

Constructing Numbers From First Principles

Brett Saiki

November 2021

This paper explores previous works in constructing the various sets of numbers seen throughout mathematics: the set of natural numbers (\mathbb{N}), the set of integers (\mathbb{Z}), the set of rational numbers (\mathbb{Q}), the set of real numbers (\mathbb{R}), the set of complex numbers (\mathbb{C}). In addition, I will briefly mention the more exotic number sets like the quaternions (\mathbb{H}), the octonians (\mathbb{O}), and the sedonians (\mathbb{S}). In each section, I will cover a set of numbers and its construction from various sources, providing some commentary along the way. While not intended to be fully rigorous, definitions, theorems and proofs will be provided to give the reader some formal understanding of these sets.

1 Review of Sets

To begin, we will briefly revisit properties of sets. A *set* is an unordered collection of distinct objects, called *elements*. Set theory is the standard foundation of all branches of mathematics, so it is only reasonable to begin with sets. We will first review the basic operations on sets.

Given two sets A and B , we have five operations: The *union* $A \cup B$ is the set of all members of A or B or both. The *intersection* $A \cap B$ is the set of the members of both A and B . In the case that $A \cap B$ has no elements, A and B are said to be *disjoint*. The *set difference* $A \setminus B$ is the set of all members belonging to A but not in B . The *symmetric difference* $A \Delta B$ is the set of all members in A or B but not both. It can be easily shown that $A \Delta B = (A \setminus B) \cup (B \setminus A)$. The *cartesian product* $A \times B$ is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$.

Fix a universal set U and let A be a subset of U . The *complement* of A is the set of all elements of U that do not belong to A , and is denoted by A^c , A' , or \bar{A} . Combining the complement with union and intersection, we have a pair of identities:

Lemma 1.1 (DeMorgan's Laws). Fix a universal set U and let $A, B \subseteq U$.

$$(A \cup B)' = A' \cap B', \quad (1.1)$$

$$(A \cap B)' = A' \cup B'. \quad (1.2)$$

The identities above can be generalized for $n \geq 2$ sets:

$$\left(\bigcup_{i=0}^n A_i \right)' = \bigcap_{i=0}^n A_i', \quad (1.3)$$

$$\left(\bigcap_{i=0}^n A_i \right)' = \bigcup_{i=0}^n A_i'. \quad (1.4)$$

Since set theory is commonly used as a foundational system for mathematics, various formalizations of sets have been developed to varying degrees of success (see Russell's paradox or Cantor's Paradox). The most common axiomatic system for set theory is *Zermelo-Fraenkel* (ZF) set theory which is often bundled with the axiom of choice, in which case, it is called ZFC set theory. The axioms are provided below for reference.

Definition 1.2 (Zermelo-Fraenkel Axioms).

- (1) *Axiom of Extensionality.* If X and Y have the same elements, then $X = Y$.
- (2) *Axiom of Pairing.* For any a and b , there exists a set $\{a, b\}$ that contains exactly a and b .
- (3) *Axiom of Subsets.* Let ϕ be a unary predicate. For any X , there exists a set $Y = \{u \in X : \phi(u)\}$.
- (4) *Axiom of Union.* For any X , there exists a set $Y = \bigcup X$, the union of all elements of X .
- (5) *Axiom of the Power Set.* For any X , there exists a set $Y = P(X)$, the set of all subsets of X .
- (6) *Axiom of Infinity.* There exists an infinite set; there exists a set S such that for all $x \in S$, $x \cup \{x\} \in S$.
- (7) *Axiom of Replacement.* If F is a function, then for any X there exists a set $Y = F[X] = \{F(x) : x \in X\}$.
- (8) *Axiom of Foundation.* Given a nonempty set S , there exists $x \in S$, such that $x \cap S$ is empty.

Definition 1.3 (Axiom of Choice). Given any set of mutually, disjoint, nonempty sets, there exists at least one set that contains exactly one element in common with each of the nonempty sets.

We call the set with no elements the *empty set*, and denote it by \emptyset . By the Axiom of Extensionality, two sets are equal if they have the same elements. As a result, there is only one set with no elements, so the empty set is unique. The empty set has the following properties.

