FUNDAMENTAL THEOREM OF ARITHMETIC

Theorem: (The Fundamental theorem of Arithmetic)

Statement:

Every integer n ≥ 2 either is a prime or can be expressed as a product of primes. The factorization into primes is unique except for the order of the factors.

Proof:

First, we will show by strong induction that n either is a prime or can be expressed as a product of primes. Then we will establish the uniqueness of such a factorization.

Let P(n) denote the statement that n is a prime or can be expressed as a product of primes.

To show that P(n) is true for every integer n ≥ 2.

Since 2 is a prime, clearly P(2) is true.

Now assume P(2),P(3),...,P(k) are true; that is, every integer ≥ 2 through k either is a prime or can be expressed as a product of primes.

If k + 1 is a prime, then P(k + 1) is true.

Suppose k + 1 is composite.

Then k + 1 = ab for some integers a and b, where 1 < a, b< k + 1.

By the inductive hypothesis, a and b either are primes or can be expressed as products of primes.

In any event, k +1 = ab can be expressed as a product of primes.

Thus, P(k +1) is also true. Thus, by strong induction, the result holds for every integer n ≥ 2.

.

To establish the uniqueness of the factorization:

Let n be a composite number with two factorizations into primes.

$n = p_1.p_2.p_3. \ . \ .p_r = q_1.q_2.q_3. \ . \ .q_s.$

We will show that $r = s$ and every p_i equals some q_j, where $1 \leq i, j \leq r$;

that is, the primes $q_1.q_2.q_3. \ . \ .q_s$ are a permutation of the primes $n = p_1.p_2.p. \ . \ .p_r.$

Assume, for convenience, that $r < s$.

Since, $p_1.p_2.p_3. \ . \ .p_r = q_1.q_2.q_3. \ . \ .q_s.$ But p_1 must divide some $q_j.$

(i.e) $p_1 | \ q_1.q_2.q_3. \ . \ .q_s$, and p_1 is prime. p_1 must divide some q_j

$\Rightarrow \ p_1 = q_j$ as they are primes.

Dividing both sides by p_1, we get, $p_2.p_3. \ . \ .p_r = q_1.q_2.q_3. \ .q_{j-1}.q_{j+1} \ . \ .q_s.$

Repeat this argument with $p_2.p_3. \ . \ .p_r.$

Since $r < s$, we get 1= a product of q' s.

$\Rightarrow 1 = \text{a product of primes.}$

Which is a contradiction.

Therefore, our assumption $r < s$ is wrong $\Rightarrow \ r \geq s.$ (1)

Similarly, if $s < r \ \Rightarrow \ s \geq r.$ (2)

For (1) and (2), $r = s.$

Thus, the factorization is unique, except for the order of the factors.

CANONICAL DECOMPOSITION

Canonical Decomposition

Definition: A canonical decomposition of any positive integer n is of the form $n = p_1^{\alpha_1}.\, p_2^{\alpha_2}\, .\, .\, .\, p_k^{\alpha_k}$, where $p_1^{\alpha_1}, p_2^{\alpha_2}, .\, .\, .\, p_k^{\alpha_k}$ are distinct primes.

Example 1: Find the canonical decomposition of 4312.

Solution: $4312 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 7 \cdot 11 = 2^3 \cdot 7^2 \cdot 11^1$

Example 2: Find the canonical decomposition of 2520.

Solution: $2520 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^1$

Example 3: Find the $(72, 108)$ using canonical decomposition.

Solution:

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2$$

$$108 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 = 2^2 \cdot 3^3$$

$$(72, 108) = 2^2 3^2 = 4 * 9 = 36.$$

Example 4: Using recursion, evaluate (18, 30, 60, 75, 132).

Solution:

$(18, 30, 60, 75, 132) = ((18, 30, 60, 75), 132)$

$= (((18, 30, 60), 75), 132)$

$= ((((18, 30), 60), 75), 132)$

$= (((6, 60), 75), 132)$

$= ((6, 75), 132)$

$= (3, 132) = 3.$