

And the definition of a set G

$$\text{Let } G = \{g \in (1, \dots, n) : \gcd(n, g) \neq 1\}$$

Throughout the course of the proof, it will be shown that expression (A) is equivalent to $|G|$

$$\text{Let } P_i = \{x \in (1, \dots, n) : p_i \mid x\} \text{ where } p_i \text{ is a prime factor of } n$$

$$\text{Claim: } G = \bigcup_{i=1}^m P_i$$

Proof:

let g be an element of G , $g \in G$

let $d = \gcd(g, n) \neq 1$

then $d \mid g$ and $d \mid n$

as $d \mid n$ and $d \neq 1 \exists p_d \in (p_1, p_2, \dots, p_m)$ s.t. $p_d \mid d$

$p_d \mid d$ and $d \mid g$ shows $p_d \mid g$

then $g \in P_d$

and $g \in \bigcup_{i=1}^m P_i$

$\therefore G \subset \bigcup_{i=1}^m P_i$

let x be an element of $\bigcup_{i=1}^m P_i$, $x \in \bigcup_{i=1}^m P_i$
 then $\exists P_x$ s.t. $x \in P_x$
 as $x \in P_x$, $p_x \mid x$
 p_x is a prime factor of n
 so $p_x \mid n$
 as $p_x \mid x$ and $p_x \mid n$ then $\gcd(x, n) \geq p_x \neq 1$
 thus $x \in G$
 $\therefore \bigcup_{i=1}^m P_i \subset G$

With $G \subset \bigcup_{i=1}^m P_i$ and also $\bigcup_{i=1}^m P_i \subset G$ then

$$G = \bigcup_{i=1}^m P_i$$

Claim: The number of elements in the intersection of any number of P sets is equivalent to the number n divided by each corresponding p .

$$|P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}| = n/p_{i_1}p_{i_2} \dots p_{i_k}$$

Proof:

Suppose $x \in P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}$

then, $p_{i_1} \mid x$, $p_{i_2} \mid x$, ..., $p_{i_k} \mid x$

as p_{i_1}, \dots, p_{i_k} are all primes and thus relatively prime to each other,

$$p_{i_1}p_{i_2} \dots p_{i_k} \mid x$$

$$x = p_{i_1}p_{i_2} \dots p_{i_k}q$$

$$\text{but } x \leq n$$

$$qp_{i_1}p_{i_2} \dots p_{i_k} \leq n$$

$$q \leq n/p_{i_1}p_{i_2} \dots p_{i_k}$$

This shows $n/p_{i_1}p_{i_2} \dots p_{i_k}$ possible solutions for q

and therefore $n/p_{i_1}p_{i_2} \dots p_{i_k}$ possible values for x

$$\therefore |P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}| = n/p_{i_1}p_{i_2} \dots p_{i_k}$$

We can now re-write expression (A) in terms of the size of sets of P

expression (B):

$$\begin{aligned}
& (|P_1| + |P_2| + \dots + |P_m|) \\
& -(|P_1 \cap P_2| + |P_1 \cap P_3| + \dots + |P_1 \cap P_m| + |P_2 \cap P_3| + \dots + |P_{m-1} \cap P_m|) \\
& + \\
& \vdots \\
& + (-1)^{m+1} \left(\left| \bigcap_{i=1}^m P_i \right| \right)
\end{aligned}$$

Here, we notice the grouping of sets of P in terms of how many possible intersections there are.

Define sets of sets to describe this grouping

$$L_k = \{P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}\} \text{ for } k = 1, \dots, m \text{ and } P_{i_k} \in (P_1, P_2, \dots, P_m)$$

In other words, that L_k is the set of all possible combinations of exactly k distinct sets of P_i intersected with each other.

