Euler's Totient Function

Q: Given $n \in \mathbb{N}$, for how many $x \in [n]$ is $\gcd(n,x) = 1$?

Definition: Given $n \in \mathbb{N}$, we define $\phi(n)$ to be
$\phi(n) = |\{x \in [n] : \gcd(x,n) = 1\}|$.
$\phi(n)$ is called Euler's Totient function or Euler's Phi function.

Examples:
$\phi(9) = 6$ as $\{x \in [9] : \gcd(9,x) = 1\} = \{1,2,4,5,7,8\}$
$\phi(10) = 4$ as $\{x \in [10] : \gcd(10,x) = 1\} = \{1,3,7,9\}$

Theorem: For all natural numbers n, if the prime factorization of n is $n = \prod_{j=1}^{\infty} p_j^{c_j}$ then
$$\phi(n) = \prod_{j : c_j > 0} p_j^{c_j - 1}(p_j - 1)$$

Examples: $9 = 3^2$ so $\phi(9) = 3 \cdot 2 = 6$ and $10 = 2 \cdot 5$ so $\phi(10) = (2-1)(5-1) = 4$

Euler's Totient Function

Theorem: For all natural numbers n, if the prime factorization of n is $n = \prod_{j=1}^{\infty} p_j^{c_j}$ then $\phi(n) = \prod_{j: c_j > 0} p_j^{c_j - 1}(p_j - 1)$.

Proof:

Lemma: If $m, n \in \mathbb{N}$ and $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.

Proof: By the Chinese Remainder Theorem, for all $a_1 \in [m]$ and all $a_2 \in [n]$, there is a unique $x \in [mn]$ such that $x \equiv a_1 \bmod m$ and $x \equiv a_2 \bmod n$.

Fact: $\forall x, m, n \in \mathbb{Z}\ (\gcd(x, mn) = 1 \leftrightarrow \gcd(x,m) = 1 \wedge \gcd(x,n) = 1)$

Thus, choosing an $x \in [mn]$ such that $\gcd(x, mn) = 1$ is equivalent to choosing $a_1 \in [m]$ and $a_2 \in [n]$ such that $\gcd(m, a_1) = \gcd(m, x) = 1$ and $\gcd(n, a_2) = \gcd(n, x) = 1$. There are $\phi(m)\phi(n)$ ways to do this.

Using this lemma, it is sufficient to show that $\phi(p_j^{c_j}) = p_j^{c_j - 1}(p_j - 1)$.

To show this, observe that $\gcd(x, p_j^{c_j}) = 1 \leftrightarrow p_j \nmid x$.

Of the numbers in $[p_j^{c_j}]$, $\frac{p_j^{c_j}}{p_j} = p_j^{c_j - 1}$ are divisible by p_j.

$p_j^{c_j} - p_j^{c_j - 1} = p_j^{c_j - 1}(p_j - 1)$ of these numbers are not divisible by p_j.