Spring 5-15-2015

# Commutative n-ary Arithmetic

Aram Bingham
*University of New Orleans*, arbingha@uno.edu

# Commutative $n$-ary Arithmetic

A Thesis

Submitted to the Graduate Faculty of the
University of New Orleans
in partial fulfillment of the
requirements for the degree of

Master of Science
in
Mathematics

by

Aram R. Bingham

B.A. McGill University, 2012

May 2015

For NP, NR.

# Acknowledgments

I AM PERSONALLY GRATEFUL to Henri Darmon, who initiated me into number theory. He transformed my relationship with mathematics, and ultimately, it seems, my entire life's course. I also thank the University of New Orleans for providing the opportunity to pursue this research. The encouraging academic environment at UNO continues to inspire my belief in public education and my hope for humanity. In particular, I thank Craig Jensen, Kenneth Holladay and Ralph Saxton for their advice and support. Finally, I acknowledge my colleague Bradford Fournier for his valuable commentary, words of encouragement, and general camaraderie.

# Contents

# Abstract

Motivated by primality and integer factorization, this thesis introduces generalizations of standard binary multiplication to commutative $n$-ary operations based upon geometric construction and representation. This class of operations are constructed to preserve commutativity and identity so that binary multiplication is included as a special case, in order to preserve relationships with ordinary multiplicative number theory. This leads to a study of their expression in terms of elementary symmetric polynomials, and connections are made to results from the theory of polyadic ($n$-ary) groups. Higher order operations yield wider factorization and representation possibilities which correspond to reductions in the set of primes as well as tiered notions of primality. This comes at the expense of familiar algebraic properties such as associativity, and unique factorization. Criteria for primality and a naïve testing algorithm are given for the ternary arithmetic, drawing heavily upon modular arithmetic. Finally, connections with the theory of partitions of integers and quadratic forms are discussed in relation to questions about cardinality of primes.

Number Theory, Partitions, Symmetric Polynomials, Primality Testing, $n$-ary Algebra, Integer Factorization

*Becoming sufficiently familiar with something is a substitute for understanding it.*

John H. Conway

# 1 Introduction

Geometry has a long history of inspiring algebraic and arithmetic investigations in mathematics. This is evident, for instance, in the extension from the complex numbers to the quaternions in order to describe spatial rotations. The development from natural numbers to integers to rationals to reals can be viewed as an endeavor to capture the notion of spatial continuum. However, this vigorous pursuit has perhaps limited development of algebraic constructions that rely only upon the most fundamental set, the natural numbers. This thesis seeks to partially remediate that deficiency by contributing a class of algebraic operations over $\mathbb{N}^n$. In motivating their construction, we will take spatial considerations into account, while keeping in mind the goal to eventually become independent of geometry.

We take natural numbers (from which we will exclude zero throughout) as fundamental correlates of

consciousness, requiring no justification or act of construction. From this vantage, how we choose to manipulate and represent those objects becomes largely arbitrary. The standard binary operations, $+$, $\times$, have been engrained as the fundamental logic of the set, impossible to deny or ignore when performing manipulations of natural numbers. Rather than argue to the contrary, we will argue to support the idea that these constitute a limited portion of what may be reasonably be called "operations" over $\mathbb{N}$.

Of course, an $n$-ary operation is merely a function that associates some $n$-tuple of elements from $n$ domain sets with some element from a co-domain set. There are limitless ways to construct arbitrary operations over natural numbers (i.e. from $\mathbb{N}^n \mapsto \mathbb{N}$). There are relatively fewer that would seem somehow natural or worthy of attention. How we choose these may be informed by which familiar notions from algebra we should wish to preserve, which we should ignore, and what new ones we might add. These attributes, perhaps owing to the success of group theory, seem to have become a sort of hierarchy in which some are seen as more fundamental than others.

This hierarchy is artificial, and need not be observed. Rather, one can look to other sources of inspiration such as geometry and symmetry to determine a bundle of algebraic properties. In order to tread the middle ground between mathematical tradition and arbitration, this thesis will develop operations that maintain a connection with conventional number theory by retaining some of the properties of our binary operations, while simultaneously illustrating the possibilities of arithmetical expansion. In particular, the properties of identity and commutativity will allow us to maintain a connection with the number theory that results from the definition of our binary operations.

The kernel of inspiration motivating these investigations is the idea that binary multiplication is simply the construction of rectangular figurate numbers. We follow the single and very thin thread of what may occur if we allow representations of other figurate numbers, especially hexagons, to define novel arithmetic operations. The opportunities for research here are vast–while substantial literature has been devoted $n$-ary algebras, non-associative algebra and the like, explicit connections with arithmetic are rarer. Perhaps the closest thing in spirit is the study of tetration and other hyper-operations which constitute another sequence of recursive arithmetic functions, however they do not increase in arity and are perhaps less relevant to multiplicative number theory.

Research in arithmetic is a lot like staring at the sun. Insight and impairment might easily be confused when performing either activity, hence it will be helpful to set down the goals and guiding principles of the treatment at hand.

Prospects. *We shall develop non-trivial n-ary generalizations of binary multiplication on the natural numbers via geometric intuition. Operations of high arity shall seek to include lower arity operations as special cases.*

To explain the motivations, we first examine the structure of ordinary, binary multiplication. As a consequence of its iterative nature, binary multiplication can be represented in a familiar rectangular grid of points. For instance, $3 \cdot 5 = 3 + 3 + 3 + 3 + 3 = 5 + 5 + 5 = 15$ can be represented by taking a row of three evenly spaced points, and laying it down beside itself five times, or vice versa. It is worth noting the resemblance between this representation and Young and Ferrers diagrams from partition theory, a subject that will be treated in more depth later on.

The resulting object, which we will refer to as a rectangular *crystal*, possesses notable symmetry qualities – two-fold reflective symmetry and one rotational symmetry. In case the operands are identical, we get a square with four of each kind of symmetry (i.e. the dihedral group $D_4$). We have had to sacrifice the diagonal symmetries of the square in order to allow for sides of distinct length, but this looser symmetry allows crystals to depict an algebraic operation that takes independent arguments from $\mathbb{N}$.

The requirement of two-fold reflective symmetry also admits parallelogram crystals. Insofar as the crystal represents an algebraic operation whose result depends only on the side lengths (in terms of number of points, rather than distance under some metric), we wish to describe a visual geometric process by which we discover the output, relying upon minimal outside mathematical machinery. Consider the following constructive process:

Geometric Construction of Binary Multiplication.

Step 1. *Select two elements, m, n, from* $\mathbb{N}$ *as arguments.*

Step 2. *Construct a set of m distinct collinear points. Starting from one point (not necessarily an endpoint) of this set, construct n collinear points (including the point in common) such that the line defined by this set is distinct from the line defined by the set of m points.*

Step 3. *Construct the line through each point that is parallel to either of the two lines defined by each set.*

Step 4. *Count the distinct intersections of all pairs of lines. This number is the product* $m \cdot n$.

This process describes a general geometric way of interpreting the product of two natural numbers. We shall refer to a set of $m$ collinear points as an *m factor* in order to distinguish if from just the number $m$. Note that

in this description, neither the spacing between the points nor the angle between the lines matters so long as the lines are distinct. If, for instance, $m$ is 1 then there is no line defined by that factor, hence we construct no new points of intersection and the product is just $n$.

The construction also suggests a further generalization - what occurs if we proceed with more sets of collinear points? Can we define operations of higher arity that are distinct from iterative binary multiplication? Here, the construction becomes much more sensitive to angle and spacing particularities of the factors. Furthermore, there arises a question of whether to count all intersections of any two lines, or only the intersections of the maximal number of lines, as well as how to classify and predict when each type of intersection arises. The delicacies here have been studied and generalized in the domain of incidence combinatorics. However, as a basis for development of algebraic operations over the natural numbers, many such constructions would be too irregular to be satisfying.

Instead, we will choose to pursue a more restrictive and "regular" regime in order to exploit its symmetry properties and demonstrate with simplicity the possibilities that arise from pursuing geometry-inspired arithmetic. Hence, given that in the binary multiplication operation, our construction yields a convex quadrilateral, we will take up a ternary operation that enumerates intersections that lie within a convex hexagon. To simplify the geometry, we will make this hexagon equiangular, and the points in each factor will be evenly spaced.

This results that the lines defined by each factor will be at angles of $\frac{2\pi}{3}$ to one another, and all points of intersection are equidistant from their nearest neighbors. In other words, the points of intersection lie on points of a hexagonal (equilateral triangle) lattice. The exceptional symmetry of this lattice corresponds to the fact that our operation will be fully commutative. First, we shall describe the construction as a process analogous to the binary case, appealing to ordinary language and perception for clarity at the temporary expense of generality and mathematical orthography.[*]

Geometric Construction of Ternary Multiplication.

