THE FUNDAMENTAL THEOREM OF ARITHMETIC IN CONTEXT OF LINEAR ALGEBRA

ÁRPÁD BÉNYI AND BRANKO ĆURGUS

Abstract. We show that the Fundamental Theorem of Arithmetic admits a natural formulation rooted in linear algebra in which the prime numbers serve as a basis for the $\mathbb{Z}$-module of positive rational numbers and factorizations become coordinate representations. This perspective yields a $\mathbb{Z}$-module isomorphism between the positive rationals and the space of integer sequences with finitely many nonzero entries, and reveals that semimodule and lattice structures are preserved. As a direct corollary, we derive a bijection between the positive rational numbers and the positive integers that requires only the concept of the radical of an integer.

1. Student's question about the Fundamental Theorem of Arithmetic

While recently teaching an introductory course in number theory, the first author was asked by a student whether the Fundamental Theorem of Arithmetic is "some sort of mapping between vector spaces." This note originated in making sense of this apparently nonsensical question.

The main protagonists in the Fundamental Theorem of Arithmetic are the positive integers greater than 1,

$$\mathbb{N}\backslash\{1\} = \big\{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \ldots\big\}$$

and the primes

$$\mathbb{P} \ = \big\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots\big\}.$$

Both of these sets are ordered, and for the primes it is convenient to introduce the sequence notation

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ p_6 = 13,\ p_7 = 17,\ p_8 = 19,\ \ldots$$

The Fundamental Theorem of Arithmetic states that for every $n \in \mathbb{N}\backslash\{1\}$ there exists a unique $j \in \mathbb{N}$ and a unique j-tuple $\big(k_1, \ldots, k_j\big)$ of integers in $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$ such that $k_j > 0$ and

$$n = p_1^{k_1} \cdots p_j^{k_j} = \prod_{i=1}^{j} p_i^{k_i}.$$

Thus, the Fundamental Theorem of Arithmetic establishes a bijection between $\mathbb{N}\backslash\{1\}$ and the set of nonzero tuples of nonnegative integers.

2020 *Mathematics Subject Classification.* Primary 11A51, 15A03, 16D70; Secondary 11B75, 06B99.

Key words and phrases. Fundamental Theorem of Arithmetic, $\mathbb{Z}$-module, semimodule, lattice, isomorphism.

Corresponding author: Branko Ćurgus `curgus@wwu.edu`.

To highlight the essence of the Fundamental Theorem of Arithmetic, we restate it as:

> There is a *special subset* of positive integers, called *primes*, such that *every* positive integer can be *uniquely represented* as a *product* of *powers* of those primes.

Students familiar with linear algebra will recognize a parallel concept in vector spaces:

> There is a *special subset* of vectors, called a *basis*, such that *every* vector in the space can be *uniquely represented* as a *sum* of *scalar multiples* of those basis vectors.

For those new to linear algebra, this analogy serves as a bridge to the core concept of a basis, with primes playing the role of a basis for the positive integers. A theorem below makes this correspondence precise.

2. Are there vector spaces in the Fundamental Theorem of Arithmetic?

The representation of exponents in the Fundamental Theorem of Arithmetic as tuples of varying lengths suggests a natural vector space interpretation. This suggestion leads us to the space of real sequences with each having only finitely many nonzero entries, which we will denote by $c_{00}(\mathbb{R})$. This vector space, equipped with standard componentwise operations, is a canonical example in linear algebra; see, for example, [8, Section 1.2, Example 5] or [11, Section 4.1, Example 8]. The tuples of nonnegative integer exponents from the Fundamental Theorem of Arithmetic are embedded in this space by padding each tuple with countably many zeros. This embedding identifies them with the subset $c_{00}(\mathbb{N}_0) \subset c_{00}(\mathbb{R})$.

Since any vector $\mathbf{a} = (k_1, k_2, \ldots) \in c_{00}(\mathbb{N}_0)$ has only finitely many nonzero entries, the infinite product

$$\mathbb{P}^{\mathbf{a}} := \prod_{i \in \mathbb{N}} p_i^{k_i}$$

is a well-defined positive integer. For the zero vector $\mathbf{0} \in c_{00}(\mathbb{N}_0)$, whose entries are all zero, we have an infinite product of ones, so, $\mathbb{P}^{\mathbf{0}} = 1$. In this setting, the Fundamental Theorem of Arithmetic is equivalent to the statement that the function

$$\Phi : \mathbb{N} \to c_{00}(\mathbb{N}_0) \quad \text{defined by} \quad \Phi(n) := \mathbf{a} \quad \text{if and only if} \quad n = \mathbb{P}^{\mathbf{a}}$$

is a bijection. That is, for every $n \in \mathbb{N}$ there exists a unique sequence of exponents $\mathbf{a} \in c_{00}(\mathbb{N}_0)$ such that $n = \mathbb{P}^{\mathbf{a}}$, and conversely for every $\mathbf{a} \in c_{00}(\mathbb{N}_0)$ we have $\mathbb{P}^{\mathbf{a}} \in \mathbb{N}$.

