Document Tag Lookup Proof Using the Uniqueness of Prime Factorization

Bruce Chidley

January 2023

We prove the following statement:

An integer a evenly divides n when all elements of the prime factorization of a appear in the prime factorization of n. Furthermore, an integer b does *not* evenly divide n if its prime factorization includes some prime numbers that do not exist in the prime factorization of n.

Proof:

Let $n = p_1p_2 \dots p_k$ such that each p_i where $1 \leq i \leq k$ are unique prime numbers, and $p_1p_2 \dots p_k$ represent the unique prime factorization of n.

Next, let $a = q_1q_2 \dots q_l$ where $l \leq k$ represents the unique prime factorization of a. Also, assume that all prime numbers $q_1, q_2, \dots, q_l$ appear in the prime factorization of n.

Clearly, a evenly divides n, since there exists a subset of the prime factorization of n such that the subset is identical to the prime factorization of a. Thus, for n/a, the identical terms will cancel out, and the result will be a string of prime numbers multiplied together, which will be an integer.

Now, let us define some b such that $b = r_1r_2 \dots r_m$ where $m \leq k$ represents the unique prime factorization of b. If there exists some prime number in this factorization that *does not exist* in the prime factorization of n, then b does not evenly divide n.

Proof by contradiction:

Assume that b evenly divides n. This implies that there exists some integer c such that $bc = n$. Since all integers can be written as a unique product of prime numbers, there exists a prime factorization of c. Therefore, we can express bc strictly in terms of prime numbers. However, since $bc = n$, and bc is completely composed of prime numbers such that *at least one prime number* is *not* in n, this would mean that n has two different prime factorizations.

However, this is a contradiction due to the uniqueness of prime factorization, and thus, b does not evenly divide n.

Relevance to Document Tag Lookup:

This relationship is essential for understanding how my solution to the Document Tag Lookup functions. Each tag is represented as a unique prime number.

Therefore, a subset of these tags will consist of some amount of prime numbers. Multiplying them together forms a unique prime factorization for some integer, which can be represented by n in terms of the above proof. From this, we know that each document has associated tags that are also represented by prime numbers. So, in terms of the proof, the product of a document's tags can either be represented by a or b depending on whether its tags are a subset of the greater subset of tags. Thus, it is clear that if the product of a document's tags evenly divide the product of the greater set of tags, the document's tags form a subset of the greater subset of tags.