Step 1. *Select three elements, i, j, k, from* $\mathbb{N}$ *as arguments.*

Step 2. *Construct the i-factor, oriented so that it makes an angle of* $\frac{2\pi}{3}$ *with the horizontal, measuring from standard position.*

[*]The construction of the convex hull can also be described in terms of movements along the vectors of the planar hexagonal lattice. We are skirting these technicalities to get directly to the arithmetic aspects.

Step 3. *From the southeast endpoint of this set, construct the j factor in the horizontal direction to the right.*

Step 4. *Beginning from the rightmost point of the j factor, construct the k factor in the northeast direction so that its containing line makes a standard position angle of* $\frac{\pi}{3}$ *with the horizontal.*

Step 5. *Proceeding clockwise from the northeast endpoint of the k factor, append, in order, another i, j and k factor such that the interior angle between each adjacent containing line segment is* $\frac{2\pi}{3}$*. The last point of the final k factor is the first point of the first i factor.*

Step 6. *Through each point in each factor, construct all lines parallel to the containing lines of each factor.*

Step 7. *Count, including factor points, the intersections of all such lines that lie on the boundary and interior of the hexagon constructed in Step 5. This number is the ternary product of i, j, and k.*

We will denote the ternary multiplication operation described above as $\langle i, j, k \rangle$, wherein the positions correspond respectively to the left, middle, and right factors along the bottom half of this standard visual representation of our operation. We are guaranteed that the hexagon is well constructed by the fact that the second set of factors constructed in Step 5 are of equal length and in opposite direction to their corresponding factors constructed prior.

We have now summarized an interest in diversifying the cannon of arithmetical operations, and we have specified an approach to creating higher arity generalizations of binary multiplication via geometric construction. Over the course of the next chapters we will discuss properties of the particular construction at hand that advance its case as a natural extension. However, it is worth restating that this is but one possibility, and there are myriad others that may lend other insights into traditional number theory.

*The investigation of the symmetries of a given mathematical structure has always yielded the most powerful results.*

Emil Artin

# 2

# Symmetry

We begin with a discussion of a few of the basic properties of this ternary multiplication operation, which may also denoted as a function $\circledast_3 : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$. These properties will be used to construct the higher arity generalizations, though we will return to a more thorough investigation of $(\mathbb{N}, \circledast_3)$ in Chapter 3. First observe that $\langle 1, 1, n\rangle = \langle 1, n, 1\rangle = \langle n, 1, 1\rangle = n$. In each case, the hexagon degenerates into a single factor that absorbs the 1 factors, and the second $n$ factor from Step 5 overlays onto the points already constructed. The only line defined is that which contains this $n$ factor so no new points of intersection are created, though the orientation of this line changes in each corresponding standard representation.

Furthermore, we have that

$$\langle 1, m, n\rangle = \langle 1, n, m\rangle = \langle m, 1, n\rangle = \langle n, 1, m\rangle = \langle m, n, 1\rangle = \langle n, m, 1\rangle = mn = nm.$$

This fact follows from that, in each construction, the 1 factors degenerate into vertices of the acute angles of a parallelogram with sides that come from the $m$ and $n$ factors. Then, the rest of the process is identical to that of binary multiplication which required only that the factor lines be at non-zero angles to one another. Hence, $\circledast_3$ contains binary multiplication of natural numbers as a subset in which one of the operands is 1. We have then preserved 1 as an identity element.

A more efficient way to characterize the operation $\circledast_3$ is to say that it enumerates the hexagonal lattice points contained by a convex lattice hexagon of side lengths (in cyclic order) $i, j, k, i, j, k$.* This phrasing, suggests a more combinatorial and discrete geometry approach, subverting the arithmetical focus of this investigation. But one of the tools of such an approach, Erhart polynomials, does suggest that we should be able to find a polynomial representation of our operation, $\circledast_3$. We turn now to the discovery of that polynomial that will capture all possible hexagonal figurate numbers.

If we dilate our hexagon by adding one to one of the factors pairs, our construction grows by the sum of the other two sides, minus the point they have in common, i.e.

$$\langle i+1, j, k\rangle = \langle i, j, k\rangle + j + k - 1. \tag{2.1}$$

Then, since $\langle 1, j, k\rangle = jk$, we can develop the sequence,

$$\begin{aligned}
\langle 1, j, k\rangle &= jk \\
\langle 2, j, k\rangle &= jk + j + k - 1 \\
\langle 3, j, k\rangle &= (jk + j + k - 1) + j + k - 1 = jk + 2(j + k - 1) \\
\langle 4, j, k\rangle &= jk + 3(j + k - 1) \\
&\vdots \\
\langle i, j, k\rangle &= jk + (i - 1)(j + k - 1),
\end{aligned} \tag{2.2}$$

*Binary multiplication again has an analogous characterization as the enumeration of lattice points within an appropriate lattice quadrilateral.

where this final equation can be rewritten as,

$$\langle i, j, k \rangle = ij + jk + ki - i - j - k + 1, \tag{2.3}$$

or,

$$\langle i, j, k \rangle = i(j-1) + j(k-1) + k(i-1) + 1 \tag{2.4}$$

or perhaps less obviously,

$$\langle i, j, k \rangle = ijk - (i-1)(j-1)(k-1). \tag{2.5}$$

We see immediately that $\circledast_3$ is commutative from its expression in terms of the commutative operations of addition and binary multiplication. This was perhaps already clear from the geometric intuition, since permuting factors just reorients the standard representation of our hexagon. This also follows from the 3-fold symmetry properties of the hexagonal lattice.

Before proceeding with a thorough investigation of the arithmetic and algebraic properties of our ternary operation, it is worth describing a means of generalizing $\circledast_3$ to operations of higher arity. We have already compressed our simple construction of intersections of parallel lines through factor points by restricting to a symmetric convex hull whose sides are determined by the operands. The shape of this hull and resulting number of interior intersections has depended on the underlying lattice. We have patterned a commutative $n$-ary operation to rely upon a lattice that shares symmetry properties with the regular $2n$-gon, since otherwise the sides of the polytope might not lie along the lattice vectors. However, a consequence of crystallographic restriction is that a lattice of 8-fold rotational and reflective symmetry (like the regular octagon, and that might correspond to a quaternary operation) must embed in at least 4-dimensional Euclidean space.[3] The embedding dimension continues to increase with the number of symmetries. While it is surely possible to enumerate the points of a higher dimensional lattice contained within a given lattice polytope through geometric reasoning, we will generalize our operation algebraically.

The form of $\circledast_3$ given by equation 2.3 suggests one way to do this. We see that this is an alternating sum of the first three elementary symmetric polynomials over three arguments. For a quaternary operation, we wish to maintain commutativity and preserve the identity by reducing to $\circledast_3$ in the case where any one of the operands is 1. To achieve this, we should first define a modified sequence of symmetric polynomials using our ternary oper-

ation.

Given a set of three elements, $i, j, k$, from $\mathbb{N}$, we assign as usual, the elementary symmetric polynomials,

$$\begin{aligned}\sigma_0(i,j,k) &= 1\\ \sigma_1(i,j,k) &= i+j+k\\ \sigma_2(i,j,k) &= ij+jk+ki\end{aligned}$$

so that each $\sigma_n$ is the sum of all $n^{th}$ degree homogeneous terms composed of distinct elements. Then our definition of $\langle i,j,k\rangle$ fits description as an alternating sum as given above, i.e.

$$\langle i,j,k\rangle = \sigma_2(i,j,k) - \sigma_1(i,j,k) + \sigma_0(i,j,k). \tag{2.6}$$

Now, we will deviate from the standard elementary symmetric polynomials by further assigning

$$\sigma_3(i,j,k) = \langle i,j,k\rangle$$

and in general for a set of $n$ natural numbers, $\{m_1, m_2, \ldots, m_n\}$,

$$\sigma_3(m_1, m_2, \ldots, m_n) = \sum_{1\le i<j<k\le n} \langle m_i, m_j, m_k\rangle. \tag{2.7}$$

In particular, we have for $n = 4$,

$$\sigma_3(h,i,j,k) = \langle h,i,j\rangle + \langle h,i,k\rangle + \langle h,j,k\rangle + \langle i,j,k\rangle. \tag{2.8}$$

Now we may define a quaternary operation $\circledast_4 : \mathbb{N}^4 \mapsto \mathbb{N}$, also denoted $\langle h,i,j,k\rangle^\dagger$ as

$$\langle h,i,j,k\rangle = \sum_{l=0}^{3} (-1)^{3-l}\sigma_l(h,i,j,k). \tag{2.9}$$

[†]For brevity, as with the ternary operation, we should like like to refer to the symbol $\circledast_4$ when referring to general properties of the operation, and the bracketed notation when describing properties specific to the arguments. In cases where the bracketed notation is possibly ambiguous, we may use the functional notation $\circledast_n(m_1, m_2, \ldots, m_n)$.