The above formulation situates the range of the bijection $\Phi : \mathbb{N} \to c_{00}(\mathbb{N}_0)$ within the framework of a familiar vector space. To do the same for the domain, we must find a vector space that reflects the multiplicative structure of $\mathbb{N}$. This requires a vector space where vector addition corresponds to ordinary multiplication. Surprisingly, such a vector space exists and is sometimes called an "exotic" vector space, as in [5]. We define this vector space on the set of positive real numbers, $\mathbb{R}_+$, with scalars from the field $\mathbb{R}$. For any vectors $x, y \in \mathbb{R}_+$ and any scalar $\alpha \in \mathbb{R}$, vector addition $\oplus$ and scalar multiplication $\odot$ are defined as

$$x \oplus y = xy, \qquad \alpha \odot x = x^{\alpha}.$$

It is an exercise in linear algebra to verify that $(\mathbb{R}_+, \oplus, \diamond)$ satisfies all the axioms of a real vector space. In this space, the number $1 \in \mathbb{R}_+$ serves as the zero vector, and for a vector $x \in \mathbb{R}_+$, its additive inverse is $1/x \in \mathbb{R}_+$.

The answer to the question posed in this section's title is a definite *yes*. The central protagonist in the Fundamental Theorem of Arithmetic, the set of positive integers $\mathbb{N}$, is embedded in the "exotic" vector space $(\mathbb{R}_+, \oplus, \diamond)$, where multiplication acts as vector addition. On the other side, the exponent tuples, represented as the set $c_{00}(\mathbb{N}_0)$, are a natural subset of the standard vector space $(c_{00}(\mathbb{R}), +, \cdot)$. The Fundamental Theorem of Arithmetic, through the bijection Φ, connects these two algebraic worlds.

In the next section, we will tighten this connection by extending the bijection Φ to a larger domain and range. This extension will naturally lead to narrowing the vector spaces in play to more general algebraic structures known as $\mathbb{Z}$-modules.

3. Φ extended to $\mathbb{Z}$-modules

A weakness of the current setting, as an answer to our student's question, is that the domain and range of the bijection $\Phi : \mathbb{N} \to c_{00}(\mathbb{N}_0)$ are embedded in vector spaces, and are not vector spaces themselves. To narrow the embedding gap, we extend the bijection Φ to the domain $\mathbb{Q}_+$, the set of positive rational numbers, thus extending the range to $c_{00}(\mathbb{Z})$. For arbitrary $m, n \in \mathbb{N}$ we define

$$\Phi_{\text{ex}}(m/n) := \Phi(m) - \Phi(n).$$

That the function $\Phi_{\text{ex}} : \mathbb{Q}_+ \to c_{00}(\mathbb{Z})$ is well-defined is a part of the next theorem.

One key significance of the natural extension Φ_{ex} is that it draws our attention to two new algebraic structures: $\big(\mathbb{Q}_+, \oplus, \diamond\big)$ and $\big(c_{00}(\mathbb{Z}), +, \cdot\big)$. These structures are much closer to being vector spaces than the original domain $\big(\mathbb{N}, \oplus, \diamond\big)$ and range $\big(c_{00}(\mathbb{N}_0), +, \cdot\big)$. The reader can verify that these new structures satisfy all the axioms for a vector space, with the crucial exception that the scalars must be restricted to the ring of integers $\mathbb{Z}$ instead of the field of real numbers $\mathbb{R}$. Such an algebraic structure is called a *module over the ring* $\mathbb{Z}$, or simply a $\mathbb{Z}$-module. The stage is now set for our first theorem.

Theorem 1. *The function $\Phi_{\text{ex}} : \mathbb{Q}_+ \to c_{00}(\mathbb{Z})$ is a $\mathbb{Z}$-module isomorphism. That is, Φ_{ex} is a bijection, and for all $z \in \mathbb{Z}$ and all $r, s \in \mathbb{Q}_+$ we have*

$$\Phi_{\text{ex}}(r \oplus s) = \Phi_{\text{ex}}(rs) = \Phi_{\text{ex}}(r) + \Phi_{\text{ex}}(s) \tag{1}$$

and

$$\Phi_{\text{ex}}(z \diamond r) = \Phi_{\text{ex}}(r^z) = z\, \Phi_{\text{ex}}(r). \tag{2}$$

Proof. Since the restriction of Φ_{ex} to $\mathbb{N}$ is Φ, we reason about Φ first. Given $m, n \in \mathbb{N}$, let $\Phi(m) = \mathbf{a}$ and $\Phi(n) = \mathbf{b}$ with $\mathbf{a}, \mathbf{b} \in c_{00}(\mathbb{N}_0)$. That is, $m = \mathbb{P}^{\mathbf{a}}$ and $n = \mathbb{P}^{\mathbf{b}}$. Then, $mn = \mathbb{P}^{\mathbf{a}+\mathbf{b}}$ or, in terms of Φ,

$$\Phi(m \oplus n) = \Phi(mn) = \Phi(m) + \Phi(n). \tag{3}$$

Note also that for $z \in \mathbb{N}$, $m^z = \mathbb{P}^{z\mathbf{a}}$, that is

$$\Phi(z \diamond m) = \Phi(m^z) = z\, \Phi(m). \tag{4}$$

Now, given $r \in \mathbb{Q}_+$, let $m, n, m', n' \in \mathbb{N}$ be such that $r = m/n = m'/n'$. From $mn' = m'n$ and (3) we obtain

$$\Phi(m) + \Phi(n') = \Phi(m') + \Phi(n) \quad \iff \quad \Phi(m) - \Phi(n) = \Phi(m') - \Phi(n').$$

This shows that Φ_{ex} is a well-defined function.