Then, we can further simplify (B) to become expression (C)

$$\sum_{k=1}^m (-1)^{k+1} \sum_{i=1}^{|L_k|} |l_{k,i}|$$

where $l_{k,i}$ is the i -th distinct element in L_k

we now decompose every set $l_{k,i}$ into $|l_{k,i}|$ number of disjoint single element subsets.

$$l_{k,i} = P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k} = \bigcup_{i=1}^{|P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}|} S_{p_{i_1} p_{i_2} \dots p_{i_k}, i}$$

where $S_{p_{i_1} p_{i_2} \dots p_{i_k}, i} = \{s_{p_{i_1} p_{i_2} \dots p_{i_k}, i}\}$, where $s_{p_{i_1} p_{i_2} \dots p_{i_k}, i}$ is the i -th element of $P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}$

As the single element sets are disjoint, then

$$|l_{k,i}| = |P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}| = \left| \bigcup_{i=1}^{|P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}|} S_{p_{i_1} p_{i_2} \dots p_{i_k}, i} \right| = \sum_{i=1}^{|P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}|} |S_{p_{i_1} p_{i_2} \dots p_{i_k}, i}|$$

Substituting this in on expression (C) we get expression (D)

$$\sum_{k=1}^m (-1)^{k+1} \sum_{i=1}^{|L_k|} \sum_{j=1}^{|P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}|} |S_{p_{i_1} p_{i_2} \dots p_{i_k}, j}|$$

when (D) is expanded out, we get the following

$$\begin{aligned}
& (|S_{p_1,1}| + |S_{p_1,2}| + \dots + |S_{p_1,|P_1|}| + |S_{p_2,1}| + \dots + |S_{p_2,|P_2|}| + \dots + |S_{p_m,|P_m|}|) \\
& - (|S_{p_1 p_2,1}| + |S_{p_1 p_2,2}| + \dots + |S_{p_1 p_2,|P_1 \cap P_2|}| + |S_{p_1 p_3,1}| + \dots + |S_{p_1 p_3,|P_1 \cap P_3|}| + \dots + |S_{p_{m-1}, p_m, |P_{m-1} \cap P_m|}|) \\
& \quad + \\
& \quad \quad \quad \vdots \\
& \quad + (-1)^{m+1} (|S_{p_1 \dots p_m,1}| + \dots + |S_{p_1 \dots p_m, |\bigcap_{i=1}^m P_i|}|)
\end{aligned}$$

However, every set S is a single element subset of G . Then, for an s in a particular S

we have that $s = g$ for some $g \in G$

Define single - element disjoint subsets of G where

$$G_i = \{g_i\} \text{ for } i = 1, \dots, |G| \text{ where } g_i \text{ is the } i\text{-th element of } G$$

we can group equivalent sets and then re-write the expanded form of (D) to become

$$\begin{aligned}
& (|G_1| + |G_1| + \dots + |G_1| + |G_2| + \dots + |G_2| + \dots + |G_{|G|}| + \dots + |G_{|G|}|) \\
& - (|G_1| + |G_1| + \dots + |G_1| + |G_2| + \dots + |G_2| + \dots + |G_{|G|}| + \dots + |G_{|G|}|) \\
& \quad + \\
& \quad \quad \quad \vdots \\
& + (-1)^{m+1} (|G_1| + |G_1| + \dots + |G_1| + |G_2| + \dots + |G_2| + \dots + |G_{|G|}| + \dots + |G_{|G|}|)
\end{aligned}$$

which is

$$\begin{aligned}
& (c_{1,1}|G_1| + c_{1,2}|G_2| + \dots + c_{1,|G|}|G_{|G|}|) \\
& - (c_{2,1}|G_1| + c_{2,2}|G_2| + \dots + c_{2,|G|}|G_{|G|}|) \\
& \quad + \\
& \quad \quad \quad \vdots \\
& + (-1)^{m+1} (c_{m,1}|G_1| + c_{m,2}|G_2| + \dots + c_{m,|G|}|G_{|G|}|)
\end{aligned}$$

and simplified to
expression (E)

$$\sum_{i=1}^{|G|} \sum_{k=1}^m (-1)^{k+1} c_{k,i} |G_i|$$

where $c_{k,i}$ is the number of times that $|G_i|$ appears in the single element disjoint subset decomposition of L_k