The operation $\circledast_4$ is guaranteed to be a commutative as well since it is also a sum of symmetric polynomials. If it generalizes the ternary operation in the sense that $\langle 1, i, j, k\rangle = \langle i, j, k\rangle$, then we can be sure that it also preserves binary multiplication and the identity as special cases where the other operands are also 1, since the ternary operation does this already. To verify this condition, we expand $\circledast_4$ out as a polynomial.

$$\begin{aligned}
\langle h, i, j, k\rangle &= \langle h, i, j\rangle + \langle h, i, k\rangle + \langle h, j, k\rangle + \langle i, j, k\rangle - hi - hj - hk - ij - ik - jk + h + i + j + k - 1 \\
&= hi + ij + jh - h - i - j + 1 + hi + ik + kh - h - i - k + 1 + hj + jk + kh - h - j - k \\
&\quad + 1 + ij + jk + ki - i - j - k + 1 - hi - hj - hk - ij - ik - jk + h + i + j + k - 1 \\
&= hi + ij + hj + ik + hk + jk - 2h - 2i - 2j - 2k + 3 \qquad (2.10) \\
&= \sigma_2(h, i, j, k) - 2\sigma_1(h, i, j, k) + 3\sigma_0 \qquad (2.11)
\end{aligned}$$

We can see from (2.10) that if we let any of the operands equal to 1, for instance $h$, then we get,

$$\begin{aligned}
\langle 1, i, j, k\rangle &= i + ij + j + ik + k + jk - 2 - 2i - 2j - 2k + 3 \\
&= ij + jk + ki - i - j - k + 1 \\
&= \langle i, j, k\rangle
\end{aligned}$$

as desired. Let us proceed to define the sequence of all $n$-ary operations that generalize binary multiplication in this way.

Definition of $n$-ary Multiplication. *Let $\{m_1, m_2, \ldots, m_n\}$ be a set of n natural numbers. Then their n-ary product under the operation $\circledast_n$ is defined to be $\langle m\rangle = m$ for $n = 1$, $\langle m_1, m_2\rangle = m_1 m_2$ for $n = 2$, and for $n \geq 3$*

$$\langle m_1, m_2, \ldots, m_n\rangle = \sum_{k=0}^{n-1} (-1)^{n-1-k} \sigma_k(m_1, m_2, \ldots, m_n) \qquad (2.12)$$

*where $\sigma_k$ is defined by the recursive sequence,*

$$\sigma_0(m_1, m_2, \ldots, m_n) = 1$$

*and for* $1 \leq k \leq n$,

$$\sigma_k(m_1, m_2, \ldots, m_n) = \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} \langle m_{i_1}, m_{i_2}, \ldots, m_{i_k} \rangle \tag{2.13}$$

There is a close relationship between $\circledast_k$ and $\sigma_n$ in that they both rely on each other recursively for definition. But they are distinguished by the fact that $\sigma_k$ can take $n \geq k$ arguments while $\circledast_n$ must take exactly $n$ operands. In words, $\sigma_k(m_1, m_2, \ldots, m_n)$ is the sum of the set of all distinct $k$-ary products from $n$ numbers. Hence, in each of these sums there are $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ summands. We are again guaranteed that the operations $\circledast_n$ are commutative by the fact that they are all sums of symmetric polynomials. It is less obvious, however, that each operation extends the operations of lower arity by preserving the identity element, which merits the following proposition.

Proposition 1. *All n-ary operations* $\circledast_n$ *as defined above satisfy* $\circledast_{n+1}(1, m_1, m_2, \ldots, m_n) = \circledast_n(m_1, m_2, \ldots, m_n)$.

*Proof.* We proceed by strong induction. In the base case, $n = 1$, we know that

$$\langle 1, m \rangle = 1m = m = \langle m \rangle$$

Then, we assume that

$$\circledast_{k+1}(1, m_1, m_2, \ldots, m_k) = \circledast_k(m_1, m_2, \ldots, m_k)$$

for all $k \leq n - 1$. We will demonstrate that this implies

$$\circledast_{n+1}(1, m_1, m_2, \ldots, m_n) = \circledast_n(m_1, m_2, \ldots, m_n)$$

by showing that all of the terms in the sum,

$$\langle 1, m_1, m_2, \ldots, m_n \rangle = \sum_{k=0}^{n} (-1)^{n-k} \sigma_k(1, m_1, m_2, \ldots, m_n)$$

cancel out except for the contribution from $\sigma_n$ of $\langle m_1, m_2, \ldots, m_n \rangle$. This can be done, in combinatorial fashion, by establishing a correspondence between the terms of $\sigma_k(1, m_1, m_2, \ldots, m_n)$ that take 1 as an operand and those from $\sigma_{k-1}(1, m_1, m_2, \ldots, m_n)$ that don't. The terms of $\sigma_k$ are all of the possible $k$-products chosen from $\{1, m_1, m_2, \ldots, m_n\}$, hence there are $\binom{n+1}{k}$ of them, $\binom{n}{k}$ of which don't take 1 as an operand. Hence, $\binom{n+1}{k} - \binom{n}{k}$

of them do take 1 as an operand. Fixing 1 as an operand, this quantity is equally expressed as the number of ways to choose the $(k-1)$ other operands from among the $n$ other possibilities, $\{m_1, m_2, \ldots, m_n\}$, i.e. $\binom{n}{k-1}$.

By our induction hypothesis, these $\binom{n}{k-1}$ $k$-ary products that have 1 as an operand reduce to $\circledast_{k-1}$ products that omit the 1 for all $k \leq n$. In the expansion of $\circledast_{n+1}(1, m_1, m_2, \ldots, m_n)$, $\sigma_{k-1}(1, m_1, m_2, \ldots, m_n)$ contributes exactly $\binom{n}{k-1}$ terms which are $(k-1)$-ary products that don't include 1. These must be identical to the degenerate cases from $\sigma_k$ since both sets comprise all possible combinations of $(k-1)$ distinct elements from the set $\{m_1, m_2, \ldots, m_n\}$. But since the sign of $\sigma_k$ alternates in the summation these identical sets of terms have opposite sign and so cancel out. Then the remaining terms of $\sigma_{k-1}$ that do take 1 as an operand will cancel with those from $\sigma_{k-2}$ that do not etc. We have a descending chain of cancellation valid for all $k \leq n$, where in the final step, $k = 1$, $\sigma_1$ contains a single term that takes 1 as an argument, i.e. $\langle 1 \rangle$ (all of the other terms have cancelled with degenerate terms from $\sigma_2$). This 1 cancels with the 1 of opposite sign coming from $\sigma_0$. Hence the only term which we haven't cancelled from

$$\langle 1, m_1, m_2, \ldots, m_n \rangle = \sum_{k=0}^{n} (-1)^{n-k} \sigma_k(1, m_1, m_2, \ldots, m_n)$$

is the $n$-ary product from $\sigma_n$ that doesn't include one. But there can only be $\binom{n}{n} = 1$ of these, hence it is the product $\langle m_1, m_2, \ldots, m_n \rangle$ as desired. □

A natural corollary from this proposition is as follows.

Corollary 1. *An $n$-ary product $\circledast_n$ in which $j$ of the operands are equal to one is equivalent to the $\circledast_{n-j}$ product of the other $n-j$ operands.*

*Proof.* This follows from repeated application of Proposition 1. By the commutativity of $\circledast_n$, we can write our product as

$$\langle \overbrace{1, \ldots, 1}^{j}, m_1, \ldots, m_{n-j} \rangle.$$

Then, applying the Proposition $j$ times to the above expression yields the desired result. □

The case of this corollary in which $j = n - 1$ establishes that 1 is the *$n$-ary identity* of our operation, $\circledast_n$, as per Dudek[5]. Several interesting questions arise out of this fact, including whether or not it makes sense to construct an operation of infinite arity along these lines; it does not. This would be an alternating series of

polynomials where each $\sigma_n$ would be taking the sums of all possible finite $n$-products from an infinite set of natural numbers of each of which is clearly divergent. The overall product is ill-defined unless only finitely many of the operands are non-unit, so it suffices to consider finitary operations. More explicitly, we can consider the sequence of $n$-products in which every operand is 2, $\circledast_n(2)$. As one may verify, this satisfies a neat progression in that $\circledast_n(2) = \circledast_{n-1}(2) + n$. As the minimal $n$-ary product that does not degenerate into a product of lower arity, we can see that its value is unbounded as $n$ grows.

Other interesting questions arise from comparison of our $n$-ary operations to the existing theories of $n$-ary algebraic structures. Most of the relevant literature has been devoted to the study of $n$-ary (or *polyadic*) groups. The axioms that define an $n$-ary group are associativity and inverse conditions that generalize those properties as they apply to ordinary groups, and imply the existence of an identity element in the case of an ordinary binary group. We will see in the next chapter exactly how the ternary operation fails to be associative. This implies that none of its higher arity generalization are associative either, since they contain the ternary operation as a special case.