Next, given $r, s \in \mathbb{Q}_+$, let us write $r = m/n$ and $s = p/q$ with $m, n, p, q \in \mathbb{N}$. Then, using again (3), we obtain

$$\begin{aligned}\Phi_{\text{ex}}(r \oplus s) &= \Phi_{\text{ex}}(rs)\\ &= \Phi(mp) - \Phi(nq)\\ &= \big(\Phi(m) + \Phi(p)\big) - \big(\Phi(n) + \Phi(q)\big)\\ &= \big(\Phi(m) - \Phi(n)\big) + \big(\Phi(p) - \Phi(q)\big)\\ &= \Phi_{\text{ex}}(r) + \Phi_{\text{ex}}(s).\end{aligned}$$

Hence, Φ_{ex} is additive, that is (1) holds.

Since $\Phi_{\text{ex}}(1) = \mathbf{0}$, it follows that $\Phi_{\text{ex}}(0 \odot r) = \Phi_{\text{ex}}(1) = \mathbf{0} = 0\,\Phi_{\text{ex}}(r)$. Let $z \in \mathbb{Z}\backslash\{0\}$. If $z > 0$, using (4) we get

$$\Phi_{\text{ex}}(z \odot r) = \Phi(m^z) - \Phi(n^z) = z\,\Phi(m) - z\,\Phi(n) = z\,\Phi_{\text{ex}}(r),$$

while for $z < 0$ we have

$$\Phi_{\text{ex}}(z \odot r) = \Phi(n^{-z}) - \Phi(m^{-z}) = (-z)\big(-\Phi_{\text{ex}}(r)\big) = z\,\Phi_{\text{ex}}(r).$$

Hence, Φ_{ex} is homogeneous, that is (2) holds.

We prove next that Φ_{ex} is an injective function. Assuming that $\Phi_{\text{ex}}(r) = \Phi_{\text{ex}}(s)$, we get

$$\begin{aligned}\Phi(m) - \Phi(n) = \Phi(p) - \Phi(q) \quad &\iff \quad \Phi(mq) = \Phi(np)\\ &\iff \quad mq = np\\ &\iff \quad r = m/n = p/q = s;\end{aligned}$$

in the second equivalence, we used the injectivity of Φ.

Finally, we prove the surjectivity of Φ_{ex}. Given an arbitrary $\mathbf{c} \in c_{00}(\mathbb{Z})$, let $\mathbf{a}, \mathbf{b} \in c_{00}(\mathbb{N}_0)$ be such that $\mathbf{c} = \mathbf{a} - \mathbf{b}$. Since Φ is surjective, there exist $m, n \in \mathbb{N}$ such that $\mathbf{a} = \Phi(m)$ and $\mathbf{b} = \Phi(n)$. It follows that there exists $m/n \in \mathbb{Q}_+$ such that

$$\mathbf{c} = \Phi(m) - \Phi(n) = \Phi_{\text{ex}}(m/n). \qquad \square$$

Before restating the Fundamental Theorem of Arithmetic in the language of the $\mathbb{Z}$-module $(\mathbb{Q}_+, \oplus, \odot)$, we need a definition, see [7, page 354], whose structure should be familiar from the discussion in the second part of Section 1.

Definition 2. Let $(\mathcal{M}, +, \cdot)$ be a $\mathbb{Z}$-module. A subset $\mathcal{B} \subseteq \mathcal{M}$ is a *basis* for $\mathcal{M}$ if for every nonzero element $v \in \mathcal{M}$ there exist a unique $j \in \mathbb{N}$, unique nonzero elements $\alpha_1, \ldots, \alpha_j \in \mathbb{Z}$, and unique distinct $b_1, \ldots, b_j \in \mathcal{B}$ such that

$$v = \alpha_1 b_1 + \cdots + \alpha_j b_j.$$

If $\mathcal{B}$ is a basis for $\mathcal{M}$, then $\mathcal{M}$ is said to be *free on* $\mathcal{B}$.

Not every $\mathbb{Z}$-module has a basis. In fact, as Artin emphasizes in [2, page 416], "Most modules have no basis." For completeness, we include a simple classical example. Consider $\mathcal{M} = \{0, 1\}$ with addition defined by $0 + 0 = 1 + 1 = 0$ and $0 + 1 = 1 + 0 = 1$, and scalar multiplication is defined for all $z \in \mathbb{Z}$ by $z \cdot 0 = 0$, and $z \cdot 1 = 0$ if z is even, and $z \cdot 1 = 1$ if z is odd. It is straightforward to verify that $\big(\{0, 1\}, +, \cdot\big)$ is a $\mathbb{Z}$-module and $\mathcal{B} = \{0\}$ is not a basis; neither is $\mathcal{B} = \{1\}$ since $1 = 1 \cdot 1 = 3 \cdot 1$, which violates the uniqueness requirement.