Define a pair of functions,

$$f_1(S, g) = \begin{cases} 1 & \text{if } g \in S \\ 0 & \text{if } g \notin S \end{cases} \text{ where } S \text{ is a set of numbers, and } g \in G$$

$$f_2(L, g) = f_1(l_1, g) + \dots + f_1(l_{|L|}, g) \text{ where } L \text{ is a set of sets and } g \in G$$

and l_i is the i -th element of L

then, we can say that $c_{k,i} = f_2(L_k, g_i)$
expression (F)

$$\sum_{i=1}^{|G|} \sum_{k=1}^m (-1)^{k+1} f_2(L_k, g_i)$$

For any particular g_i we can say that $\gcd(n, g_i) = p_{b_1}^{\beta_1} \dots p_{b_r}^{\beta_r}$ is the prime factorization.

Let L_{k,g_i} be a subset of L_k which is all the sets in L_k that contains g_i

$$L_{k,g_i} = \{S \in L_k : g_i \in S\}$$

then, $L_k \setminus L_{k,g_i}$ is the set of sets in L_k that do not contain g_i . So,

$$L_{k,g_i} \cup L_k \setminus L_{k,g_i} = L_k$$

Take f_2 of both sides with respect to g_i

$$f_2(L_{k,g_i} \cup L_k \setminus L_{k,g_i}, g_i) = f_2(L_k, g_i)$$

and as $L_{k,g_i} \cup L_k \setminus L_{k,g_i} = \emptyset$ then

$$f_2(L_{k,g_i}, g_i) + f_2(L_k \setminus L_{k,g_i}, g_i) = f_2(L_k, g_i)$$

but, $\forall S \in L_k \setminus L_{k,g_i}, g \notin S$, then

$$f_2(L_k \setminus L_{k,g_i}, g_i) = 0, \text{ and}$$

$$f_2(L_{k,g_i}, g_i) + 0 = f_2(L_k, g_i)$$

$$f_2(L_{k,g_i}, g_i) = f_2(L_k, g_i)$$

If given a set of the intersection of exactly k number of P sets, $P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}$ then

$$g_i \in P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k} \text{ only if } \{p_{i_1}, \dots, p_{i_k}\} \subset \{p_{b_1}, \dots, p_{b_r}\}$$

That is, from b_r number of sets P_{b_i} , a set $P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}$ can be constructed by selecting

exactly k number of sets from $\{P_{b_1}, \dots, P_{b_r}\}$ with $g \in P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}$

The number of potential sets $P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}$ is equivalent to the combination function of

$$C(b_r, k)$$

then

$$f_2(L_k, g_i) = C(b_r, k)$$

Continuing from expression (F)

$$\begin{aligned} & \sum_{i=1}^{|G|} \sum_{k=1}^m (-1)^{k+1} f_2(L_k, g_i) \\ & \sum_{i=1}^{|G|} \left(\sum_{k=b_r+1}^m (-1)^{k+1} f_2(L_k, g_i) + \sum_{k=1}^{b_r} (-1)^{k+1} f_2(L_k, g_i) \right) \\ & \sum_{i=1}^{|G|} \left(\sum_{k=b_r+1}^m (-1)^{k+1} C(b_r, k) + \sum_{k=1}^{b_r} (-1)^{k+1} C(b_r, k) \right) \\ & \quad \text{but when } k > b_r, C(b_r, k) = 0 \\ & \sum_{i=1}^{|G|} \left(\sum_{k=b_r+1}^m (-1)^{k+1} (0) + \sum_{k=1}^{b_r} (-1)^{k+1} C(b_r, k) \right) \\ & \sum_{i=1}^{|G|} \left(0 + \sum_{k=1}^{b_r} (-1)^{k+1} C(b_r, k) \right) \end{aligned}$$