Lemma 1.4. Let A be any set.

- (i) $\emptyset \subseteq A$;
- (ii) $A \cup \emptyset = A$;
- (iii) $A \cap \emptyset = \emptyset$;
- (iv) $A \times \emptyset = \emptyset$.

From (i), we can conclude that the only subset of the empty set is itself. In addition, we have the following:

Lemma 1.5. Let P be a property. A set S is the empty set if and only if the following are true:

- (i) For every element of S , P holds;
- (ii) There is no element of S for which P holds.

2 The Natural Numbers

The natural numbers are the first set of numbers we learn about in life; they are the counting numbers as we use them every day to record the number of a type of objects. This paper will use the symbol \mathbb{N} to denote the natural numbers including the number zero. Because natural numbers are so rudimentary, it is difficult to formalize them without declaring certain axioms. One of these constructions is based on the Peano axioms (also Dedekind-Peano axioms). These axioms are named after the Italian mathematician Giuseppe Peano from his 1889 treatise titled “Arithmetices principia, nova methodo exposita” (The Principles of Arithmetic, Presented by a New Method).

The Peano axioms, in modern formulations, define the properties of natural numbers *including* zero. (In his original work, Peano started with the constant 1 instead of 0.) They consist of only two basic symbols: the constant 0 and the unary function S called the *successor function*.

Definition 2.1 (Peano Axioms).

- (1) 0 is a natural number.
- (2) For every natural number x , $x = x$; equality is reflexive.
- (3) For all natural number x and y , if $x = y$ then $y = x$; equality is symmetric.
- (4) For all natural numbers x , y , and z , if $x = y$ and $y = z$, then $x = z$; equality is transitive.

- (5) For all a and b if b is a natural number and $a = b$, then a is also a natural number; the natural numbers are closed under equality.
- (6) For every natural number n , $S(n)$ is a natural number; the natural numbers are closed under S .
- (7) For all natural numbers m and n , $m = n$ if and only if $S(m) = S(n)$; S is an injection.
- (8) For every natural number n , $S(n) = 0$ is false; there is no natural number whose successor is 0.

Often, axioms 2-5 are ignored since they are the result of equality being well-defined for the natural numbers. Induction is a direct result of these axioms and is sometimes included as the ninth axiom, the *axiom of induction*.

Definition 2.2 (Induction Axiom). Let φ be a unary predicate defined for all natural numbers. If $\varphi(0)$ is true and for every natural number n , $\varphi(n)$ implies $\varphi(S(n))$, then $\varphi(n)$ must be true for all $n \in \mathbb{N}$.

With the element 0 and the successor function, all natural numbers can be constructed. We define the element 1 to be the successor of 0, the element 2 to be the successor of 1, and so on. In the context of set theory, the number 0 and the successor function become more concrete. Let the number 0 be the empty set \emptyset . Then the successor of each natural number $n \in \mathbb{N}$ is defined by $S(n) = n \cup \{n\}$. That is,

$$\begin{aligned} 1 &= \{\emptyset\} = \emptyset \cup \{\emptyset\} = 0 \cup \{0\} = S(0), \\ 2 &= \{\emptyset, \{\emptyset\}\} = \{\emptyset\} \cup \{\{\emptyset\}\} = 1 \cup \{1\} = S(1), \end{aligned}$$

and so on.

Definition 2.3. Addition (+) maps two natural number $a, b \in \mathbb{N}$ to another natural number. It is defined by

$$a + 0 = a \tag{2.5}$$

$$a + S(b) = S(a + b). \tag{2.6}$$

Since adding some $n \in \mathbb{N}$ by 0 produces n , 0 is the left-identity element of \mathbb{N} under addition. (By Theorem 2.6, it is also the right-identity, and thus, just the identity element.)

Theorem 2.4. Addition is well defined for the natural numbers.