The fact that the $\mathbb{Z}$-module $\big(\mathbb{Q}_+, \oplus, \diamond\big)$ is a free module on $\mathbb{P}$ is a part of mathematical folklore, see, for example, [13, Exercise 34, page 147] or [15, Section: Definition and examples]. We show here how it follows from the existence of the module isomorphism Φ_{ex}.

Theorem 3. *The set $\mathbb{P}$ of prime numbers is a basis for the $\mathbb{Z}$-module $\big(\mathbb{Q}_+, \oplus, \diamond\big)$.*

Proof. Recall our notation: $\mathbb{P} = \big\{p_i : i \in \mathbb{N}\big\}$. By the definition of Φ_{ex} and Φ, for every $i \in \mathbb{N}$ we have $\Phi_{\text{ex}}(p_i) = \Phi(p_i) = \mathbf{e}_i$, where $\mathbf{e}_i \in c_{00}(\mathbb{Z})$ has all entries 0 except the i-th, which is 1.

Let $r \in \mathbb{Q}_+$ and $\mathbf{a} = (\alpha_1, \alpha_2, \dots, \alpha_j, 0, 0, \dots) \in c_{00}(\mathbb{Z})$ be arbitrary. Since by Theorem 1, $\Phi_{\text{ex}} : \mathbb{Q}_+ \to c_{00}(\mathbb{Z})$ is a $\mathbb{Z}$-module isomorphism we have $\Phi_{\text{ex}}(1) = \mathbf{a}$ if and only if $\mathbf{a} = \mathbf{0}$, and

$$r = \big(\alpha_1 \diamond p_1\big) \oplus \cdots \oplus \big(\alpha_j \diamond p_j\big) \iff \Phi_{\text{ex}}(r) = \alpha_1\mathbf{e}_1 + \cdots + \alpha_j\mathbf{e}_j \iff \Phi_{\text{ex}}(r) = \mathbf{a} \quad (5)$$

Let $r \in \mathbb{Q}_+\backslash\{1\}$ be arbitrary and set $\mathbf{a} = \Phi_{\text{ex}}(r) \in c_{00}(\mathbb{Z})$. Then $\mathbf{a} \neq \mathbf{0}$; set $\hat{\jmath} \in \mathbb{N}$ to be the cardinality of the set of the nonzero entries in $\mathbf{a}$ and let $\alpha_{i_1}, \dots, \alpha_{i_{\hat{\jmath}}}$ be the nonzero entries of $\mathbf{a}$. By the equivalence (5) we have the unique representation:

$$r = \big(\alpha_{i_1} \diamond p_{i_1}\big) \oplus \cdots \oplus \big(\alpha_{i_{\hat{\jmath}}} \diamond p_{i_{\hat{\jmath}}}\big). \qquad \square$$

At the beginning of this section, we gave a "definition" of a module over the ring $\mathbb{Z}$ just by pointing out its seemingly minor difference from the definition of a vector space over $\mathbb{R}$. Having established Theorem 3, we can now illustrate a major distinction between these algebraic structures. By Theorem 3, the $\mathbb{Z}$-module $\big(\mathbb{Q}_+, \oplus, \diamond\big)$ is infinite-dimensional, as its basis, the set $\mathbb{P}$ of primes, is infinite. At the same time, $\big(\mathbb{Q}_+, \oplus, \diamond\big)$ is embedded in the one-dimensional vector space $\big(\mathbb{R}_+, \oplus, \diamond\big)$ over $\mathbb{R}$.

That the last vector space has dimension one follows from the change of base formula for logarithms. For any vector $x \in \mathbb{R}_+$ and any potential basis vector $b \in \mathbb{R}_+\backslash\{1\}$, for the scalar $\alpha = (\log x)/(\log b) \in \mathbb{R}$ we have

$$x = b^\alpha = \alpha \diamond b.$$

This shows that any single (nonzero) vector $b \in \mathbb{R}_+\backslash\{1\}$ forms a basis for $\big(\mathbb{R}_+, \oplus, \diamond\big)$ over $\mathbb{R}$.

4. A theorem about Φ

We now return to the original function $\Phi : \mathbb{N} \to c_{00}(\mathbb{N}_0)$. Viewing $\mathbb{N}$ as a subset of $\mathbb{Q}_+$ and $c_{00}(\mathbb{N}_0)$ as a subset of $c_{00}(\mathbb{Z})$, and restricting scalars from the ring $\mathbb{Z}$ to the semiring $\mathbb{N}_0$, we no longer have modules but rather *semimodules*. The $\mathbb{N}_0$-semimodules $\mathbb{N}$ and $c_{00}(\mathbb{N}_0)$, with the operations inherited from the modules in Theorem 1, are interesting since each carries an additional lattice structure, and Φ preserves that structure as well. Before proving this in the next theorem, we introduce the lattice orders on $c_{00}(\mathbb{N}_0)$ and $\mathbb{N}$. See [6, Chapter 2] for a detailed introduction to lattices.