The question of inverses could be resolved, as is typical, by completing to a larger set. For instance, zero and the negative integers are constructed in order to complete the natural numbers and form a group under the operation of addition. The fractions $\frac{1}{n}$ are the completion of naturals with respect to group formation under the multiplication operation. It is possible that we could construct a number system that leads to invertibility under our $n$-ary operation, but we are mainly concerned with factorization and primality among the naturals, so we will ignore here these more algebraic concerns.

However, we can at this point prove the non-associativity of $\circledast_n$ without specific calculation by referring to the theory of polyadic groups. Here, a set with an $n$-ary operation is referred to as an $n$-ary *groupoid*. The most obvious way of constructing an $n$-ary operation is to simply take a binary operation and glue it to itself repeatedly in an $n$-fold product; such an $n$-ary operation is said to be *derived* from the binary operation. Then, the $n$-ary operation clearly inherits the associativity and identity properties of the binary operation. In our case, this would mean considering the repeated binary multiplication of three natural numbers, $a \cdot b \cdot c$, as a trivial ternary operation $f(a, b, c)$, and so on. It turns out that this construction is the *only* associative ternary operation on the natural numbers that takes $f(1, a, b) = a \cdot b$, so we should not be too chagrinned by the failure of associativity in our generalizations of binary multiplication.

We will not give here the exact definitions of $n$-ary associativity and invertibility, as they don't apply to

our operation. It should be noted that an $n$-ary group, $(G, f)$, that satisfies such properties may have multiple identity elements, or none at all. An $n$-ary identity element, or *neutral* element, $e$, is understood to be one that fixes an arbitrary element $x \in G$ under the operation where $x$ appears as any single operand, and every other operand is $e$. An $n$-ary group $(G, f)$ is said to be *reducible* whenever $f(x_1, x_2, \ldots, x_n) = x_1 \circ x_2 \circ \ldots \circ x_n$ where $(G, \circ)$ is an ordinary group. We now state a theorem originally due to Dorntë[4] and later generalized by Post[9], which gives necessary and sufficient conditions for when an $n$-ary group is reducible into a binary group operation.

THEOREM. *An $n$-ary group $(G, f)$ is reducible if and only if it contains a neutral element. In particular, it is reducible to the group $(G, \circ)$ where $\circ$ is given by the evaluation of $f$ in which all but two of the operands is the neutral element.*

The proof of the above theorem relies only upon the $n$-ary associativity of $f$. Hence, it applies equally well to $n$-ary *semigroups* which are associative but need not exhibit invertibility. Then, the $n$-ary semigroup operation reduces into repeated application of an ordinary semigroup operation in exactly the same way, as has been stated by Dudek and Mukhin[6]. Since the binary semigroup operation is given by the $n$-ary semigroup operation in which all but two of operands are this neutral element, this binary semigroup then inherits the identity element and is in fact a monoid. It is then clear that if $\circledast_n$ was an $n$-ary semigroup derived from any associative binary operation, it would have to be from ordinary multiplication. Since it does not reduce into a simple string of repeated multiplications, it must fail one of the hypotheses, namely that it was associative. Thus the only associative $n$-ary operation on the natural numbers which has 1 as an identity element, and contains binary multiplication is the one whose operation is repeated binary multiplication.

We should also remind ourselves that associativity appears as a more basic property than commutativity only in order to generalize the definition of group. Any perceived hierarchy of algebraic properties is more a matter of historical tradition than mathematical significance. Even without associativity, we will discover a form of "reducibility" into more tractable polynomials, which is to say that our operation can be collapsed into a sequence of additions, just like binary multiplication and any other fully specified map that takes $\mathbb{N}^n \mapsto \mathbb{N}$.

Recall from before that in (2.10), upon reducing $\circledast_4$ into binary multiplication and addition, the constant coefficients of the $\sigma_1$ and $\sigma_0$ terms changed. All $n$-ary products are given in terms of sums of lower order products that are ultimately recursively decomposed into sums of the first three elementary symmetric polynomials. Hence we will always be able to reduce $\circledast_n$ into such an expression which we call the *quadratic form* of $\circledast_n$

(precisely it is an $n$-ary inhomogeneous quadratic form). That is, it can be expressed as a linear combination of the elementary symmetric polynomials $\sigma_2$, $\sigma_1$, and $\sigma_0[=1]$ over $n$ arguments:

$$\circledast_n(m_1, m_2, \ldots, m_n) = a_n\sigma_2(m_1, m_2, \ldots, m_n) + b_n\sigma_1(m_1, m_2, \ldots, m_n) + c_n \tag{2.14}$$

This form is considerably kinder for the purposes of evaluating $n$-products, and all that is left is a determination of the constants $a_n$, $b_n$, $c_n$. It turns out that $a_n = 1$, $b_n = 2 - n$, and $c_n = \frac{(n-1)(n-2)}{2}$ (that is, $c_n = T_{n-2}$ where $T_n$ is the $n$-th triangular numbers) for all $n$, but the details are messy and will be left for the appendix.

*The Way gave birth to unity; unity gave birth to duality; duality gave birth to trinity; trinity gave birth to the myriad creatures.*

Dao De Jing

# 3

# Arithmetic

We now retreat back to the ternary operation that began this pursuit in order to investigate the derangements of arithmetic that it may yield. It bears repeating that this will entail a study of the class of hexagonal figurate numbers, in the same way that that ordinary multiplicative number theory is a study of quadrilateral figurate numbers. Primes are then those numbers which only have representation as degenerate quadrilateral crystals. There is also a sense in which all quadrilateral crystals are degenerate hexagonal crystals, corresponding to the fact that $\langle 1, j, k \rangle = jk$.

Essentially, by including binary multiplication as a special case of our ternary operation, we expect to allow a more diverse range of factorization possibilities that will lead to a more subtle classification of numbers. To clarify this discussion let us introduce some terminology and notation. We will refer to the set of ordinary

primes from binary arithmetic as *2-primes*, $\mathbb{P}_2 = \{2, 3, 5, 7, 11, 13, \ldots\}$. The *3-primes* are the numbers that can only be represented in ternary multiplication as $\langle 1, 1, p\rangle$. Alternatively, we can also define this set as numbers that are not *3-factorable*.

Definition 1. *A number $n \in \mathbb{N}$ is said to be 3-factorable if and only if it is the ternary product of natural numbers i,j,k no more than one of which is equal to 1.*

The 3-prime numbers which are not 3-factorable constitute the set $\mathbb{P}_3 = \{2, 3, 5, 11, 17, \ldots\}$. This set is a strict subset of $\mathbb{P}_2$, since many 2-primes have hexagonal representations. These include the "perfect hexagons" $7 = \langle 2, 2, 2\rangle$ and $19 = \langle 3, 3, 3\rangle$. In fact, all 2-primes congruent to 1 mod 3 have nondegenerate hexagonal representations (and are thus 3-factorable), as the following proposition shows.

Proposition 2. *Every natural number congruent to 1 modulo 3 is 3-factorable.*

*Proof.* Since $n \equiv 1 \bmod 3$ we can write $n = 3j + 1$, where $j \geq 2$. Then,

$$\begin{aligned} n &= 3j + 1 \\ &= 4j - (j - 1) \\ &= (2)(j)(2) - (2 - 1)(j - 1)(2 - 1) \\ &= \langle 2, j, 2\rangle \end{aligned}$$

where the last equality comes from (2.5). □

The 3-factorability of 2-primes congruent to 1 mod 3 follows as a subset. This is perhaps unsurprising, since the underlying lattice of our hexagonal representations is exactly the lattice of Eisenstein integers. Recall that these are the complex numbers of the form $z = a + b\omega$, where $\omega = \frac{1}{2}(-1 + i\sqrt{3}) = e^{\frac{2\pi i}{3}}$, one of the cube roots of unity. It can be shown that integers congruent to 1 mod 3 are factorable into Eisenstein integers, while primes congruent to 2 mod 3 are not. Here instead we find that some 2-primes congruent to 2 mod 3 are 3-factorable, such as $29 = \langle 3, 3, 5\rangle$.

Also recall that hexagonal representations of integers are certainly not unique, since, for instance $19 = \langle 2, 6, 2\rangle = \langle 3, 3, 3\rangle$. We may be tempted to claim that factorization into ternary products of 3-primes is unique, but there we find the early counterexample $34 = \langle 2, 2, 11\rangle = \langle 2, 5, 5\rangle$.

Given the failure of a number of desirable algebraic properties here, it may be interesting to determine exactly how and by how much they fail. Here, we refer, for comparison, to the theory of ternary semigroups as described in Duplij et. al.[2] A nonempty set $G$ with one ternary operation $[\,]$ is said to be a *ternary groupoid*. If this ternary operation satisfies the associativity relationship

$$[[ghi]jk] = [g[hij]k] = [gh[ijk]] \tag{3.1}$$

then the pair $(G, [\,])$ is a *ternary semigroup*. It is interesting to note that we might have instead constructed a family of associative $n$-ary operations over $\mathbb{N}$ that did not treat 1 as an identity element, but it is unclear what relationships with binary multiplication could have been salvaged in that case. Furthermore, it is possible to construct any number of commutative $n$-ary operations by taking sums of multiples of symmetric polynomials. In this respect, the nice properties and geometric foundations of our operation makes it a good starting point for further investigation.