Proof. Let $m \in \mathbb{N}$ be any natural number and let T be the set of all $n \in \mathbb{N}$ for which $m + n$ is defined. We will prove by induction that T is in fact \mathbb{N} , that is, addition is well-defined for natural numbers. Since $m + 0$ is defined, $0 \in T$. Next, assume $n \in T$. Since $S(m + n) = m + S(n)$ and $m + n$ is defined, $m + S(n)$ is in T , that is $S(n) \in T$. By induction, $T = \mathbb{N}$, so addition of $m + n$ is defined for all $n \in \mathbb{N}$ and all $m \in \mathbb{N}$ since m was arbitrary. □

Lemma 2.5. For $a, b \in \mathbb{N}$, $m + S(n) = S(m + n)$.

Proof. We will prove by induction. For $b = 0$,

$$a + S(0) = S(a + 0) = S(a) + 0.$$

Assume that $a + S(b) = S(a + b)$ holds for some $b \geq 0$. For $b + 1 = S(b)$,

$$a + S(b + 1) = a + S(S(b)) = S(a + S(b)) = S(S(a + b)) = S(a + b) + 1 = S(a + S(b)).$$

Since it holds for the next case, this property must hold for all natural numbers. □

Theorem 2.6. For $a, b, c \in \mathbb{N}$, $a + (b + c) = (a + b) + c$.

Proof. We will prove by induction. We first show that this property holds for $c = 0$. By the definition of addition,

$$(a + b) + 0 = a + b = a + (b + 0).$$

Now assume that the property holds for some $c \geq 0$. By similar reasoning,

$$(a + b) + S(c) = S((a + b) + c) = S(a + (b + c)) = a + S(b + c) = a + (b + S(c))$$

Therefore, this property must hold for every triple of natural numbers. □

Theorem 2.7. For $a, b \in \mathbb{N}$, $a + b = b + a$.

Proof. We will prove by induction on both a and b . First let $b = 0$. For $a = 0$, the equation is tautologically true. Assume $a + 0 = 0 + a$ holds true for some $a \geq 0$. Applying the results of the previous lemma,

$$S(a) + 0 = a + S(0) = S(a + 0) = S(0 + a) = 0 + S(a).$$

Thus, the equation holds true if a is any natural number. Now assume that $a + b = b + a$ holds true for some $b \geq 0$ and consider the equation for $b + 1 = S(b)$:

$$a + S(b) = S(a + b) = S(b + a) = b + S(a) = S(b) + a.$$

The equation is still true, so this property must hold for all pairs of natural numbers. □

Definition 2.8. Multiplication (\cdot) maps two natural number $a, b \in \mathbb{N}$ to another natural number. It is defined by

$$a \cdot 0 = 0 \tag{2.7}$$

$$a \cdot S(b) = a + (a \cdot b). \tag{2.8}$$

Theorem 2.9. Multiplication is well defined for the natural numbers.

Proof. Let $m \in \mathbb{N}$ be any natural number and let T be the set of all $n \in \mathbb{N}$ for which $m + n$ is defined. We will prove by induction that T is in fact \mathbb{N} , that is, addition is well-defined for natural numbers. Since $m \cdot 0$ is defined, $0 \in T$. Next, assume $n \in T$. Since $m + (m \cdot n) = m \cdot S(n)$ and $m \cdot n$ is defined, $m \cdot S(n)$ is in T , that is $S(n) \in T$. By induction, $T = \mathbb{N}$, so addition of $m \cdot n$ is defined for all $n \in \mathbb{N}$ and all $m \in \mathbb{N}$ since m was arbitrary. □

Corollary 2.10. For every natural number a , $a \cdot 1 = a$. That is, 1 is the right-identity element of \mathbb{N} under multiplication. (By Theorem 2.15, it is also the left-identity element, and thus, just the identity element.)

Proof. The successor of 0 is 1, so

$$a \cdot 1 = a \cdot S(0) = a + (a \cdot 0) = a + 0 = a$$

□

Lemma 2.11. For $a, b, c \in \mathbb{N}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Proof. We will prove by induction on c . We first show that this property holds for $c = 0$, By the definitions of addition and multiplication,

$$a \cdot (b + 0) = a \cdot b = (a \cdot b) + 0 = (a \cdot b) + (a \cdot 0).$$

Now assume that the property holds for some $c \geq 0$. Using Theorem 2.6 and Theorem 2.7,

$$a \cdot (b + S(c)) = a \cdot S(b + c) = a + a \cdot (b + c) = (a \cdot b + a \cdot c) + a = a \cdot b + (a \cdot c + a) = a \cdot b + (a + a \cdot c) = a \cdot b + a \cdot S(c).$$