We equip $c_{00}(\mathbb{N}_0)$ with the componentwise partial order: for $\mathbf{a} = (\alpha_1, \alpha_2, \dots)$ and $\mathbf{b} = (\beta_1, \beta_2, \dots)$ in $c_{00}(\mathbb{N}_0)$ we set

$$\mathbf{a} \preceq \mathbf{b} \qquad \text{if and only if} \qquad \alpha_i \leq \beta_i \quad \text{for all} \quad i \in \mathbb{N}.$$

With this partial order, $c_{00}(\mathbb{N}_0)$ is a lattice where the *meet* of $\mathbf{a}$ and $\mathbf{b}$ is

$$\mathbf{a} \curlywedge \mathbf{b} = \big(\min\{\alpha_1, \beta_1\}, \min\{\alpha_2, \beta_2\}, \dots\big)$$

and the *join* is

$$\mathbf{a} \curlyvee \mathbf{b} = \big(\max\{\alpha_1, \beta_1\}, \max\{\alpha_2, \beta_2\}, \ldots\big).$$

Thus $c_{00}(\mathbb{N}_0)$ is a semimodule over $\mathbb{N}_0$ and a lattice under componentwise order. The meet and join are characterized as follows: for all $\mathbf{c} \in c_{00}(\mathbb{N}_0)$,

$$\mathbf{c} \preceq \mathbf{a} \ \text{ and } \ \mathbf{c} \preceq \mathbf{b} \quad \Longleftrightarrow \quad \mathbf{c} \preceq \mathbf{a} \curlywedge \mathbf{b}, \tag{6}$$

respectively

$$\mathbf{a} \preceq \mathbf{c} \ \text{ and } \ \mathbf{b} \preceq \mathbf{c} \quad \Longleftrightarrow \quad \mathbf{a} \curlyvee \mathbf{b} \preceq \mathbf{c}. \tag{7}$$

The set $\mathbb{N}$ is also a semimodule over $\mathbb{N}_0$ and a lattice under the partial order introduced by divisibility. For $m, n \in \mathbb{N}$, their meet is $\gcd(m, n)$ and their join is $\operatorname{lcm}(m, n)$.

Theorem 4. *The function $\Phi : \mathbb{N} \to c_{00}(\mathbb{N}_0)$ is an isomorphism of $\mathbb{N}_0$-semimodules and lattices. That is, Φ is a bijection and it has the following properties: For all $m, n \in \mathbb{N}$ and all $z \in \mathbb{N}_0$ we have:*

(a) $\Phi(m \oplus n) = \Phi(mn) = \Phi(m) + \Phi(n)$,

(b) $\Phi(z \diamond n) = \Phi(n^z) = z\,\Phi(n)$,

(c) $m \mid n$ *if and only if* $\Phi(m) \preceq \Phi(n)$,

(d) $\Phi\big(\gcd(m, n)\big) = \Phi(m) \curlywedge \Phi(n)$,

(e) $\Phi\big(\operatorname{lcm}(m, n)\big) = \Phi(m) \curlyvee \Phi(n)$.

Proof. Properties (a) and (b) follow from Theorem 1.

For the proof of (c), it is useful to observe that by the definition of the partial order $\preceq$ in $c_{00}(\mathbb{N}_0)$, for arbitrary $\mathbf{a}, \mathbf{b} \in c_{00}(\mathbb{N}_0)$ we have $\mathbf{a} \preceq \mathbf{b}$ if and only if $\mathbf{b} - \mathbf{a} \in c_{00}(\mathbb{N}_0)$. The next equivalences are straightforward

$$\begin{aligned} m \mid n \quad &\Longleftrightarrow \quad \frac{n}{m} \in \mathbb{N} \\ &\Longleftrightarrow \quad \Phi_{\text{ex}}\Big(\frac{n}{m}\Big) \in c_{00}(\mathbb{N}_0) \\ &\Longleftrightarrow \quad \Phi(n) - \Phi(m) \in c_{00}(\mathbb{N}_0) \\ &\Longleftrightarrow \quad \Phi(m) \preceq \Phi(n). \end{aligned}$$

To prove (d) we use (c), the fact that Φ is a surjection, the characterization in (6), and the following characterization of $\gcd(m, n)$: for all $k \in \mathbb{N}$ the following equivalence holds

$$k \mid m \ \text{ and } \ k \mid n \quad \Longleftrightarrow \quad k \mid \gcd(m, n).$$

Let $\mathbf{c} \in c_{00}(\mathbb{N}_0)$ be arbitrary and let $k \in \mathbb{N}$ be such that $\mathbf{c} = \Phi(k)$. Then, we have

$$\begin{aligned} \mathbf{c} \preceq \Phi\big(\gcd(m, n)\big) \quad &\Longleftrightarrow \quad \Phi(k) \preceq \Phi\big(\gcd(m, n)\big) \\ &\Longleftrightarrow \quad k \mid \gcd(m, n) \\ &\Longleftrightarrow \quad k \mid m \ \text{ and } \ k \mid n \\ &\Longleftrightarrow \quad \Phi(k) \preceq \Phi(m) \ \text{ and } \ \Phi(k) \preceq \Phi(n) \\ &\Longleftrightarrow \quad \mathbf{c} \preceq \Phi(m) \curlywedge \Phi(n). \end{aligned}$$

This proves (d).

