The Fundamental Theorem of Arithmetic

In this post I prove Proposition 2.3.1 and Theorem 2.3.2.

Proposition 1. Let $a \in \mathbb{Z}$ and $a > 1$. Then the set

$$S = \big\{ x \in \mathbb{Z} : x|a \quad \text{and} \quad x > 1 \big\}$$

has a minimum and that minimum is a prime.

Proof. Clearly $S \subseteq \mathbb{Z}$. Since $a > 1$ and $a|a$ we have that $a \in S$. Hence $S \neq \emptyset$. Clearly S is bounded below by 1. By the Well Ordering Axiom $\min S$ exists. Set $d = \min S$. Next we will prove the following statement:

$$\text{Let } y \in S. \text{ If } y \text{ is composite, then } d < y. \tag{1}$$

Here is a proof. Assume that $y \in S$ and $y = uv$ with $u > 1$ and $v > 1$. Multiplying $v > 1$ by u we get $y = uv > u$. Since $u|y$ and $y|a$, we have $u|a$. Thus $u \in S$ and hence $d \leq u$. Since $u < y$, this proves that $d < y$.

The following statement is the contrapositive of the statement (1):

$$\text{Let } y \in S. \text{ If } y = d, \text{ then } y \text{ is a prime.}$$

This proves that $\min S$ is a prime. ☐

Definition 2. For an integer a such that $a > 1$ the prime $\min S$ from Proposition 1 is called the *least prime divisor of* a. It is denoted by $\operatorname{lpd}(a)$.

Proposition 3. Let $a \in \mathbb{Z}$ and $a > 1$. Let $y \in \mathbb{Z}$ be such that $1 \leq y < a$ and $y \,|\, a$. Then there exists $q \in \mathbb{P}$ such that $(yq) \,|\, a$.

Proof. Since $y \,|\, a$ there exists $b \in \mathbb{Z}$ such that $a = yb$. Since $a = yb > y$ and $y \geq 1$, we conclude $b > 1$. Let $q = \operatorname{lpd}(b)$. Then $q \in \mathbb{P}$ and there exists $j \in \mathbb{Z}$ such that $b = qj$. Consequently $a = yb = yqj$. Hence $(yq)|a$. ☐

Theorem 4. Let $a \in \mathbb{Z}$ and $a > 1$. Then a is a prime or a product of primes.

Proof. Consider the set

$$T = \big\{ x \in \mathbb{Z} : x|a \quad \text{and} \quad x \ \text{ is a prime or a product of primes} \big\}.$$

Clearly $T \subseteq \mathbb{Z}$. Also, clearly $\operatorname{lpd}(a) \in T$. Hence $T \neq \emptyset$. Let $x \in T$. Then there exists $k \in \mathbb{Z}$ such that $a = xk$. Since $a > 1$ and $x > 1$ we conclude

$k \geq 1$. Multiplying the last inequality by $x > 1$ we get $a = kx \geq x$. Hence T is bounded above by a. By the Well Ordering Axiom $\max T$ exists.

Next we will prove the following statement:

$$\text{Let } y \in T. \text{ If } y < a, \text{ then } y < \max T. \tag{2}$$

Here is a proof. Assume that $y \in T$ and $y < a$. Then also $y > 1$ and by Proposition 3 there exist $q \in \mathbb{P}$ such that $(yq)|a$. Since $y \in T$, y is a prime or a product of primes. Therefore yq is a product of primes. Consequently $yq \in T$ and thus $yq \leq \max T$. Since $q \in \mathbb{P}$, $1 < q$. Thus $y < yq \leq \max T$. This proves $y < \max T$.

The contrapositive of the statement (2) is:

$$\text{Let } y \in T. \text{ If } y = \max T, \text{ then } y = a.$$

Thus $a = \max T$. In particular $a \in T$. Therefore a is a prime or a product of primes. □

The English phrase "a is a prime or a product of primes" can be formally expressed as: There exist $m \in \mathbb{N}$ and $p_1, \ldots, p_m \in \mathbb{P}$ such that

$$a = p_1 \cdots p_m = \prod_{j=1}^{m} p_j.$$

Lemma 5. Let $m \in \mathbb{N}$ and let $p_1, \ldots, p_m$ be primes such that $p_1 \leq p_2 \leq \cdots \leq p_m$ and $a = p_1 \cdots p_m$. Then $\operatorname{lpd}(a) = p_1$.