Since the property is true for $S(c)$ and c was arbitrary, it must also hold for every triple of natural numbers. \square

Theorem 2.12. For $a, b, c \in \mathbb{N}$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Proof. We will prove by induction. We first show that this property holds for $c = 0$ By definition of multiplication,

$$(a \cdot b) \cdot 0 = 0 = a \cdot 0 = a \cdot (b \cdot 0).$$

Now assume that the property holds for some $c \geq 0$. From Lemma 2.11,

$$(a \cdot b) \cdot S(c) = (a \cdot b) + ((a \cdot b) \cdot c) = (a \cdot b) + (a \cdot (b \cdot c)) = a \cdot (b + b \cdot c) = a \cdot (b \cdot S(n)).$$

Since the property is true for $S(c)$ and c was arbitrary, it must also hold for every triple of natural numbers. \square

Lemma 2.13. For $a \in \mathbb{N}$, $0 \cdot a = 0$.

Proof. We will prove by induction on b . We first show that this property holds for $b = 0$:

$$0 \cdot 0 = 0$$

Now assume that the property holds for some $b \geq 0$.

$$0 \cdot S(a) = 0 + \cdot(0 \cdot a) = 0 + 0 = 0$$

Since the property is true for $S(a)$ and a was arbitrary, it must also hold for every natural number. \square

Lemma 2.14. For $a, b \in \mathbb{N}$, $S(a) \cdot b = a \cdot b + b$.

Proof. We will prove by induction on b . We first show that this property holds for $b = 0$:

$$S(a) \cdot 0 = 0 = 0 + 0 = x \cdot 0 + 0.$$

Now assume that the property holds for some $b \geq 0$. Using Theorem 2.6 and Theorem 2.7,

$$\begin{aligned} S(a) \cdot S(b) &= S(a) \cdot b + S(a) \\ &= (a \cdot b + b) + S(a) \\ &= S((a \cdot b + b) + a) \\ &= S(a \cdot b + (b + a)) \\ &= S(a \cdot b + (a + b)) \\ &= S((a \cdot b + a) + b) \\ &= (a \cdot b + a) + S(b) \\ &= a \cdot S(b) + S(b). \end{aligned}$$

\square

Theorem 2.15. For $a, b \in \mathbb{N}$, $a \cdot b = b \cdot a$.

Proof. We will prove by induction on b . We first show that this property holds for $b = 0$. Using Lemma 2.13,

$$a \cdot 0 = 0 = 0 \cdot a.$$

Now assume that the property holds for some $b \geq 0$. Using Lemma 2.14,

$$a \cdot S(b) = a + (a \cdot b) = a + (b \cdot a) = (b \cdot a) + a = S(a) \cdot b$$

Since the property is true for $S(b)$ and b was arbitrary, it must also hold for every pair of natural numbers. \square

3 The Integers

The integers are the next set of numbers after the natural numbers. They are the smallest algebraic group and ring containing the natural numbers. This paper will use the symbol \mathbb{Z} to denote the integers, and will abuse notation by using the symbols $+$ and \cdot for addition and multiplication for natural numbers and integers. The main features of the integers is the existence of negative numbers, numbers that are less than 0, and the subtraction operator.

Before constructing the integers, we will consider pairs of natural numbers (a, b) and their associated solutions to the equation $a + x = b$. Then we will construct an equivalence relation on $\mathbb{N} \times \mathbb{N}$ and prove that $\mathbb{N} \times \mathbb{N}$ modulo the equivalence relation is the set of all integer numbers.

Definition 3.1. For (a, b) and $(c, d) \in \mathbb{N} \times \mathbb{N}$, we define a relation $(a, b) \simeq (c, d)$ if and only if $a + d = b + c$.

Theorem 3.2. The relation \simeq is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.

