Section 1.5: The Fundamental Theorem of Arithmetic and consequences

Proposition 1.18 Let a be a natural and $n > 1$. Using the FTA there is a unique string of primes $p_1 < p_2 < \ldots < p_r$ and naturals $k_1, k_2, \ldots, k_r$ with

$$n = {p_1}^{k_1}{p_2}^{k_2} \ldots {p_r}^{k_r}.$$

A natural number d is a divisor of n if and only if d can be expressed in the form

$$d = {p_1}^{l_1}{p_2}^{l_2} \ldots {p_r}^{l_r}$$

where $0 \leq l_1 \leq k_1;\ 0 \leq l_2 \leq k_2;\ \ldots;\ 0 \leq l_r \leq k_r$.

NB. This theorem characterizes all divisors of n in terms of the prime factorization of n.

Theorem 1.19 Let a and b be natural numbers with $a > 1$ and $b > 1$. Using the FTA, write $a = {p_1}^{k_1}{p_2}^{k_2} \ldots {p_r}^{k_r}$ and $b = {q_1}^{l_1}{q_2}^{l_2} \ldots {q_s}^{l_s}$. Let $P_1 < P_2 < \ldots < P_t$ denote the primes $p_1, \ldots, p_r, q_1, \ldots, q_s$ combined [without repetition] and listed in increasing order. With this we can rewrite $a = {P_1}^{k_1}{P_2}^{k_2} \ldots {P_t}^{k_t}$ and $b = {P_1}^{l_1}{P_2}^{l_2} \ldots {P_t}^{l_t}$ where some of the exponents listed may be zero.

With the notation as above $(a, b) = {P_1}^{m_1}{P_2}^{m_2} \ldots {P_t}^{m_t}$ where each $m_i = \min(k_i, l_i)$.

NB. The first part of the statement of the theorem is meant to 'fill out' the prime factorizations for a and b with trivial factors of 1 [ie primes to the power 0] so that we can combine associated exponents in the conclusion of the theorem. This theorem tells us how to compute the gcd of a and b using their prime factorizations.

Why are we not concerned with $a = 1$ or $b = 1$ [or negative integers for that matter]?

Definition Let $n > 1$. We say n is <u>square-free</u> if the only perfect square dividing n is 1.