Prime Factorization and Denumerability: A Function Approach

Efraim P. Armendariz, PhD. †
Mark. L. Daniels, PhD. ‡

Abstract

The uniqueness of prime factorization is utilized in this article to show that certain sets are countably infinite. A consistent "function approach" is used to accomplish this task. The authors feel this is an effective and connected way to present the concept of denumerability to undergraduate mathematics and preservice mathematics majors.

Introduction

The concept of function is a fundamental idea in the study of mathematics. A firm understanding of functions, their construction, and their language should constitute one goal of any course and curriculum designed to introduce mathematics majors to proofs. Typically, such a course follows a calculus sequence and carries a title such as "Sets, Functions, and Relations." Prior to such a course, students encounter functions that are almost always given in closed form, usually involving algebraic expressions that include compositions with transcendental functions. In contrast, an introduction to proof course usually includes exploration of abstract sets and their algebra, distinction between finite and infinite sets, and combinatorial arguments.

Functions play a major role when formulating the distinction between finite and infinite sets as well as countable and uncountable sets. It is here that the use of the special language of functions should be employed consistently, especially regarding the concepts of *injective* (one-to-one) and *surjective* (onto) functions as well as *bijective* (one-to-one and onto) functions.

We will employ the following terminology. A function f from set A to B is *injective* if for all $u, v \in A$ with $u \neq v$, it follows that $f(u) \neq f(v)$, equivalently, if $f(u) = f(v)$ then $u = v$. A function f from set A to B is *surjective* if given $z \in B$ there exists $u \in A$ such that $f(u) = z$. A function f from set A to B is *bijective* if f is both injective and surjective.

Our goal in this article is to show how a consistent approach to defining specific functions can be combined with basic properties of the integers to address questions of finite and infinite and countable versus uncountable. The results presented here are not claimed to be new (see [**1**], [**2**]). Rather, we are stressing the importance of consistency in developing significant concepts that reinforce student learning and understanding. Additionally, the substance of this article can be easily scaffolded so that students can engage in guided discovery exploration of the topic.

Prime Factorization and Denumerability

In what follows, $\mathbb{N}$ denotes the set of positive integers. An infinite set S is *denumerable* if there exists an injective function (i.e., a one-to-one function) $f : S \to \mathbb{N}$.

There exists a well-known proof [**1**] (cf. [**2**]) that makes use of the Uniqueness of Prime Factorization to show that the set $\mathbb{Q}^+$ of positive rational numbers is a denumerable set. Assuming that each positive rational number x is written in the form

$$x = a/b, \quad \text{where } a, b \in \mathbb{N},\ b \neq 0 \text{ and } \gcd(a, b) = 1,$$

we define the function

$$f : \mathbb{Q}^+ \to \mathbb{N} \quad \text{by} \quad f(x) = 2^a 3^b.$$

Uniqueness of Prime Factorization easily leads to a verification that f is an injective function.

In this note, we wish to show how the same idea can be used to establish denumerability of other sets. Before proceeding, we'd like to acknowledge the support of the Educational Advancement Foundation in the preparation of this article.

From classroom experience, the function approach appears to be more appealing to students than the standard "listing and counting along diagonals" approach. In fact, students often try to construct a function that achieves the diagonalization. Describing such a function in closed form can be involved. In presenting this material in the classroom, we also include a preliminary result whose proof makes use of the well ordering property of the integers: *If there exists an injective function from the infinite set S into N, then there exists a bijection from S onto N.* This implies that a denumerable set can be "labeled" by the positive integers.

Proposition 1. *A denumerable union of denumerable sets is denumerable.*

Proof. We are given a denumerable collection $\{A_i : i \in \mathbb{N}\}$ each of which is denumerable. Thus for each $i \in \mathbb{N}$, we can write each set A_i as

$A_{ij} = \left\{ a_{ij} : j \in \mathbb{N} \right\}$. Let S be the disjoint union of the A_i's. The function $f : S \to \mathbb{N}$ given by $f(a_{ij}) = 2^i 3^j$ is an injection.

Although we work with a disjoint union of sets in the proof of Proposition 1, the proof for a general union can now be modified as a good exercise.

The next result is easily verified.

Proposition 2. *Assume* $p_0, p_1, p_2, \dots, p_n$ *are distinct primes and* $a_0, a_1, a_2, \dots, a_n$ *are integers (not necessarily positive). If* $p_0^{a_0} \cdot p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_n^{a_n} = 1$ *then* $a_0 = a_1 = \dots = a_n = 0$.

We can make use of Proposition 2 to show

Proposition 3. *The set* $\mathbb{Z}[x]$ *of all polynomials with integer coefficients is a denumerable set.*

Proof. Let $\left\{ p_0, p_1, p_2, \dots \right\}$ denote the set of all primes. Define $f : \mathbb{Z}[x] \to \mathbb{Q}$ by

$$f\left(a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \right) = p_0^{a_0} \cdot p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_n^{a_n}.$$

Then f is injective by Proposition 2.

An alternate proof that does not make use of Proposition 2 can be given:

Since $\mathbb{Z}$ is a denumerable set, let $\alpha : \mathbb{Z} \to \mathbb{N}$ be an injective function. Then $f : \mathbb{Z}[x] \to \mathbb{N}$ given by

$$f\left(a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \right) = p_0^{\alpha(a_0)} \cdot p_1^{\alpha(a_1)} \cdot p_2^{\alpha(a_2)} \cdot \dots \cdot p_n^{\alpha(a_n)}$$

is an injective function.

An *algebraic real number* is a root of a polynomial in $\mathbb{Z}[x]$. Thus a consequence of Proposition 3 is:

Proposition 4. *The set of all algebraic real numbers is denumerable.*

A result that generalizes Proposition 3 can also be given.

Proposition 5. *Let R be a denumerable ring. Then the polynomial ring $R[x]$ is a countable ring.*

Proof. Use the alternate proof of Proposition 2.

Corollary. *Let R be a denumerable ring and* $X = \left\{ x_i \mid i \in \mathbb{N} \right\}$ be *a set of commuting* *indeterminates. Then* $R[x]$, *the set of all polynomials over R in a finite number of variables, is a denumerable set.*

Proof. Since $R[x] \subseteq R[x_1, x_2] \subseteq \ldots$ the result follows from Propositions 1 and 5.

Summary

In this article we show how the uniqueness of prime factorization can be used to show that certain sets are countably infinite. This is done in a way that utilizes a consistent "function approach" that the authors feel is an effective and connected way to present the concept of denumerability to undergraduate mathematics and preservice mathematics majors.

† *Efraim P. Armendariz, PhD*, University of Texas at Austin, USA
‡ *Mark. L. Daniels, PhD*, University of Texas at Austin, USA

References

1. Aliprantis, C. D., *Principles of real analysis*, ACADEMIC PRESS, 1998.

2. Rapke, Tina, Confronting analysis, *MAA*, *Math Horizons*, September, 2010, 13-15.