Proposition: (φ factorization) For a prime number $p \in \mathbb{N}$, if $k \in \mathbb{N}$, then

$$\boxed{\varphi(p^k) = p^k - p^{k-1}.}$$

Consequently, if $n \in \mathbb{N}$ and n has prime decomposition

$$n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$$ for

distinct primes $p_1, p_2, \ldots, p_m$ and $k_1, k_2, \ldots, k_m \in \mathbb{N}$, then

$$\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdot \ldots \cdot \varphi(p_m^{k_m})$$

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdot \ldots \cdot (p_m^{k_m} - p_m^{k_m-1})$$

Proof: Counting Principle: Sometimes, it is easier to count what you'd like to exclude, rather than include.

For a prime p and $k \in \mathbb{N}$, then the natural numbers less than or equal to p^k that are not relatively prime to p^k are characterized by the existence of a factor of p.

These numbers are

$$p = p \cdot 1,\ p \cdot 2,\ p \cdot 3,\ p \cdot 4,\ \dots,\ p \cdot p^{k-1}.$$

We get p^{k-1} such numbers.

So

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Now we simply apply the previous proposition. If

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m},$$

then if $m = 2$, by the proposition, we have

$\gcd(p_1^{k_1}, p_2^{k_2}) = 1$, so

$$\varphi(n) = \varphi(p_1^{k_1} p_2^{k_2}) = \varphi(p_1^{k_1})\,\varphi(p_2^{k_2}).$$

Now assume the result holds true for $m-1$ distinct primes (inductive step). Then since

$$\gcd(p_1^{k_1},\ p_2^{k_2} \cdot p_3^{k_3} \cdot \ldots \cdot p_m^{k_m}) = 1,$$

the proposition gives us

$$\varphi(n) = \varphi(p_1^{k_1} \cdot p_2^{k_2} p_3^{k_3} \cdot \ldots \cdot p_m^{k_m})$$

$$= \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2} p_3^{k_3} \cdot \ldots \cdot p_m^{k_m})$$

(induction) $$= \varphi(p_1^{k_1})\,\varphi(p_2^{k_2}) \cdot \ldots \cdot \varphi(p_m^{k_m})$$

So

$$\varphi(n) = \varphi(p_1^{k_1})\,\varphi(p_2^{k_2}) \cdot \ldots \cdot \varphi(p_m^{k_m})$$

$$= \left(p_1^{k_1} - p_1^{k_1-1}\right) \cdot \left(p_2^{k_2} - p_2^{k_2-1}\right) \cdot \ldots \cdot \left(p_m^{k_m} - p_m^{k_m-1}\right)$$

$\square$

Theorem: (Euler) Let $n \in \mathbb{N}$. If $m \in \mathbb{Z}$, $\gcd(m,n) = 1$, then

$$m^{\varphi(n)} \equiv 1 \mod n.$$