The proof of (e) is similar. It uses (c), Φ is a surjection, the characterization in (7), and the following characterization of $\operatorname{lcm}(m,n)$: for all $k \in \mathbb{N}$ the following equivalence holds

$$m \mid k \text{ and } n \mid k \quad \Longleftrightarrow \quad \operatorname{lcm}(m,n) \mid k. \qquad \square$$

5. Bonus: A bijection between $\mathbb{N}$ and $\mathbb{Q}_+$

Since we introduced the two bijections

$$\Phi_{\text{ex}} : \mathbb{Q}_+ \to c_{00}(\mathbb{Z}) \quad \text{and} \quad \Phi : \mathbb{N} \to c_{00}(\mathbb{N}_0),$$

we do not want to miss the opportunity to use them to create a bijection between $\mathbb{N}$ and $\mathbb{Q}_+$ which seems to be missing from the literature. Let

$$\psi : \mathbb{N}_0 \to \mathbb{Z} \quad \text{such that} \quad \psi(0) = 0$$

be a bijection. For example, for all $n \in \mathbb{N}_0$ and all $z \in \mathbb{Z}$ define

$$\psi(n) = (-1)^n \left\lceil \frac{n}{2} \right\rceil \quad \text{and} \quad \psi^{-1}(z) = 2\left|z + \frac{1}{4}\right| - \frac{1}{2}.$$

Then define the bijection

$$\Psi : c_{00}(\mathbb{N}_0) \to c_{00}(\mathbb{Z})$$

by applying $\psi : \mathbb{N}_0 \to \mathbb{Z}$ componentwise. The resulting compositions

$$(\Phi_{\text{ex}})^{-1} \circ \Psi \circ \Phi : \mathbb{N} \to \mathbb{Q}_+ \qquad \text{and} \qquad (\Phi)^{-1} \circ \Psi^{-1} \circ \Phi_{\text{ex}} : \mathbb{Q}_+ \to \mathbb{N} \tag{8}$$

are bijections that are mutual inverses. The first 256 positive rational numbers in the sequence given by the bijection $\mathbb{N} \to \mathbb{Q}_+$ in (8) are shown in Table 1.

Table 1. The first 256 rationals in the enumeration $\mathbb{N} \to \mathbb{Q}_+$ in (8)

