The GCD–Formula

Notation: The prime decomposition of an integer $n > 1$ is its prime factorization of the form

(1) $$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r},$$

where $p_1 < p_2 < \ldots < p_r$ are distinct primes.

If p is any prime number, then the integer

(2) $$expt_p(n) := \begin{cases} e_i, & \text{if } p = p_i \text{ for some } i \\ 0, & \text{if } p \neq p_i \text{ for any } i \end{cases}$$

is called the exponent of p in n.

Theorem 9 ("GCD–Formula"): Let $m, n \in \mathbb{Z}$ be non-zero integers.

a) $m|n \Leftrightarrow expt_p(m) \le expt_p(n)$, for all primes p.

b) For any prime p we have

$$expt_p(gcd(m,n)) = min(expt_p(m), expt_p(n)).$$

Thus, if $p_1 < p_2 < \ldots < p_r$ denote the distinct prime factors of $m \cdot n$, then

$$gcd(m,n) = p_1^{g_1} p_2^{g_2} \cdots p_r^{g_r},$$

where $g_i = min(expt_{p_i}(m), expt_{p_i}(n))$.