Proof of Euler's φ (Phi) Function Formula

Presented by Emils Kalugins

Paper[1] authored by:
Shashank Chorge[2] Juan Vargas[3]

Univesity of Latvia

October 8, 2017

[1] Available at: http://scholar.rose-hulman.edu/rhumj/vol14/iss2/6
[2] Mumbai University
[3] UNC Charlotte

Formulation

Euler's φ function counts the number of positive integers up to a given integer n that are relatively prime to n.

Example 1.1

Suppose $n = 36$, then there are twelve positive integers that are coprime with 36 and lower than 36: 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31 and 35. Which means that $\varphi(n) = 12$.

Goal

Theorem 1.2

For all $n \in \mathbb{N}$ *we have*

$$\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_m}\right),$$

where $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ *is the prime factorization of* n*.*

Lemma

Lemma 2.1

Define $G_k = \{r \in \mathbb{N} \,|\, 0 < r < kn$ *and* $gcd(n, r) = 1\}$. *Then* $|G_k| = k\varphi(n)$.

Proof.

Let H_n be the set of numbers less than n that are coprime to n. By Definiton 1.2, $|H_n| = \varphi(n)$. Suppose $h \in H_n$. Then any number of the form $kn + h$ is coprime to n. Since this holds for all $k \in \mathbb{N}$ and and every $h \in H_n$, then for any given k there are exactly $\varphi(n)$ coprime numbers to n in

$$E_k = \{r \in \mathbb{N} \,|\, kn < r < k(n+1) \text{ and } gcd(r, n) = 1\}.$$

Hence, $|G_k|$ is equal to the number of intervals k times $\varphi(n)$. $\square$

Example

Example 2.2

Consider $n = 10$, then by the previous lemma $gcd(r, n) = gcd(r + 10, n)$.

$H_{10} = \{1, 3, 7, 9\}$.

$E_1 = \{11, 13, 17, 19\}$,
$E_2 = \{21, 23, 27, 29\}$,
...
$E_k = \{10k + 1, 10k + 3, 10k + 7, 10k + 9\}$.

First case

Lemma 3.1

Let p be a prime number and $p \mid n$, then $\varphi(pn) = p\varphi(n)$.

Proof.

We first note that every number that is coprime to pn is also coprime to n. Since $gcd(pn, n) = n$ and $p \mid n$ the following result follows: $gcd(r, pn) = 1$ if and only if $gcd(r, n) = 1$ for $r \in \mathbb{N}$.
There are p intervals, each with $\varphi(n)$ numbers relatively prime to n, hence to pn and therefore by Lemma 2.1, the set $G_p = \{r \in \mathbb{N} \mid 0 < r < pn \text{ and } gcd(n, r) = 1\}$ has $|G_p| = p\varphi(n)$ elements. □

Second case

Lemma 3.2

Let p be a prime number and $p \nmid n$, then $\varphi(pn) = (p-1)\varphi(n)$.

Proof.

By Lemma 2.1 we know that $p\varphi(n)$ is the number of coprime numbers to n that are less than pn. Take the set of all multiples of p whose factors are coprime to n. The set $\{r_1 p, r_2 p, \ldots, r_{\varphi(n)} p\}$ contains all the elements we have overcounted because n is coprime to p and r by definition. Subtracting this amount from the original count, we conclude that
$\varphi(pn) = p\varphi(n) - \varphi(n) = (p-1)\varphi(n)$.

□

General case

Theorem

For all $n \in \mathbb{N}$ *we have*

$$\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right),$$

where $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ *is the prime factorization of* n*.*

Proof

Proof.

We can apply Lemma 3.2 to all of the prime factors of n. Thus we get the following,

$$\varphi(n) = \varphi(p_1^{k_1} \dots p_m^{k_m}) = p_1^{k_1 - 1} \dots p_m^{k_m - 1} \varphi(p_1 p_2 \dots p_m).$$

Now we apply Lemma 3.1:

$$\varphi(n) = p_1^{k_1 - 1} \dots p_m^{k_m - 1} (p_1 - 1)(p_2 - 1) \dots (p_m - 1).$$

We can clean this up by multiplying with $\frac{p_s}{p_s}$ for all $1 \leq s \leq m$ (cont.).

Proof

Proof.

$$\begin{aligned}\varphi(n) &= \left(\frac{p_1}{p_1}\right)\left(\frac{p_2}{p_2}\right)\dots\left(\frac{p_m}{p_m}\right)p_1^{k_1-1}\dots p_m^{k_m-1}(p_1-1)(p_2-1)\dots(p_m-1)\\ &= p_1^{k_1}p_2^{k_2}\dots p_m^{k_m}\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)\dots\left(\frac{p_m-1}{p_m}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_m}\right).\end{aligned}$$

□

Thank you for your attention!