As we have mentioned, associativity must fail in our ternary operation since otherwise we would have the ternary semigroup derived from binary multiplication given by $[ijk] = i \cdot j \cdot k$, or we might otherwise sacrifice 1 as an identity element. Equivalently, we can say that $(\mathbb{N}, \cdot)$ is the *retract* of $(\mathbb{N}, [])$. How exactly does associativity fail under $\circledast_3$? We may directly calculate, using (2.5)

$$\begin{aligned} \langle\langle g, h, i\rangle, j, k\rangle &= \langle gh + hi + ig - g - h - i + 1, j, k\rangle \\ &= (gh + hi + ig - g - h - i)(j + k - 1) + jk, \end{aligned} \tag{3.2}$$

where the second equality comes from equation (2.2). By symmetry, we can then get that

$$\langle g, \langle h, i, j\rangle, k\rangle = (hi + ij + jh - h - i - j)(g + k - 1) + gk \tag{3.3}$$

$$\langle g, h, \langle i, j, k\rangle\rangle = (ij + jk + ki - i - j - k)(g + h - 1) + gh \tag{3.4}$$

and subtracting (3.2) from (3.3) and simplifying gives

$$\langle\langle g, h, i\rangle, j, k\rangle = \langle g, \langle h, i, j\rangle, k\rangle + (j - g)(hi - hk - ik + 2k - 1) \tag{3.5}$$

This equation captures the basic "associativity" relationship. Notice that this single-shift associativity obviously holds in case $j = g$, since both nested and outer products are identical. Alternatively we can have

$$hi - 1 = k(h + i - 2) \tag{3.6}$$

$$hi \equiv 1 \bmod h + i - 2 \tag{3.7}$$

There is a class of solutions to these equations where $h = i =: n$ is an odd integer, since then we can take

$$\begin{aligned} n^2 - 1 &= k(2n - 2) \\ (n+1)(n-1) &= 2k(n-1) \\ k &= \frac{n+1}{2}. \end{aligned}$$

Furthermore, if we let $k = 1$, then we can write (3.6) as

$$\begin{aligned} hi - i - j + 1 &= 0 \\ (h-1)(i-1) &= 0 \end{aligned}$$

so either of $h$ or $i$ must be 1. This case corresponds to our nested ternary products degenerating into a sequence of binary multiplications, whence the associativity. Explicitly, and without loss of generality, we may let $h = 1$ and observe

$$\langle\langle g, 1, i\rangle, j, 1\rangle = \langle gi, j, 1\rangle = (gi)j = g(ij) = \langle g, ij, 1\rangle = \langle g, \langle 1, i, j\rangle, 1\rangle. \tag{3.8}$$

Whether or not there are other solutions from the naturals to (3.6) seems like a potentially difficult problem.[*] We will limit ourselves to the suggestive remark that it bears some resemblance to the problem from RSA cryptography of solving

$$ed - 1 = k(N - (p + q - 1)) \tag{3.9}$$

where $(N, e)$ is a public key pair, $d$, $p$ and $q$ are secret and $k$ is unknown.[8]

Let us check the failure of associativity when two arguments are shifted. We can apply (3.5) and commu-

[*] Recall Hilbert's 10th problem on the decidability of Diophantine equations.

tativity to get

$$\langle g, \langle h, i, j\rangle, k\rangle = \langle g, h, \langle i, j, k\rangle\rangle + (k-h)(ij - gi - gj + 2g - 1), \tag{3.10}$$

and substituting this back into (3.5) we get

$$\langle\langle g, h, i\rangle, j, k\rangle = \langle g, h, \langle i, j, k\rangle\rangle + (k-h)(ij - gi - gj + 2g - 1) + (j-g)(hi - hk - ik + 2k - 1), \tag{3.11}$$

which simplifies to

$$\langle\langle g, h, i\rangle, j, k\rangle = \langle g, h, \langle i, j, k\rangle\rangle + ghk + ghj - gjk - hjk + 2jk - 2gh + g + h - j - k. \tag{3.12}$$

Again we find an easy set of solutions that reduces the non-associative part to zero when $g = j$ and $h = k$ (or equivalently $g = k$, $h = j$). Non-trivial solutions (or proving their non-existence) is probably an even greater challenge here though, since the non-associative part does not factor quite as nicely.

Studying the failure of associativity leads to the question of how much a ternary product can change when one or two of the operands are held fixed. Referring back to (2.2) we have the identity

$$\langle i, j, k\rangle \equiv ik \bmod i + k - 1 \tag{3.13}$$

and we can capture all numbers that satisfy this congruence and are greater than $ik$ just by incrementing $j$. Should we wish to keep one argument fixed, $i$ for instance, and examine which numbers are expressible as "3-multiples" of $i$, it is useful to note

$$\begin{aligned} ik + i^2 - i &= i(i + k - 1) \\ ik &= i - i^2 + i(i + k - 1) \end{aligned} \tag{3.14}$$

so that

$$\langle i, j, k\rangle \equiv ik \equiv i - i^2 \bmod i + k - 1. \tag{3.15}$$

This form allows us to increment our modulus ranging over $k$ while keeping $i$ and hence $i - i^2$ fixed. In order to make this explicitly independent of the other arguments we might note that, since we can choose $k$ to

make our modulus anything we want greater than or equal to $i$, we can express this congruence as

$$\langle i, j, k \rangle \equiv i - i^2 \equiv n \bmod i^2 - i + n \tag{3.16}$$

where

$$i^2 - i + n \geq i$$

$$n \geq 2i - i^2$$

since,

$$i - i^2 - n = -(i^2 - i + n) \equiv 0 \bmod i^2 - i + n.$$

Given the spectacular failure of unique factorization under this operation, integer factorization becomes a more delicate and disparate problem; we might be interested in finding a particular factorization of a given number or all of the factorizations of that number. However, it appears slightly more straightforward to ask whether or not an arbitrary number is a 3-prime. This will come down to determining whether it satisfies any of the congruence relations above. We now describe a naive sieving method for determining 3-primality. This will consist of fixing a modulus $m = i + k - 1$ and checking whether the number $N$ we are testing satisfies any of the possible congruences achievable by $ik \bmod i + k - 1$, i. e. we will run through the list of partitions of $m$ into two smaller numbers and check whether those any of those products give the same residue mod $i + k - 1$. When this condition is satisfied, we may recover *a* 3-factorization of $N$, but this is not necessarily *the only* factorization of $N$. If in no case $N$ satisfies one of these congruences up to a bound on $m$, then we can be sure that it is not a "multiple" of any pair of $i$ and $k$, and hence $N$ is not 3-factorable.

We will assume $N$ is odd, otherwise it is trivially not 3-prime. This will also allow us to eliminate the need to test any of the congruences for even $m$, as the following proposition shows.

Proposition 3. *Let $N \in \mathbb{N}$. Then $N$ is odd if and only if all of its 3-factors have the same parity.*

*Proof.* Let $N = \langle i, j, k \rangle$. Then

$$\begin{aligned} N &\equiv ik \bmod i + k - 1 \\ &\equiv jk \bmod j + k - 1 \\ &\equiv ij \bmod i + j - 1. \end{aligned}$$

Assume some pair of the factors have different parity so that one of the above moduli will be even. Suppose, without loss of generality, that this is true of $i$ and $k$. Then $N \equiv i - i^2 \bmod i + k - 1$. We know that $i$ and $i^2$ must have the same parity, so their difference must be even. Then $N$ is congruent to an even number with an even modulus, so $N$ is even.

Suppose all three factors have the same parity. Then we may recall (2.5) and observe that $N = ijk - (i - 1)(j - 1)(k - 1)$, and since $ijk$ and $(i - 1)(j - 1)(k - 1)$ clearly have opposite parity, their difference, $N$, must be odd. □

Hence, we have eliminated a need to check even moduli $m$, once we have determined that $N$ is not even. Given a natural number $N$, the following algorithm determines whether or not $N$ is 3-prime.

3-Primality Test.

*For odd $m$ where $3 \leq m \leq \lfloor \sqrt{N} \rfloor$ :*

*Calculate $N \bmod m$. Let $i_m = m$, $k_m = 1$. While $i_m \geq \frac{m+1}{2}$, calculate $i_m k_m \bmod m$. If $N \equiv i_m k_m \pmod m$, then $N$ is not 3-prime and we are done. Otherwise, set $i_m := i_m - 1$, $k_m := k_m + 1$ and continue the while loop.*

*If in no case for any such $m$ we find a congruence $N \equiv i_k m_k \bmod m$, then conclude $N$ is 3-prime.*

This test is certainly not optimal, but will effectively give us a 3-factorization of $N$ in case $N$ is not 3-prime, much like trial division in 2-primality testing. In this case, when we find that $N \equiv i_m k_m \pmod m$, we have found that $N = \langle i_m, j_m, k_m \rangle$ where

$$j_m = \frac{N - i_m k_m}{i_m + k_m - 1} + 1 \tag{3.17}$$

by solving for $j_m$ in the decomposition of the ternary product formula (2.2).