1	$\frac{1}{2}$	$\frac{1}{3}$	**2**	$\frac{1}{5}$	$\frac{1}{6}$	$\frac{1}{7}$	$\frac{1}{4}$	**3**	$\frac{1}{10}$	$\frac{1}{11}$	$\frac{2}{3}$	$\frac{1}{13}$	$\frac{1}{14}$	$\frac{1}{15}$	**4**
$\frac{1}{17}$	$\frac{3}{2}$	$\frac{1}{19}$	$\frac{2}{5}$	$\frac{1}{21}$	$\frac{1}{22}$	$\frac{1}{23}$	$\frac{1}{12}$	**5**	$\frac{1}{26}$	$\frac{1}{9}$	$\frac{2}{7}$	$\frac{1}{29}$	$\frac{1}{30}$	$\frac{1}{31}$	$\frac{1}{8}$
$\frac{1}{33}$	$\frac{1}{34}$	$\frac{1}{35}$	**6**	$\frac{1}{37}$	$\frac{1}{38}$	$\frac{1}{39}$	$\frac{1}{20}$	$\frac{1}{41}$	$\frac{1}{42}$	$\frac{1}{43}$	$\frac{2}{11}$	$\frac{3}{5}$	$\frac{1}{46}$	$\frac{1}{47}$	$\frac{4}{3}$
7	$\frac{5}{2}$	$\frac{1}{51}$	$\frac{2}{13}$	$\frac{1}{53}$	$\frac{1}{18}$	$\frac{1}{55}$	$\frac{1}{28}$	$\frac{1}{57}$	$\frac{1}{58}$	$\frac{1}{59}$	$\frac{2}{15}$	$\frac{1}{61}$	$\frac{1}{62}$	$\frac{3}{7}$	**8**
$\frac{1}{65}$	$\frac{1}{66}$	$\frac{1}{67}$	$\frac{2}{17}$	$\frac{1}{69}$	$\frac{1}{70}$	$\frac{1}{71}$	$\frac{3}{4}$	$\frac{1}{73}$	$\frac{1}{74}$	$\frac{5}{3}$	$\frac{2}{19}$	$\frac{1}{77}$	$\frac{1}{78}$	$\frac{1}{79}$	$\frac{4}{5}$
9	$\frac{1}{82}$	$\frac{1}{83}$	$\frac{2}{21}$	$\frac{1}{85}$	$\frac{1}{86}$	$\frac{1}{87}$	$\frac{1}{44}$	$\frac{1}{89}$	$\frac{3}{10}$	$\frac{1}{91}$	$\frac{2}{23}$	$\frac{1}{93}$	$\frac{1}{94}$	$\frac{1}{95}$	$\frac{1}{24}$
$\frac{1}{97}$	$\frac{7}{2}$	$\frac{3}{11}$	**10**	$\frac{1}{101}$	$\frac{1}{102}$	$\frac{1}{103}$	$\frac{1}{52}$	$\frac{1}{105}$	$\frac{1}{106}$	$\frac{1}{107}$	$\frac{2}{9}$	$\frac{1}{109}$	$\frac{1}{110}$	$\frac{1}{111}$	$\frac{4}{7}$
$\frac{1}{113}$	$\frac{1}{114}$	$\frac{1}{115}$	$\frac{2}{29}$	$\frac{3}{13}$	$\frac{1}{118}$	$\frac{1}{119}$	$\frac{1}{60}$	**11**	$\frac{1}{122}$	$\frac{1}{123}$	$\frac{2}{31}$	$\frac{1}{25}$	$\frac{3}{14}$	$\frac{1}{127}$	$\frac{1}{16}$
$\frac{1}{129}$	$\frac{1}{130}$	$\frac{1}{131}$	$\frac{2}{33}$	$\frac{1}{133}$	$\frac{1}{134}$	$\frac{1}{45}$	$\frac{1}{68}$	$\frac{1}{137}$	$\frac{1}{138}$	$\frac{1}{139}$	$\frac{2}{35}$	$\frac{1}{141}$	$\frac{1}{142}$	$\frac{1}{143}$	**12**
$\frac{1}{145}$	$\frac{1}{146}$	$\frac{7}{3}$	$\frac{2}{37}$	$\frac{1}{149}$	$\frac{5}{6}$	$\frac{1}{151}$	$\frac{1}{76}$	$\frac{3}{17}$	$\frac{1}{154}$	$\frac{1}{155}$	$\frac{2}{39}$	$\frac{1}{157}$	$\frac{1}{158}$	$\frac{1}{159}$	$\frac{1}{40}$
$\frac{1}{161}$	$\frac{9}{2}$	$\frac{1}{163}$	$\frac{2}{41}$	$\frac{1}{165}$	$\frac{1}{166}$	$\frac{1}{167}$	$\frac{1}{84}$	**13**	$\frac{1}{170}$	$\frac{3}{19}$	$\frac{2}{43}$	$\frac{1}{173}$	$\frac{1}{174}$	$\frac{5}{7}$	$\frac{4}{11}$
$\frac{1}{177}$	$\frac{1}{178}$	$\frac{1}{179}$	$\frac{6}{5}$	$\frac{1}{181}$	$\frac{1}{182}$	$\frac{1}{183}$	$\frac{1}{92}$	$\frac{1}{185}$	$\frac{1}{186}$	$\frac{1}{187}$	$\frac{2}{47}$	$\frac{1}{63}$	$\frac{1}{190}$	$\frac{1}{191}$	$\frac{8}{3}$
$\frac{1}{193}$	$\frac{1}{194}$	$\frac{1}{195}$	**14**	$\frac{1}{197}$	$\frac{3}{22}$	$\frac{1}{199}$	$\frac{5}{4}$	$\frac{1}{201}$	$\frac{1}{202}$	$\frac{1}{203}$	$\frac{2}{51}$	$\frac{1}{205}$	$\frac{1}{206}$	$\frac{3}{23}$	$\frac{4}{13}$
$\frac{1}{209}$	$\frac{1}{210}$	$\frac{1}{211}$	$\frac{2}{53}$	$\frac{1}{213}$	$\frac{1}{214}$	$\frac{1}{215}$	$\frac{1}{36}$	$\frac{1}{217}$	$\frac{1}{218}$	$\frac{1}{219}$	$\frac{2}{55}$	$\frac{1}{221}$	$\frac{1}{222}$	$\frac{1}{223}$	$\frac{1}{56}$
15	$\frac{1}{226}$	$\frac{1}{227}$	$\frac{2}{57}$	$\frac{1}{229}$	$\frac{1}{230}$	$\frac{1}{231}$	$\frac{1}{116}$	$\frac{1}{233}$	$\frac{3}{26}$	$\frac{1}{235}$	$\frac{2}{59}$	$\frac{1}{237}$	$\frac{1}{238}$	$\frac{1}{239}$	$\frac{4}{15}$
$\frac{1}{241}$	$\frac{11}{2}$	$\frac{1}{27}$	$\frac{2}{61}$	$\frac{7}{5}$	$\frac{1}{246}$	$\frac{1}{247}$	$\frac{1}{124}$	$\frac{1}{249}$	$\frac{1}{50}$	$\frac{1}{251}$	$\frac{6}{7}$	$\frac{1}{253}$	$\frac{1}{254}$	$\frac{1}{255}$	**16**

The second bijection in the last displayed formula, mapping $\mathbb{Q}_+$ to $\mathbb{N}$, has a particularly simple form:

$$\frac{p}{q} \quad \longmapsto \quad \frac{p^2q^2}{\operatorname{rad}(q)},$$

where p and q are relatively prime positive integers and $\operatorname{rad}(q)$ is the radical of q, defined to be the product of the distinct prime divisors of q if $q > 1$, and $\operatorname{rad}(1) = 1$. One can use this formula to determine the position of each rational number in the above table. For example, $2/55$ is at the position $2^2 55^2/(5 \cdot 11) = 220$.