expression (G)

$$\sum_{i=1}^{|G|} \sum_{k=1}^{b_r} (-1)^{k+1} C(b_r, k)$$

Claim: $C(a+1, b) = C(a, b) + C(a, b-1)$

Proof:

$$\begin{aligned}
C(a, b) + C(a, b-1) &= \frac{a!}{b!(a-b)!} + \frac{a!}{(b-1)!(a-b+1)!} \\
&= \frac{a!}{b(b-1)!(a-b)!} + \frac{a!}{(a+1+b)(b-1)!(a-b)!} \\
&= \frac{a!}{(b-1)!(a-b)!} \left(\frac{1}{b} + \frac{1}{a+1-b} \right) \\
&= \frac{a!}{(b-1)!(a-b)!} \left(\frac{a+1-b}{b(a+1-b)} + \frac{b}{b(a+1-b)} \right) \\
&= \frac{a!}{(b-1)!(a-b)!} \left(\frac{a+1}{b(a+1-b)} \right) \\
&= \frac{(a+1)a!}{b(b-1)!(a+1-b)(a-b)!} \\
&= \frac{(a+1)!}{b!(a+1-b)!} \\
&= C(a+1, b)
\end{aligned}$$

Claim: $\sum_{i=1}^a (-1)^{i+1} C(a, i) = 1$ for any a

Proof:

$$\begin{aligned}
\sum_{i=1}^a (-1)^{i+1} C(a, i) &= C(a, 1) - C(a, 2) + C(a, 3) - \dots + (-1)^a C(a, a-1) + (-1)^{a+1} C(a, a) \\
&= (C(a-1, 0) + C(a-1, 1)) - (C(a-1, 1) + C(a-1, 2)) + (C(a-1, 2) + C(a-1, 3)) - \dots \\
&\quad + (-1)^a (C(a-1, a-2) + C(a-1, a-1)) + (-1)^{a+1} C(a, a) \\
&= C(a-1, 0) + (C(a-1, 1) - C(a-1, 1)) + (C(a-1, 2) - C(a-1, 2)) + \dots \\
&\quad + (-1)^a C(a-1, a-1) + (-1)^{a+1} C(a, a) \\
&= C(a-1, 0) + (-1)^a C(a-1, a-1) + (-1)^{a+1} C(a, a) \\
&= 1 + (-1)^a (1) + (-1)(-1)^a (1) \\
&= 1 + (-1)^a - (-1)^a \\
&= 1 + 0 \\
&= 1
\end{aligned}$$

From expression (G)

$$\sum_{i=1}^{|G|} \sum_{k=1}^{b_r} (-1)^{k+1} C(b_r, k)$$

but $\sum_{k=1}^{b_r} (-1)^{k+1} C(b_r, k) = 1$

$$\sum_{i=1}^{|G|} 1$$

expression (H)

$$|G|$$

we have that $(A) = (H)$.

The totient function, $\varphi(n)$ is the number of integers less than or equal to n that are relatively prime to n

As G is the set of numbers that are less than or equal to n that are not relatively prime to n , then