We should explain the upper bound for $m$. This limit allows for the case that $N$ does not have a completely nondegenerate 3-factorization in which one of the operands is 1, but is not 2-prime either, as occurs for the perfect square 9. There are clearly redundancies in this algorithm however. When $m$ is not a 2-prime, there may be cases where $(i_m k_m \pmod m)$ and $m$ are not relatively prime. In these cases, the test of whether $N \equiv i_m k_m \bmod m$ will already have been performed by the divisibility check when $m$ was equal to

$$g := gcd(i_m k_m \pmod m, m).$$

In fact, even if $g = 1$, we can entirely ignore the composite $m$, as a result of the following proposition.

Proposition 4. *Let $m = pq$, where $p$ and $q$ are not necessarily distinct integers. Then every residue class $i_m k_m \pmod m$ is congruent to some $i_p k_p \pmod p$ and some $i_q k_q \pmod q$ where $i_p + k_p = p + 1$, and $i_q + k_q = q + 1$.*

*Proof.* We can write, using (3.14) and that $pq = i_m + k_m - 1$,

$$\begin{aligned} i_m k_m &= i_m(pq + 1 - i_m) \\ &= pqi_m + i_m - {i_m}^2 \\ &\equiv i_m - {i_m}^2 \bmod p \\ &\equiv i_p - {i_p}^2 \bmod p \end{aligned}$$

where $i_m \equiv i_p \bmod p$. Since $i_p$ may range from 1 to $p$, we know such an $i_p$ exists. Then by equation (3.15) we know that $i_p k_p$ with $k_p = p + 1 - i_p$ satisfies the same congruence. We can proceed identically for $q$. Hence, all of the products $i_m k_m$ for composite $m$ satisfy a congruence modulo $p$ with $i_p k_p$ for each divisor $p$ of $m$. □

From this proposition follows the easy corollary that the residue classes of such $ik$ for any composite modulus are already contained by those of its prime factors. We may then revise our test to restrict only to where $m$ is an odd 2-prime. Enumerating the 2-primes less that $\sqrt{N}$ can be computationally demanding in itself, though the algorithm could be readily bootstrapped to include the sieve of Eratosthenes in order to do this. We may note that allowing this algorithm to run completely will give us all of the 3-factorizations of $N$, some of which may be redundant, but where we can determine each factorization as in (3.17) upon collision.

In contrast with the demonstration of redundancy in the previous proposition, we have the following for prime moduli.

Proposition 5. *Let $m$ be an odd 2-prime. Then the residue classes given by $i_m k_m \bmod m$ are distinct for each pair of distinct $i_m, k_m$ where $i_m + k_m - 1 = m$.*

*Proof.* Assume $i_a k_a \equiv i_b k_b \pmod{m}$ where $i_a + k_a = i_b + k_b = m + 1$. Then we can also write

$$\begin{aligned} i_a - {i_a}^2 &\equiv i_b - {i_b}^2 \pmod{m} \\ {i_a}^2 - {i_b}^2 - i_a + i_b &\equiv 0 \pmod{m} \\ (i_a - i_b)(i_a + i_b - 1) &\equiv 0 \pmod{m} \end{aligned}$$

so that $m$ divides the product on the left hand side of the last congruence. Since $m$ is a 2-prime, this means that either $m \mid i_a - i_b$ or $m \mid i_a + i_b - 1$. Since each of $i_a$, $i_b$ are bounded between 1 and $m$, we can write the inequalities

$$\begin{aligned} 1 - m \leq i_a - i_b \leq m - 1 \\ 1 \leq i_a + i_b - 1 \leq 2m - 1. \end{aligned}$$

Then if $m | i_a - i_b$ we must have that $i_a = i_b$, since 0 is the only number within the bounds of the inequality that divisible by $m$, and so also $k_a = k_b$. If $m \mid i_a + i_b - 1$, then $i_a + i_b = m + 1$ since $m$ is the only value within the bounds of the inequality that is divisible by $m$. This implies that $k_a = i_b$ and $k_b = i_a$. In either case, the $\{i, k\}$ pairs consist of the same values, so when two such products are in the same residue class, then the pairs that give those products must be the same. The contrapositive of this statement is the statement of the proposition. □

As a brief digression, this last proposition suggests a possible 2-primality test. For a given $N$, we may calculate the set of residues $i_N k_N \bmod N$. In case any of these are duplicated for distinct pairs of $i_N$, $k_N$, one can conclude that N is not prime (so this is really a compositeness test). Limited evidence does seem to suggest that for composite $N > 8$, there will occur at least one pair of duplicate residues. But, there is also the possibility of Carmichael-like composite numbers for which the set of all residues $i_N k_N \bmod N$ is distinct; a proof or conclusive computer search is in order to shed more light, as the parallels with the Fermat primality test are certainly worthy of further investigation.

We observed at the beginning of the chapter that the 3-primes are a subset of the 2-primes. Just how much smaller is this set? Recalling Dirichlet's theorem on arithmetic progressions, we may note that each congruence class $i_m k_m \pmod{m}$ for 2-prime $m$ comprises an infinite number of 2-primes. For each $m$, there are $\frac{m-1}{2}$

of these congruence classes corresponding to the distinct partitions of $m$ into two parts. Since the proportion of 2-primes in each residue class is $\frac{1}{\phi(m)}$, where $\phi$ is Euler's totient function, and $\phi(m) = m - 1$, each fixed $m$ eliminates $\frac{1}{2}$ of all of the 2-primes from our list of candidate 3-primes. If we repeat this process over any number of $m$'s, taking account of the overlap between the congruence classes of distinct $m$'s, it is a natural question to ask whether or not our list is still infinite. The next chapter investigates a number of possible approaches to this and similar questions.

*Looks like it's pretty hairy.*

General Jack Ripper

# 4

# Partitions and More

The divergence of ternary arithmetic from binary arithmetic can be nicely expressed in terms of partition theory. Since we are mainly concerned with conditions for factorability in the more generalized context, we again begin by describing these properties in binary multiplication.

Fact. *A number n is composite if and only if there exists a partition of n where each part is equal and greater that one.*

This is an obvious consequence of the definition of multiplication as iterated addition. There is another generalized description of the partitions of composite numbers based on their representation as rectangular crystals. Counting groups of points along diagonals rather than in vertical or horizontal groups, we can see that every

rectangular crystal can be enumerated by a sum of the form

$$1+2+3+\ldots+(m-1)+\overbrace{m+m+\ldots+m}^{k}+(m-1)+(m-2)+\ldots+3+2+1. \tag{4.1}$$

In particular, consider the rectangular crystal representation of the product of two natural numbers, $m$ and $n$. Then assume without loss of generality that $n \geq m$. We claim that $mn$ is expressed exactly by (4.1) where $k = n - m + 1$. Notice that on either end of the summation we have the sum of the naturals from 1 to $m-1$, i. e. the $(m-1)$-th triangular number $T_{m-1} = \frac{(m-1)m}{2}$. Hence,

$$\frac{(m-1)m}{2} + m(n-m+1) + \frac{(m-1)m}{2} = m(m-1+n-m+1) = mn \tag{4.2}$$

and the claim is true. Moreover, this partition is unique to the choice of factors $m$ and $n$. This will be a sticking point in the distinction between binary and ternary multiplication. There are, of course, distinct partitions of a given number $N$ of this form depending on which pair of factors we choose for it. For instance 12 has the two partitions*

$$\begin{aligned} 12 &= 1+2+3+3+2+1 \\ &= 1+2+2+2+2+2+1 \end{aligned}$$

corresponding to factorizations as $4\cdot3$ and $6\cdot2$, respectively. And of course we can write any number as a partition into as many ones, corresponding to the product $n \cdot 1$. Any of these types of partitions will be referred to as *mesa partitions*. Thus, the number of distinct mesa partitions of a given number $N$ is equal to half of the number of distinct divisors of $N$, $\frac{d(N)}{2}$, unless $N$ is a square in which case we have $\frac{d(N)+1}{2}$. 2-primes have only the trivial mesa partition that is a sum of 1's, semi-primes exhibit one other, and so on. Since all of these mesa partitions begin at 1, we may wonder what happens if we relax this restriction, in the way that triangular numbers generalize to polite numbers and trapezoidal numbers. This question corresponds exactly to the distinction between binary and ternary multiplication, and the representations of numbers as rectangular and hexagonal crystals.