What is the value of this bijection? In [4], Calkin and Wilf state: "It is well known (indeed, as Paul Erdős might have said, every child knows) that the rationals are countable. However, the standard presentations of this fact do not give an explicit enumeration; rather they show how to *construct* an enumeration." The authors of [4] then proceed with a beautiful recursion which leads to their bijection between $\mathbb{N}$ and $\mathbb{Q}_+$. As with most recursions, they are well suited for implementation on a computer, but hard to do on a simple calculator, or even less so by hand; see also [1, 9, 12], and [10, Section 4.5 Relative primality]. In fact, Calkin and Wilf cite Stan Wagon [14], who asked for the numerator of the fraction in the 90,316th position of their enumeration. Equivalently, Wagon's question concerns the number of hyperbinary representations of the integer 90316, an elegant connection that highlights the beauty of the Calkin-Wilf enumeration.

In our bijection, to find the fraction at the 90,316th position requires the prime factorization $90316 = 2^2 \cdot 67 \cdot 337$; then we calculate that it is $2/(67 \cdot 337) = 2/22579$. In fact, given the list of all 168 primes which are smaller than 1000 and a lazy Sunday afternoon, a student could calculate the first 1000 fractions in our bijection with a little help from an old-fashioned calculator.

Even more interestingly, none of the enumerations we have encountered in the literature explores the inverses of the bijections they introduce. And that is where our bijection excels. It turns out that the fraction at the 90,316th position in the Calkin-Wilf enumeration is $843/494$; see the playful numbering of the problem in [14]! At which position is $843/494$ in our bijection? We just need to verify that $494 = 2 \cdot 13 \cdot 19$ is squarefree to calculate that this fraction is at the $843^2 \cdot 494 = 351{,}060{,}606$th position. Furthermore, in our enumeration, with $n \in \mathbb{N}$, the positive rational $n/1$ is at the n^2-th position (shown in boldface in Table 1), while if n is squarefree, the unit fraction $1/n$ can be found at the n-th position.

Although verifying that a large positive integer is squarefree is computationally demanding (see [3]), our bijection is more accessible for "human-sized" integers. While it is less efficient for extremely large inputs, it can serve as an intuitive first step toward understanding the countability of the positive rationals for beginning students of number theory.

A question, in the spirit of [4]: Is there a bijection between $\mathbb{N}$ and $\mathbb{Q}_+$ which, together with its inverse, can be given by a closed-form expression?

6. Declarations

Funding: Árpád Bényi is supported by an AMS-Simons Research Enhancement Grant for PUI Faculty. Branko Ćurgus received no funding.
Author Contributions: Both authors contributed equally.
Corresponding author: Branko Ćurgus.

Conflicts of interest/Competing interests: The authors have no conflicts of interest to declare that are relevant to the content of this article.

References

[1] D. E. Andreev, On a remarkable enumeration of the positive rational numbers. In Russian. Available at ftp://ftp.mccme.ru/users/vyalyi/matpros/i2126134.pdf.zip.

[2] M. Artin, *Algebra*, 2nd ed., Classic Version (Pearson Modern Classics for Advanced Mathematics), Pearson, 2017.

[3] A. R. Booker, G. A. Hiary, and J. P. Keating, Detecting squarefree numbers, Duke Mathematical Journal **164**(2) (2015), 235–275. doi:10.1215/00127094-2856619.

[4] N. Calkin and H. S. Wilf, Recounting the rationals, The American Mathematical Monthly 107 (2000), no. 4, 360–363. JSTOR 2589182.

[5] M. A. Carchidi, Generating exotic-looking vector spaces, The College Mathematics Journal, Vol. 29 (1998), no. 4, 304–308.

[6] B. A. Davey and H. A. Priestley, *Introduction to Lattices and Order*, 2nd ed., Cambridge University Press, 2002.

[7] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., John Wiley & Sons, 2004.

[8] S. H. Friedberg, A. J. Insel, L. E. Spence, *Linear Algebra*, 4th ed., Prentice-Hall, 2002.

[9] J. Gibbons, D. Lester, and R. Bird, Functional pearl: Enumerating the rationals, Journal of Functional Programming 16 (2006), no. 3, 281–291. doi:10.1017/S0956796806005880.

[10] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, 2nd ed., Addison-Wesley, Reading, MA, 1994.

[11] D. C. Lay, S. R. Lay, J. J. McDonald, *Linear Algebra and Its Applications*, 6th ed., Pearson, 2020.

[12] A. Malter, D. Schleicher, and D. Zagier, New looks at old number theory, The American Mathematical Monthly 120 (2013), no. 3, 243–264. doi:10.4169/amer.math.monthly.120.03.243.

[13] C. Musili, *Introduction to Rings and Modules*, Narosa Publishing House, New Delhi, 1992.

[14] S. Wagon, Problem of the Week 843: Sums of powers of two, a problem from *Quantum*, September/October 1997, posted on October 2, 1998. Available at https://stanwagon.com/potw/fall97/p843.html.

[15] Free abelian group. Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Free_abelian_group, accessed September 2, 2025.

Department of Mathematics, Western Washington University, 516 High St, Bellingham, WA 98225, USA

Email address: benyia@wwu.edu

Department of Mathematics, Western Washington University, 516 High St, Bellingham, WA 98225, USA

Email address: curgus@wwu.edu