Translation between 2 worlds

The unique prime factorization provides a family of functions

$$\upsilon_p : \mathbb{Z}_+ \longrightarrow \mathbb{N},$$

where p is a prime number, mapping each positive integer n to the exponent e_p of p in its prime factorization. These functions provide a translator between the following two worlds:

1. positive integers, equipped with multiplication and ordered by the divisibility $|$,
2. natural numbers, equipped with additions and ordered by the natural order $\leqslant$.

Theorem 2.3.1

Let a, b be two positive integers.

1. $a = 1$ *if and only if for all prime* p, $v_p(a) = 0$.
2. $a = b$ *if and only if for all prime* p, $v_p(a) = v_p(b)$.
3. *For all prime* p, $v_p(ab) = v_p(a) + v_p(b)$.
4. $a \mid b$ *if and only if for all prime* p, $v_p(a) \leqslant v_p(b)$.
5. *For all prime* p, $v_p(\gcd(a, b)) = \min\{v_p(a), v_p(b)\}$.
6. *For all prime* p, $v_p(\operatorname{lcm}(a, b)) = \max\{v_p(a), v_p(b)\}$.

The proof

1. $a = 1$ *if and only if for all prime* p, $v_p(a) = 0$.

   Proof. Follows by the prime factorization of 1. □

The proof

1. $a = 1$ *if and only if for all prime* p, $v_p(a) = 0$.

   Proof. Follows by the prime factorization of 1. $\square$

2. $a = b$ *if and only if for all prime* p, $v_p(a) = v_p(b)$.

   Proof. Follows by the uniqueness of prime factorization. $\square$

1. $a = 1$ *if and only if for all prime* p, $v_p(a) = 0$.
   Proof. Follows by the prime factorization of 1. $\square$

2. $a = b$ *if and only if for all prime* p, $v_p(a) = v_p(b)$.
   Proof. Follows by the uniqueness of prime factorization. $\square$

3. *For all prime* p, $v_p(ab) = v_p(a) + v_p(b)$.
   Proof. Follows by the prime factorization and the power rule. $\square$

$$p^{v_p(a)} \cdot p^{v_p(b)} = p^{v_p(a)+v_p(b)}$$

4. *$a \mid b$ if and only if for all prime p, $v_p(a) \leqslant v_p(b)$.*
Proof. ($\Longrightarrow$) Suppose $a \mid b$, say $b = ac$. By 3, for all prime p,

$$v_p(b) = v_p(a) + v_p(c) \geqslant v_p(a).$$

4. $a \mid b$ *if and only if for all prime* p, $v_p(a) \leqslant v_p(b)$.
   Proof. ($\Longrightarrow$) Suppose $a \mid b$, say $b = ac$. By 3, for all prime p,

$$v_p(b) = v_p(a) + v_p(c) \geqslant v_p(a).$$

   ($\Longleftarrow$) Conversely, suppose for all prime p, $v_p(a) \leqslant v_p(b)$, say $v_p(b) = v_p(a) + e_p$. Note that there are only finitely many positive e_p, otherwise there will be infinitely many prime divisors of b, which is impossible.

4. $a \mid b$ *if and only if for all prime* p, $v_p(a) \leqslant v_p(b)$.

Proof. ($\Longrightarrow$) Suppose $a \mid b$, say $b = ac$. By 3, for all prime p,

$$v_p(b) = v_p(a) + v_p(c) \geqslant v_p(a).$$

($\Longleftarrow$) Conversely, suppose for all prime p, $v_p(a) \leqslant v_p(b)$, say $v_p(b) = v_p(a) + e_p$. Note that there are only finitely many positive e_p, otherwise there will be infinitely many prime divisors of b, which is impossible.

Let $c = \prod_p p^{e_p}$, then $v_p(c) = e_p$. By 3, for all prime p,

$$v_p(b) = v_p(a) + e_p = v_p(a) + v_p(c) = v_p(ac).$$

By 2, $b = ac$. Namely, $a \mid b$. $\square$

5. *For all prime* p, $v_p(\gcd(a,b)) = \min\{v_p(a), v_p(b)\}$.
   Proof. Let $g = \gcd(a,b)$. The first defining property says that $g \mid a$ and $g \mid b$. By 4, for all prime p, $v_p(g) \leqslant v_p(a)$ and $v_p(g) \leqslant v_p(b)$.

5. *For all prime* p, $v_p(\gcd(a,b)) = \min\{v_p(a), v_p(b)\}$.

   Proof. Let $g = \gcd(a,b)$. The first defining property says that $g \mid a$ and $g \mid b$. By 4, for all prime p, $v_p(g) \leqslant v_p(a)$ and $v_p(g) \leqslant v_p(b)$. Conversely, suppose e is any natural number smaller than both $v_p(a)$ and $v_p(b)$. By 4, $p^e \mid a$ and $p^e \mid b$. By the second defining property of gcd, $p^e \mid g$. By 4, $e \leqslant v_p(g)$.

5. *For all prime* p, $v_p(\gcd(a,b)) = \min\{v_p(a), v_p(b)\}$.
   Proof. Let $g = \gcd(a,b)$. The first defining property says that $g \mid a$ and $g \mid b$. By 4, for all prime p, $v_p(g) \leqslant v_p(a)$ and $v_p(g) \leqslant v_p(b)$.
   Conversely, suppose e is any natural number smaller than both $v_p(a)$ and $v_p(b)$. By 4, $p^e \mid a$ and $p^e \mid b$. By the second defining property of gcd, $p^e \mid g$. By 4, $e \leqslant v_p(g)$.
   Therefore, $\min\{v_p(a), v_p(b)\} = v_p(g)$. □

5. *For all prime* p, $v_p(\gcd(a,b)) = \min\{v_p(a), v_p(b)\}$.
   Proof. Let $g = \gcd(a,b)$. The first defining property says that $g \mid a$ and $g \mid b$. By 4, for all prime p, $v_p(g) \leqslant v_p(a)$ and $v_p(g) \leqslant v_p(b)$.
   Conversely, suppose e is any natural number smaller than both $v_p(a)$ and $v_p(b)$. By 4, $p^e \mid a$ and $p^e \mid b$. By the second defining property of gcd, $p^e \mid g$. By 4, $e \leqslant v_p(g)$.
   Therefore, $\min\{v_p(a), v_p(b)\} = v_p(g)$. □

6. *For all prime* p, $v_p(\operatorname{lcm}(a,b)) = \max\{v_p(a), v_p(b)\}$.
   Proof. Similar to 5. □

Moreover, the family of functions $v_p : \mathbb{Z}_+ \to \mathbb{N}$ ($p \in \mathbb{P}$) decomposes the Hasse diagram of divisibility of positive integers into individual dimensions: the value of $v_p(n)$ can be viewed as the coordinate of n on the p-axis.

This is analogous to the decomposition of the usual Euclidean space into (three) individual dimensions via the x, y, z-axises.