We may specify a mesa partition within this larger class by determining three parameters. The *base* of a

*We are abusing terminology slightly here. Partitions are order independent summations and generally written in descending order, which we are not doing in order to make clearer the correspondence in the crystal representation.

mesa partition is the smallest number appearing in the summation. For all of the partitions based on binary factorizations above, the base was 1. But in the mesa partition of 29 as $3 + 4 + 5 + 5 + 5 + 4 + 3$, the base is 3. The *range* of a mesa partition is how many distinct consecutive numbers appear. In binary multiplication, this corresponded to the smaller factor, $m$, which happened to coincide with the largest number in the partition; which we will occasionally refer to largest number in a mesa partition as the *cap*. Finally, there is the *diameter* of the mesa partition, which is how many times the cap appears. The diameter for mesa partitions based on rectangular crystals was $n - m + 1$ above.

As might be expected, any given 3-factorization of a number $N$ does not uniquely determine a mesa partition of $N$. There are up to three possibly distinct mesa partitions for each 3-factorization $N = \langle i, j, k \rangle$ corresponding to a choice of base of as $i$, $j$, or $k$. We will for the moment ignore degenerate 3-factorizations where any of the arguments is equal to 1, recognizing that that will put us into the case of the binary multiplication mesa partitions described above.

First, some notation. A mesa partition $\mu$ of a natural number $N$ is specified by its base $b$, range $r$, and diameter $d$, and written $\mu(b, r, d) = N$. Now suppose that $i = j = k$. Then we claim that

$$N = \langle i, i, i \rangle = i + (i + 1) + \ldots + (2i - 2) + (2i - 1) + (2i - 2) + \ldots + (i + 1) + i = \mu(i, i, 1). \tag{4.3}$$

First we note that the last equality follows from our definitions just given. The mesa partition begins at $i$, consists of the $i$ distinct numbers from $i$ to $2i - 1$, and $2i - 1$ only appears once. The expanded sum can be written as

$$2i - 1 + 2 \sum_{l=0}^{i-2} i + l. \tag{4.4}$$

The sum $\sum_{l=0}^{i-2}$ is a trapezoidal number meaning it is equal to the difference of triangular numbers,

$$T_{2i-2} - T_{i-1} = \frac{(2i - 2)(2i - 1)}{2} - \frac{(i - 1)i}{2}$$

so (4.4) becomes

$$2i - 1 + (2i - 2)(2i - 1) - (i - 1)i = 3i^2 - 3i + 1 = \langle i, i, i \rangle \tag{4.5}$$

as desired.

These numbers given by $\langle i,i,i\rangle = \mu(i,i,1)$ are in fact the centered hexagonal numbers {1,7,19,37,61,91,...} (sequence A003215 in OEIS). For comparison, the perfect squares might be described as generated by the mesa partitions $\mu(1,i,1)$ as one can verify visually.

Now we consider the case $i = j \neq k$. We will treat this as two subcases. First, let $i < k$ so that the hexagonal crystal representation is like an augmented perfect hexagon. By permuting the arguments of (2.2) we know we can write

$$\langle i,i,i\rangle = i^2 + (i-1)(2i-1)$$
$$\langle i,i,k\rangle = i^2 + (k-1)(2i-1)$$

and subtracting these two equations gives the identity

$$\langle i,i,k\rangle = \langle i,i,i\rangle + (k-i)(2i-1) \tag{4.6}$$

so that we have enlarged the partition $\mu(i,i,1)$ by adding $k-i$ copies of the cap $(2i-1)$ giving a new diameter of $d = k-i+1$. Hence $\langle i,i,k\rangle$, with $i<k$ has a mesa partition of $\mu(i,i,k-i+1)$. There is another mesa partition corresponding to treating $k$ as the base. This is given by

$$\begin{aligned}
\mu(k,i,1) &= k + (k+1) + \ldots + (k+i-2) + (k+i-1) + (k+i-2) + \ldots + (k+1) + k \\
&= k + i - 1 + 2\sum_{l=0}^{i-2} k + l \\
&= k + i - 1 + 2(T_{k+i-2} - T_{k-1}) \\
&= k + i - 1 + (k+i-2)(k+i-1) - (k-1)k \\
&= 2ik + i^2 - k - 2i + 1 \\
&= \langle i,i,k\rangle
\end{aligned}$$

where the last two inequalities come from simplifying and applying (2.3), so the claim is proved.

Now we treat the subcase $i = j > k$. Using $k$ as a base, the mesa partition $\mu(k,i,1)$ still applies, however $\mu(i,i,k-i+1)$ is now invalid since this will give a negative diameter. Instead, we claim that the partition with

base $i$ becomes $\mu(i, k, i-k+1)$. By similar calculations, we can derive

$$\begin{aligned}
\mu(i,k,i+k-1) &= i + (i+1) + \ldots + (i+k-2) + (i+k-1)(i-k+1) + (i+k-2)\ldots + (i+1) + i \\
&= (i+k-1)(i-k+1) + 2(T_{i+k-2} - T_{i-1}) \\
&= (i+k-1)(i-k+1) + (i+k-2)(i+k-1) - (i-1)i \\
&= i^2 + 2ik - 2i - k + 1 \\
&= \langle i, i, k \rangle
\end{aligned}$$

Finally, we may discuss the case where none of $i, j, k$ are equal. Without loss of generality we may assume $i > j > k$. By very similar calculation, one can find that the base $i$ partition is $\mu(i, j, k-j+1)$, and the base $j$ partition is $\mu(j, i, k-i+1)$, and the base $k$ partition is $\mu(k, i, j-i+1)$. This last set of equations makes it clear that there is a correspondence between the set of mesa partitions of a number $N$ and its 3-factorizations. For any natural numbers $b$, $r$, or $d$, we can find an $i, j$, and $k$ such that $\mu(b, r, d) = \langle i, j, k \rangle$. Furthermore, we may enumerate the number of mesa partitions of a given number $N$ by applying the algorithm from the previous chapter to find all of the 3-factorizations of $N$, and for each type of factorization we may have up to 3 mesa partitions depending on the case.

The mesa partition counting function, $\mathrm{M}(N)$ may then be defined. This may also be an approach to determining the cardinality of the set of 3-primes. In case this function can be eventually bounded away from 1, then there are finitely many 3-primes. This thesis has drawn the connections between mesa partitions and factorizations, analogous to how the politeness of a number is determined by the number of its odd divisors. However, a more rigorous treatment of this topic in terms of classical partition theory and q-series is in order.

Instead, we will mention another possible approach to resolving the cardinality of the 3-primes. Recalling (2.3), and substituting notation to get

$$\langle x, y, z \rangle = xy + yz + xz - x - y - z + 1,$$

we may recognize this more familiarly as a *inhomogeneous ternary quadratic form*, when considered as a polynomial over $\mathbb{Z}^3$. These polynomials are said to be *almost universal* when they are capable of representing all but finitely many natural numbers. The classification of almost universal inhomogeneous ternary quadratic forms has

been performed by Haensch.[7] In our case, we have an *indefinite* quadratic form since the quadratic part can be represented as

$$x^T Q x$$

where

$$Q = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

which has eigenvalues $\lambda = -1, \frac{-1 \pm i\sqrt{3}}{2}$, again revealing our connection with the Eisenstein integers. There do certainly exist almost universal inhomogeneous indefinite ternary quadratic forms, but in order to conclude the cardinality of the 3-primes we would be adding the additional restriction of requiring all of $x$, $y$ and $z$ to be positive, not more than one of which can be equal to one. There doesn't seem to be a tidy theorem in extant literature that resolves such cases, so any conclusions from this line of attack would require a more specific treatment of such quadratic forms.

As a final note, we mention that as the arity of our operation $\circledast_n$ increases, the list of $n$ primes is reduced further and further. For instance, $\langle 2, 2, 2, 2 \rangle = 11$. Hence, if there are infinitely many 3-primes, we may ask the question of whether there exists an $n \in \mathbb{N}$ such that there are only finitely many $n$-primes.

# A

# The Quadratic Form

This section is dedicated to the proof of the formula for $\circledast_n$ as an inhomogeneous $n$-ary quadratic form given below, where $n \geq 2$.

$$\langle m_1, m_2, \ldots, m_n \rangle = \sigma_2(m_1, m_2, \ldots, m_n) - (n-2)\sigma_1(m_1, m_2, \ldots, m_n) + \frac{(n-1)(n-2)}{2} \tag{A.1}$$

It was described at the end of Chapter 2 why such a symmetric quadratic representation should be possible. It remains to prove the value of the coefficients of each symmetric polynomial, including the constant term which goes with $\sigma_0$.

