of n. Suppose that we have another prime factorization

$$n = q_1 q_2 \ldots q_s.$$

It follows that

$$p_1 \mid n \quad \Rightarrow \quad p_1 \mid q_1 q_2 \ldots q_s,$$

and hence Remark 11.2 gives that $p_1 \mid q_i$ for some $i \in \{1, 2, \ldots, s\}$.

Reordering $q_1, q_2, \ldots q_s$ gives that $p_1 \mid q_1$. Since q_1 is a prime, it follows that $p_1 = q_1$. Hence

$$p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s.$$

Continuing the above process gives that $r = s$ and that after reordering,

$$p_i = q_i \quad \forall i \in \{1, 2, \ldots, s\}.$$

□

Corollary 11.4 (Unique Prime Factorization of Integers)**.** *Any integer $n \in \mathbb{Z}$ such that $n \neq 0, \pm 1$ has a* canonical decomposition

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

where $p_1, p_2, \ldots, p_r$ are primes, $1 < p_1 < p_2 < \ldots < p_r$ and

$$\alpha_i \in \mathbb{N} \quad \forall i \in \{1, 2, \ldots, r\}.$$

Remarks 11.5. (1) Suppose that $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ has canonical decomposition $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. Suppose further that $m \in \mathbb{Z} \setminus \{\pm 1\}$ divides n: $m \mid n$. Then m has canonical decomposition

$$m = \pm p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$$

for some $\beta_1, \beta_2, \ldots, \beta_r \in \overline{\mathbb{N}}$ with

$$0 \le \beta_i \le \alpha_i \quad \forall i \in \{1, 2, \ldots, r\}.$$

(2) If $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ and $m = \prod_{i=1}^{r} p_i^{\beta_i}$ where $p_1, p_2, \ldots, p_r$ are primes, $1 < p_1 < p_2 < \ldots < p_r$ and $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_r \in \overline{\mathbb{N}}$, then

$$(m, n) = \prod_{i=1}^{r} p_i^{\min\{\alpha_i, \beta_i\}} \quad \text{(greatest common divisor)},$$

$$[m, n] = \prod_{i=1}^{r} p_i^{\max\{\alpha_i, \beta_i\}} \quad \text{(least common multiple)}.$$