Any $x$ star $y$
less than $m$ does imply
so is $y$, on this side of the border.

(theorem 10E)
And now comes some further chit-chat
about $m$, and any $x$ that
is big: that implies
that $x$ star $i$ is
big; it’s a big copycat.

(theorem 10E, #2)
$i$ star $x$ has a similar niche.
i with $x$, just make that switch.
Yep, that little $m$
is kind of a gem.
I could auction it off and get rich.

(theorem 10F)
$F$ is like $C$, but a whiff
stronger because it’s an iff.
So soon, we shall see
we’ll get to prop $G$
and that will make all the diff.
(theorem 10G)
At last! At last! At last!
We got there, though not very fast.
It took six prelims.
We got more than a glimpse.
But even those came to pass.

I’m sure there’s a shorter way.
But my high-school teachers would say
“You’re the master” – in truth –
“of the longest proof”.
And we all thought that was okay.

Okay, star’s assoc, not a myth.
But is it assoc arith?
We don’t know yet,
I must regret.
That’s something we’ll have to live with.

No, we won’t get an answer, alas.
But we will find a certain class
- yes, a healthy dose –
of stars assoc
that are up to our present task.

(theorem 11)
Though this prop might sound a tad clinical
of success it could give us the pinnacle.
It could give us a sharp
that’ll make the mark
and render us much less cynical.

(reality check)
As these poems you so dutifully edit
keep one thing in mind, to my credit:
I know that “mark”
doesn’t rhyme with “sharp”
but it worked for where I was headed.
(**Theorem 11, #2: the success-building prop**)

If for every $x$ in $\mathbb{Z}$
there’s an $a$, which is $1 \mod p$
and whose row $x$ is in
and if $a$ has no twin
we can find a nice sharp, yipperee!

(**Reality check**)
I know, I meant $\mathbb{Z}^+$
in the very-first line; how disgusting, and so I’m grievin’
because it’s not even mathematically robust.

(**Theorem 11, #3**)
Here’s the formula: $x$ sharp $y$
equals $a$ star $(x + i)$
where $i$ is the place
where $y$ shows its face
in the $a$-row. Just give it a try.

No, we won’t know it all, although
some things we will get to know.
Namely, examples.
I’ll give you some samples.
They soon will appear below.

(**Theorem 12**)
In the case $p$ prime, and $m 1$
sharp is almost said and done
unless $y$ haps to be
$0 \mod p$.
That would turn all our glee to glum.

(**Theorem 12 #2**)
So we must add to the hypoth
unique $a$ for those $x$ so wroth.
But it’s easy to find.
Lots of stars come to mind.
I knew we could pull it off.
Here’s one such example so cozy.
But we have to express it in rows-y.
And remember, they’re finite
both by day and by night.
The next verse is nigh, if you’re nosy.

Yes, now let us stop all the teasin’.
For such rows it might be the season:
1, 2, 3, 4, 5
6, 7, 8, 9, 10
No rhyme there but plenty of reason.

That’s just one example, please note.
It’s the easiest one to quote.
Of others there’s plenty
far more than twenty.
We have every right to gloat.

Still, there’s one star that we can’t crack
though I try like a maniac.
1, 2, 3, 4, 5
6, 7, 8, 9, 5.
But that rhymes, at least on this Mac.

So now we’ve got plenty of ways
to make non-ordinary a-a’s.
But questions remain.
Well, no pain, no gain.
And the converse won’t hold nowadays.

Here’s a question that’s really quite chewy.
We cannot dismiss it as hooey:
*Commut* a-a’s exist.
We could make a whole list.
But we don’t know them all, or do we?
(reality check)

As these poems you so deftly go through
keep one thing in mind as you do:
I know that third line
could be more confined.
But it’s mathematically true.
(And don’t dare jump up and shout Boo.)

No, I haven’t yet been enough wise
to completely characterize
either a-a’s commut
or assoc, nope, can’t do it.
But at least I’ve not told any lies.