First we prove that the coefficient of $\sigma_2$ is 1, i.e. that each pair of products $m_i m_j$ appears exactly once

after cancellations in the expansion of $\circledast_n$, where $n$ is at least two (otherwise the product is undefined). We proceed here by induction. In the base case, we have trivially that $\langle m_1 m_2 \rangle = m_1 m_2$ and the formula is valid. Now assume that the formula is valid for all $\circledast_k$ where $k \leq n$. We will prove that this implies that the coefficient of $\sigma_2$ in the quadratic form of $\circledast_{n+1}$ is 1. Recall from the definition of $n$-ary multiplication and equation (2.13) that $\circledast_{n+1}$ is an alternating sum of symmetric polynomials of $k$-products $\circledast_k$ where $k \leq n$. We can then fix an arbitrary product pair $m_i m_j$ and determine its coefficient in the quadratic form of $\circledast_{n+1}$ by calculating the sum of its coefficients over all of the $\circledast_k$ products in which it appears. By our induction hypothesis, the pair has coefficient 1 in the quadratic form of every $k$-product, where $k$ ranges from 2 to $n$. The sign of the symmetric polynomial of $k$-products alternates and is positive when $k = n$. Furthermore, for each symmetric polynomial of $\circledast_k$ products, the pair will appear in $\binom{n-1}{k-2}$ of the terms of the sum in (2.13) corresponding to choosing the other $(k-2)$ elements for a $k$-product from out of the $(n-1)$ other distinct $m_i$. . Hence, the coefficient of that pair in the quadratic form can be expressed as the sum,

$$\sum_{k=2}^{n} (-1)^{n-k} \binom{n-1}{k-2} \tag{A.2}$$

which can be re-indexed as

$$\sum_{j=0}^{n-2} (-1)^{n-j} \binom{n-1}{j}. \tag{A.3}$$

Since $(-1)^{n-j}\binom{n-1}{j}$ evaluates to $-1$ when $j = n-1$, we can write (A.3) as

$$1 + \sum_{j=0}^{n-1} (-1)^{n-j} \binom{n-1}{j}. \tag{A.4}$$

The we may recall the well-known identity,

$$\sum_{j=0}^{n} (-1)^j j \binom{n}{j} = 0. \tag{A.5}$$

Since the positive terms and the negative terms balance each other exactly, it doesn't matter where the alternation begins. Then, we can see that the summation on the right of (A.4) is equal to 0, and hence the coefficient of our arbitrary pair is the remaining 1. Since, the choice of $m_i m_j$ is arbitrary, every possible pair has the same coefficient (the quadratic form is still a symmetric polynomial), and hence $\sigma_2$ has a coefficient of 1 in the quadratic from of $\circledast_{n+1}$.

We may prove that $\sigma_1$ has a coefficient of $-(n-2)$ in the quadratic form of $\circledast_n$ along very similar lines. Here, we can even say that this fact extends to the base case $n = 1$, where $\langle m \rangle = m = \sigma_1(m)$. Again, proceeding by strong induction, assume that $\circledast_k$ obeys (A.1) so that the coefficient of $\sigma_k$ is $-(k-2)$ for all $k \leq n$. We will prove that an arbitrary operand $m$ appears with coefficient $-(n-1)$ in the quadratic form of $\circledast_{n+1}$. Such an element will appear in $\binom{n}{k-1}$ distinct $k$-products corresponding to the choices of $(k-1)$ other elements from the set of $n$ other operands. Each in each one of these it will have coefficient $-(k-2)$, which alternates down from $n$. Hence the sum of coefficients can be written

$$\sum_{k=1}^{n} (-1)^{n-k-1} \binom{n}{k-1} (k-2) \tag{A.6}$$

which can be re-indexed and rearranged as

$$\begin{aligned}\sum_{j=0}^{n-1} (-1)^{n-j} \binom{n}{j} (j-1) &= \sum_{j=0}^{n-1} (-1)^{n-j} j \binom{n}{j} + \sum_{j=0}^{n-1} (-1)^{n-j-1} \binom{n}{j} \\ &= -n + \sum_{j=0}^{n} (-1)^{n-j} j \binom{n}{j} + 1 + \sum_{j=0}^{n} (-1)^{n-j-1} \binom{n}{j}\end{aligned}$$

to which we may apply the identity (A.5) and another well-known identity, $\sum_{j=0}^{n} (-1)^j \binom{n}{j} = 0$ to discover that both of the summations above drop out leaving us with $-n + 1 = -(n-1)$ as desired.

Finally, we may prove the value of the constant term (or the coefficient of $\sigma_0$) which is

$$\frac{(n-1)(n-2)}{2} = \binom{n-1}{2} \tag{A.7}$$

for $\circledast_n$. Again we proceed by induction. In the base case, for $n = 1$, the constant term is $\frac{(1-1)(1-2)}{2} = 0$ which holds since $\circledast_1$ is just the identity map. We assume that (A.7) gives the value of the constant term for all $\circledast_k$, $k \leq n$. We will prove that the constant term in the quadratic form of $\circledast_{n+1}$ is $\frac{n(n-1)}{2}$. By the induction hypothesis, each $\circledast_k$ product contributes a constant of $\binom{k-1}{2}$, and there are $\binom{n+1}{k}$ of these corresponding to all choices of $k$ operands from the list of $(n+1)$. They alternate over $k$, and are positive when $k = n$. Finally, $\sigma_0(m_1, m_2, \ldots, m_n)$ enters as $(-1)^n$. We can then write the total value of the constant term as

$$(-1)^n + \sum_{k=1}^{n} (-1)^{n-k} \binom{n+1}{k} \binom{k-1}{2} \tag{A.8}$$

which can be rewritten using the recursive formula $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ to give

$$(-1)^n + \sum_{k=1}^{n}(-1)^{n-k}\binom{n}{k-1}\binom{k-1}{2} + \sum_{k=1}^{n}(-1)^{n-k}\binom{n}{k}\binom{k-1}{2}. \tag{A.9}$$

We can re-index the first summation as

$$\sum_{j=0}^{n-1}(-1)^{n-j-1}\binom{n}{j}\binom{j}{2} \tag{A.10}$$

and apply the identity[1]

$$\sum_{j=0}^{n}(-1)^{j}\binom{n}{j}\binom{j}{m} = 0 \tag{A.11}$$

to get that (A.9) is equal to

$$(-1)^n + \frac{n(n-1)}{2} + \sum_{k=1}^{n}(-1)^{n-k}\binom{n}{k}\binom{k-1}{2}. \tag{A.12}$$

By another application of the recursive formula for binomial coefficients, we have that

$$\binom{k-1}{2} = \binom{k}{2} - \binom{k-1}{1} = \binom{k}{2} - (k-1)$$

so that (A.12) equals

$$(-1)^n + \frac{n(n-1)}{2} + \sum_{k=1}^{n}(-1)^{n-k}\binom{n}{k}\binom{k}{2} + \sum_{k=1}^{n}(-1)^{n-k-1}\binom{n}{k}(k-1). \tag{A.13}$$

We can then absorb the leading $(-1)^n$ into the second summation, and use that $\binom{0}{2} = 0$ to write this as,

$$\frac{n(n-1)}{2} + \sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}\binom{k}{2} + \sum_{k=0}^{n}(-1)^{n-k-1}\binom{n}{k}(k-1). \tag{A.14}$$

Then the first summation is zero by the identity (A.11) and the second summation can be shown to vanish as well by splitting it and applying (A.5) and the other alternating sum identity for binomial coefficients. All that is left is $\frac{n(n-1)}{2}$, as desired. This concludes the proof of the constant term of $\circledast_n$, and of (A.1).

# References


[1] Arthur T. Benjamin and Jennifer J. Quinn, *An alternate approach to alternating sums: A method to die for*, The College Mathematics Journal 39 (2008), no. 3, 191–201.

[2] Andrzej Borowiec, Wieslaw A. Dudek, and Steven Duplij, *Basic concepts of ternary hopf algebras*, Journal of Kharkov National University - Nuclei, Particles and Fields 529 (2001), no. 3(15), 21–29.

[3] H. S. M. Coxeter, *Introduction to geometry*, 2nd ed., Wiley, March 1989.

[4] Wilhelm Dorntë, *Untersuchungen über einen verallgemeinerten gruppenbegriff*, Mathematische Zeitschrift (1929), no. 1, 1–19.

[5] Wieslaw A. Dudek, *Remarks to glazek's results on n-ary groups*, Discussiones Mathematicae - General Algebra and Applications 27 (2007), no. 199-233.

[6] Wieslaw A. Dudek and Vladimir V. Mukhin, *On n-ary semigroups with adjoint neutral element*, Quasigroups and Related Systems 14 (2006), 163–168.

[7] Anna Haensch, *A characterization of almost universal ternary quadratic forms with odd prime power conductor*, Journal of Number Theory 141 (2014), 202–213.

[8] Ellen Jochemsz and Alexander May, *Advances in cryptology - asiacrypt 2006*, Lecture Notes in Computer Science, vol. 4284, ch. A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA Variants, pp. 267–282, Springer Berlin Heidelberg, 2006.

[9] Emil. L. Post, *Polyadic groups*, Transactions of the American Mathematical Society 48 (1940), 208–350.

# Vita

The author was born in Philadelphia and attended secondary school in Vermont. After completing an undergraduate degree in Montreal, he moved to New Orleans in 2012 and enrolled at the University of New Orleans the following year. A proud product of the public education systems of the United States and Canada, he is reluctant and grateful to be pursuing a doctorate Tulane University beginning in fall of 2015, where he plans to continue his current line of research.