$$\begin{aligned} \varphi(n) + |G| &= n \\ \varphi(n) &= n - |G| \end{aligned}$$

And finally

$$\begin{aligned} \varphi(n) &= n \\ &- (p_1^{\alpha_1-1} p_2^{\alpha_2} \dots p_m^{\alpha_m} + p_1^{\alpha_1} p_2^{\alpha_2-1} p_3^{\alpha_3} \dots p_m^{\alpha_m} + \dots + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m-1}) \\ &+ (p_1^{\alpha_1-1} p_2^{\alpha_2-1} p_3^{\alpha_3} \dots p_m^{\alpha_m} + p_1^{\alpha_1-1} p_2^{\alpha_2} p_3^{\alpha_3-1} p_4^{\alpha_4} \dots p_m^{\alpha_m} + \dots + p_1^{\alpha_1-1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_m^{\alpha_m-1} \\ &+ p_1^{\alpha_1} p_2^{\alpha_2-1} p_3^{\alpha_3-1} p_4^{\alpha_4} \dots p_m^{\alpha_m} + p_1^{\alpha_1} p_2^{\alpha_2-1} p_3^{\alpha_3} p_4^{\alpha_4-1} p_5^{\alpha_5} \dots p_m^{\alpha_m} + \dots + p_1^{\alpha_1} p_2^{\alpha_2-1} p_3^{\alpha_3} \dots p_m^{\alpha_m-1} \\ &+ \dots + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{m-1}^{\alpha_{m-1}-1} p_m^{\alpha_m-1}) \\ &- \\ &\vdots \\ &+ (-1)^m (p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_m^{\alpha_m-1}) \end{aligned}$$

□

Summary of Proof

$$\begin{aligned}
& (p_1^{\alpha_1-1} p_2^{\alpha_2} \dots p_m^{\alpha_m} + p_1^{\alpha_1} p_2^{\alpha_2-1} p_3^{\alpha_3} \dots p_m^{\alpha_m} + \dots + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m-1}) \\
& - (p_1^{\alpha_1-1} p_2^{\alpha_2-1} p_3^{\alpha_3} \dots p_m^{\alpha_m} + p_1^{\alpha_1-1} p_2^{\alpha_2} p_3^{\alpha_3-1} p_4^{\alpha_4} \dots p_m^{\alpha_m} + \dots + p_1^{\alpha_1-1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_m^{\alpha_m-1} \\
& + p_1^{\alpha_1} p_2^{\alpha_2-1} p_3^{\alpha_3-1} p_4^{\alpha_4} \dots p_m^{\alpha_m} + p_1^{\alpha_1} p_2^{\alpha_2-1} p_3^{\alpha_3} p_4^{\alpha_4-1} p_5^{\alpha_5} \dots p_m^{\alpha_m} + \dots + p_1^{\alpha_1} p_2^{\alpha_2-1} p_3^{\alpha_3} \dots p_m^{\alpha_m-1} \\
& \quad + \dots + p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{m-1}^{\alpha_{m-1}-1} p_m^{\alpha_m-1}) \\
& \quad + \\
& \quad \vdots \\
& + (-1)^{m+1} (p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_m^{\alpha_m-1}) \\
& \\
& = (|P_1| + |P_2| + \dots + |P_m|) \\
& - (|P_1 \cap P_2| + |P_1 \cap P_3| + \dots + |P_1 \cap P_m| + |P_2 \cap P_3| + \dots + |P_{m-1} \cap P_m|) \\
& \quad + \\
& \quad \vdots \\
& + (-1)^{m+1} \left(\left| \bigcap_{i=1}^m P_i \right| \right) \\
& = \sum_{k=1}^m (-1)^{k+1} \sum_{i=1}^{|L_k|} |l_{k,i}| \\
& = \sum_{k=1}^m (-1)^{k+1} \sum_{i=1}^{|L_k|} \sum_{j=1}^{|P_{i_1} \cap P_{i_2} \cap \dots \cap P_{i_k}|} |S_{p_{i_1} p_{i_2} \dots p_{i_k}, j}| \\
& = \sum_{i=1}^{|G|} \sum_{k=1}^m (-1)^{k+1} c_{k,i} |G_i| \\
& = \sum_{i=1}^{|G|} \sum_{k=1}^m (-1)^{k+1} f_2(L_k, g_i) \\
& = \sum_{i=1}^{|G|} \sum_{k=1}^{b_r} (-1)^{k+1} C(b_r, k) \\
& = |G|
\end{aligned}$$