Proof. Set $d = \operatorname{lpd}(a)$. Then d is prime and $d|a$. Since $a = p_1 \cdots p_m$, Proposition 2.2.8 implies that there exists $j \in \{1, \ldots, m\}$ such that $d|p_j$. Since d and p_j are primes, we have $d = p_j$. Since d is the smallest prime divisor of a and $p_1|a$, we have $d \leq p_1$. Hence $d \leq p_1 \leq p_j = d$. The last relation implies $d = p_1 = p_j$. □

Lemma 6. Let $n \in \mathbb{N}$ and let $q_1, \ldots, q_n$ be primes such that $q_1 \leq q_2 \leq \cdots \leq q_n$ and $a = q_1 \cdots q_n$. Let $m \in \mathbb{N}$ be such that $m \leq n$. If $q_1 \cdots q_m = a$, then $m = n$.

Proof. It is easier to prove the contrapositive of the last implication: If $m < n$, then $q_1 \cdots q_m < a$. This is almost trivial, but here is a proof. Since $q_{m+1}, \ldots, q_n$ are primes, their product is greater than 1: $q_{m+1} \cdots q_n > 1$. Multiplying the last inequality by $q_1 \cdots q_m > 1$ we get

$$a = q_1 \cdots q_m q_{m+1} \cdots q_n > q_1 \cdots q_m.$$ □

Theorem 7. Let $m, n \in \mathbb{N}$ be such that $m \leq n$. Let $p_1, \ldots, p_m$ and $q_1, \ldots, q_n$ be primes such that

$$p_1 \leq p_2 \leq \cdots \leq p_m \qquad \text{and} \qquad a = p_1 \cdots p_m, \tag{3}$$
$$q_1 \leq q_2 \leq \cdots \leq q_n \qquad \text{and} \qquad a = q_1 \cdots q_n. \tag{4}$$

Then $m = n$ and $p_1 = q_1, p_2 = q_2, \ldots, p_m = q_m$.

Proof. Lemma 5 and the assumption (3) imply that $\operatorname{lpd}(a) = p_1$. Lemma 5 and the assumption (4) imply that $\operatorname{lpd}(a) = q_1$. Therefore $p_1 = q_1$. Since

$$a = p_1 \cdots p_m = q_1 \cdots q_n,$$

the equality $p_1 = q_1$ implies

$$p_2 \cdots p_m = q_2 \cdots q_n.$$

Set

$$a_1 = p_2 \cdots p_m = q_2 \cdots q_n.$$

Now Lemma 5 applied twice to the number a_1 implies

$$\operatorname{lpd}(a_1) = p_2 \qquad \text{and} \qquad \operatorname{lpd}(a_1) = q_2.$$

Therefore $p_2 = q_2$. Repeating this process $m - 2$ more times we get

$$p_1 = q_1, \quad p_2 = q_2, \quad \ldots, \quad p_m = q_m.$$

Since $a = p_1 \cdots p_m$, it follows that $a = q_1 \cdots q_m$. Now, Lemma 6 implies $m = n$. □

Example 8. Let $a = 4688133359$. Since

$$4688133359 = 7 \cdot 7 \cdot 13 \cdot 19 \cdot 19 \cdot 19 \cdot 29 \cdot 37$$

in the representation $a = p_1 \cdots p_m$ where $p_1, \ldots, p_m$ are primes such that $p_1 \leq p_2 \leq \cdots \leq p_m$ we have $m = 8$ and

$$p_1 = 7,\ p_2 = 7,\ p_3 = 13,\ p_4 = 19,\ p_5 = 19,\ p_6 = 19,\ p_7 = 29,\ p_8 = 37.$$

The canonical form of 4688133359 is $7^2 \cdot 13 \cdot 19^3 \cdot 29 \cdot 37$.