Proof. Suppose $(a, b), (c, d), (e, f) \in \mathbb{N} \times \mathbb{N}$. Since $a + b = b + a$, $(a, b) \simeq (a, b)$, so \simeq is reflexive. If $(a, b) \simeq (c, d)$, then $(c, d) \simeq (a, b)$ because $a + d = b + c$, then $c + b = d + a$ by Theorem 2.7. Therefore, \simeq is symmetric. Now suppose that $(a, b) \simeq (c, d)$ and $(c, d) \simeq (e, f)$. That is $a + d = b + c$ and $c + f = d + e$. If we add $e + f$ to both sides of the first equation and apply commutativity and associativity, then we get

$$\begin{aligned} a + d + (e + f) &= b + c + (e + f) \\ (a + f) + (d + e) &= (b + e) + (c + f) \end{aligned}$$

Then if we substitute $d + e$ for $c + f$, we get

$$(a + f) + (d + e) = (b + e) + (d + e)$$

Therefore, $a + f = b + e$ or $(a, b) \simeq (e, f)$. That is, \simeq is transitive. \square

If we consider the equivalence classes of $\mathbb{N} \times \mathbb{N}$ under \simeq , we find that each class $[(a, b)]$ represents the same solution to the equation $a + x = b$ for every pair of natural numbers within that equivalence class. For every equivalence class, we can define a canonical representation of that class.

Theorem 3.3. Every equivalence class $[(a, b)]$ contains an ordered pair with at least one 0 coordinate. Therefore every equivalence class can be written either as $[(0, k)]$ or $[(k, 0)]$ for some $k \in \mathbb{N}$. The equivalence class containing $[(0, 0)]$ is the only equivalence class containing an ordered pair with more than one 0 coordinate.

Proof. If $a \leq b$, then there is a $k \in \mathbb{N}$ for which $a + k = b + 0$. Therefore, $(a, b) \simeq (0, k)$, so $[(a, b)] = [(0, k)]$. If $b < a$, then there is a $k \in \mathbb{N}$ for which $b + k = a + 0$. Then $(a, b) \simeq (0, k)$ and $[(a, b)] = [(k, 0)]$. \square

We will let the pair containing one 0 coordinate be the canonical representation of each equivalence class. With the relation \simeq and the canonical representations of each equivalence class, we can finally define the integers.

Definition 3.4. The set of *integers* \mathbb{Z} is given by

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \simeq .$$

That is the integers are the set of solutions to $a + x = b$ for all natural number pairs (a, b) . We can assign convenient names to each of these equivalence classes.

$$\begin{aligned} & \vdots \\ -2 &= [(0, 2)] \\ -1 &= [(0, 1)] \\ 0 &= [(0, 0)] \\ 1 &= [(1, 0)] \\ 2 &= [(2, 0)] \\ & \vdots \end{aligned}$$

We can classify these equivalence classes into three groups. The *negative integers* are the equivalence classes of the form $[(0, k)]$ for $k > 0$. The *positive integers* are those equivalence classes of the form $[(k, 0)]$ for $k > 0$. The integer 0 is neither negative nor positive.

Definition 3.5. We extend addition and multiplication in \mathbb{Z} in the following ways. Suppose $[(a, b)] \in \mathbb{Z}$ and $[(c, d)] \in \mathbb{Z}$. Define addition in \mathbb{Z} to be

$$[(a, b)] + [(c, d)] = [(a + c, b + d)]$$

and define multiplication in \mathbb{Z} to be

$$[(a, b)] \cdot [(c, d)] = [(ac + bd, bc + ad)].$$

Theorem 3.6. Addition in \mathbb{Z} is well-defined.

Proof. Assume that $[(a, b)] = [(c, d)]$ and $[(e, f)] = [(g, h)]$ are integers, that is, $a + d = b + c$ and $e + h = f + g$. Adding the two equations together,

$$\begin{aligned} (a + d) + (e + h) &= (b + c) + (f + g) \\ (a + e) + (d + h) &= (b + f) + (c + g) \end{aligned}$$

The result implies that $[(a + e, b + f)] = [(c + g, d + h)]$ and that addition is well-defined. □

Lemma 3.7. For $x \in \mathbb{Z}$, $0 + x = 0$, i.e 0 is the additive identity element.

Proof. Let $x = [(a, b)]$ be arbitrary. The integer 0 is represented by the equivalence class $[(0, 0)]$. Adding x and 0, we get

$$[(0, 0)] + [(a, b)]$$

□

Theorem 3.8. Addition in \mathbb{Z} is commutative, i.e $x + y = y + x$ for $x, y \in \mathbb{Z}$.

Proof. We use commutativity for natural numbers. For any $[(a, b)], [(c, d)]$ in \mathbb{Z} ,

$$[(a, b)] + [(c, d)] = [(a + c, b + d)] = [(c + a, d + b)] = [(c, d)] + [(a, b)].$$

□

Theorem 3.9. Addition in \mathbb{Z} is associative, i.e $x + (y + z) = (x + y) + z$ for $x, y, z \in \mathbb{Z}$.

Proof. We use associativity for natural numbers. For any $[(a, b)], [(c, d)], [(e, f)]$ in \mathbb{Z} ,

$$\begin{aligned} ([[(a, b)] + [(c, d)]] + [(e, f)]) &= [(a + c, b + d)] + [(e, f)] \\ &= [((a + c) + e, (b + d) + f)] \\ &= [(a + (c + e), b + (d + f))] \\ &= [(a, b)] + [(c + e, d + f)] \\ &= [(a, b)] + ([[(c, d)] + [(d, f)])] \end{aligned}$$

□

Theorem 3.10. Multiplication in \mathbb{Z} is well defined.

Proof. Assume that $[(a, b)] = [(c, d)]$ and $[(e, f)] = [(g, h)]$ are integers, that is, $a + d = b + c$ and $e + h = f + g$. Taking each of the sums and multiplying them by e, f, c, d , we get

$$e(a + d) + f(c + b) + c(e + h) + d(g + f) = e(b + c) + f(a + d) + c(f + g) + d(e + h).$$

where we simply apply the previous equations. Using distributivity, and associativity and commutativity of addition, we get

$$\begin{aligned} e(a + d) + f(c + b) + c(e + h) + d(g + f) &= e(b + c) + f(a + d) + c(f + g) + d(e + h) \\ ae + de + cf + bf + ce + ch + dg + df &= be + ce + af + df + cf + cg + de + df \\ (ae + bf + dg + ch) + (de + cf + ce + df) &= (be + af + cg + dh) + (de + cf + ce + df). \end{aligned}$$

The four right products are the same on either side, so

$$ae + bf + dg + ch = be + af + cg + dh.$$

Reconstructing the integers, we have

$$\begin{aligned} (ae + bf) + (dg + ch) &= (be + af) + (cg + dh) \\ [(ae + bf, be + af)] &= [(cg + dh, dg + ch)] \\ [(a, b)] \cdot [(e, f)] &= [(c, d)] \cdot [(g, h)]. \end{aligned}$$

□

Lemma 3.11. For any $z \in \mathbb{Z}$, $z \cdot 0 = 0$.

Proof. Let $x = [(a, b)]$ be arbitrary. The integer 0 is represented by the equivalence class $[(0, 0)]$. The product of 0 and x is

$$[(0, 0)] \cdot [(a, b)] = [(0 \cdot a + b \cdot 0), (0 \cdot a + 0 \cdot b)] = [(0, 0)].$$

□

Lemma 3.12. For any $x \in \mathbb{Z}$, $1 \cdot x = x$, i.e. 1 is the multiplicative identity element.

Proof. Let x be an arbitrary integer. Either x is positive, negative, or zero. In the case that x is 0,

$$[(1, 0)] \cdot [(0, 0)] = [(1 \cdot 0 + 0 \cdot 0, 0 \cdot 0 + 1 \cdot 0)] = [(1, 0)].$$

In the case that x is positive, we can write $x = [(a, 0)]$ for some natural number a , so

$$[(1, 0)] \cdot [(a, 0)] = [(1 \cdot a + 0 \cdot 0, 0 \cdot a + 1 \cdot 0)] = [(a, 0)].$$

In the case that x is negative, we can write $x = [(0, a)]$ for some natural number a , so

$$[(1, 0)] \cdot [(0, a)] = [(1 \cdot 0 + 0 \cdot a, 0 \cdot 0 + 1 \cdot a)] = [(0, a)].$$

□