**Rose-Hulman Undergraduate Mathematics Journal**

Volume 14
Issue 2

Article 6

# Proof of Euler's φ (Phi) Function Formula

Shashank Chorge
*Mumbai University*, chorgeshashank@yahoo.co.in

Juan Vargas
*UNC Charlotte*, jvargas9@uncc.edu

Rose-Hulman Undergraduate Mathematics Journal

# Proof of Euler's $\phi$ (Phi) Function Formula

Shashank Chorge[a] Juan Vargas[b]

Volume 14, no. 2, Fall 2013

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]Mumbai University
[b]UNC Charlotte

Rose-Hulman Undergraduate Mathematics Journal
Volume 14, no. 2, Fall 2013

# Proof of Euler's $\phi$ (Phi) Function Formula

Shashank Chorge Juan Vargas

**Abstract.** Euler's $\phi$ (phi) Function counts the number of positive integers not exceeding $n$ and relatively prime to $n$. Traditionally, the proof involves proving the $\phi$ function is multiplicative and then proceeding to show how the formula arises from this fact. We ignore this fact, at least directly, and show a practical and sound method to calculate $\phi$. We offer a proof of the closed form formula for this function relying on similar, but subtly different counting techniques.

**Acknowledgements**: This collaboration would not have been possible without Dr. Harold Reiter. His encouragement for this collaborative effort, despite the great distance between the authors, is greatly appreciated. We would like to thank Dr. David Rader and the referees who reviewed the paper for the abundance of useful suggestions and comments. Thank you.

# Introduction

If a 100-floor building needed repairs in every floor whose number had a prime factor in common with 100, how many floors would need repairs? Questions of this nature most clearly exemplify Euler's $\phi$ Function. In essence $\phi(100)$ is the number of floors that need no repairs.

We say two numbers are relatively prime if they have no prime factors in common. The floors needing no repair are relatively prime to 100. Hence, the following definition.

**Definition 1.** *For $n \geq 1$, $\phi(n)$ denotes the number of positive integers not exceeding $n$ and relatively prime to $n$.*

For the purpose of self-containment and clarity the gcd is defined as follows.

**Definition 2** (Greatest Common Divisor)**.** *The greatest common divisor of two nonzero integers a and b is the largest of all common divisors of a and b. We denote this integer by gcd(a,b). When gcd(a,b)=1, we say a and b are relatively prime.*

In view of this manner of thinking about $\phi(n)$ and the definition of the greatest common divisor we can restate definition 1 as

**Definition 3.** *For $n \geq 1$, $\phi(n)$ denotes the number of positive integers $r$ such that $r \leq n$ and $gcd(n, r) = 1$.*

At first it may seem as if learning how to calculate $\phi(n)$ would serve no purpose beyond satisfying our curiosity in answering the posed question. In Number Theory and Computer Science, however, calculating $\phi(n)$ plays a crucial rule in determining properties of theoretically defined functions and perfoming calculations with large numbers (for example, RSA and exponentiation under a modulus).

At this point we might be curious about the motivation for $\phi(n)$. A little history may be in order. In a paper titled " Theoremata arithmetica nova methodo demonstrata" (Demonstration of a new method in the Theory of Arithmetic) presented to the St. Petersburg Academy on October 15, 1759, Euler introduces this function [1]. This paper contained the formal proof of the generalized version of Fermat Little's Theorem, also known as The Fermat-Euler Theorem, ( $a^{\phi(n)} \equiv 1 \ mod \ n$ when $gcd(n, a) = 1$).

Originally, Fermat had made an observation for a special case restricted to prime numbers instead of $n$. After verifying it for several primes Fermat concluded it held true for all prime numbers; this was his version of induction, which Euler criticized in the introduction of his paper proving the very same formula (presented on August 2, 1736 to St. Petersburg Academy) before discovering the general version years later [2]. Euler proved it using induction as we know it today.

The standard proof, given by Euler himself in his 1759 paper, first shows $\phi(n)$ is multiplicative and then establishes the formula; that is, for every $m, l \in \mathbb{N}$ we have $\phi(ml) = \phi(m)\phi(l)$ and the closed form fomula follows from here.

**Theorem 1.1.** *If the integer $n \geq 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

The formula for Euler's $\phi$ Function has been proved using its multiplicative property and separately using group theory. Any textbook designed as an introduction to number theory will contain the former method [3]. The following proof makes use of two observations; one quite simple and the other quite subtle.

We shall ignore, at least directly, the multiplicative property altogether and approach the statement from a different point of view.

# Counting Consecutive Intervals

First let's agree on notation use. The notation $|G|$ is used in group theory to denote the order, or number of elements, of the group $G$. Similarly, this notation shall be used here to denote the number of elements in a set. Unless otherwise noted, all variables and constants are natural numbers.

We shall begin with the following lemma:

**Lemma 2.1.** *Define $G_k = \{r \in \mathbb{N} \mid 0 < r \leq kn \quad and \quad gcd(n, r) = 1\}$. Then $|G_k| = k\phi(n)$.*

*Proof.* Let $H$ be the set of numbers relatively prime to $n$ and not exceeding $n$. That is, $H = \{h \in \mathbb{N} \mid 0 < h \leq n \ \ and \ \ gcd(n, h) = 1\}$. By Definition 3, $|H| = \phi(n)$.

Any multiple of $n$ plus $h$, a number of the form $kn + h$, will contain no prime factor $p$ of $n$ because if $p|kn + h$, then $p|kn$ and $p|h$. But, we know that $p|kn$ and $p \nmid h$ since $p$ is a factor of $n$ and $gcd(n, h) = 1$. Thus, we get $gcd(kn + h, n) = 1$.

Since this last result holds for all $k \in \mathbb{N}$ and all $h \in H$, for any given $k$ there are exactly $|H| = \phi(n)$ relatively prime numbers to $n$ in $G = \{r \in \mathbb{N} \mid (k-1)n < r \leq kn \ \ and \ \ gcd(r, n) = 1\}$ . That is, in any interval between two consecutive multiples of $n$ there are exactly $\phi(n)$ relatively prime numbers to $n$.

Hence, $|G_k|$ is equal to the number of intervals of length $n$ times $\phi(n)$, or $|G_k| = k\phi(n)$. □

An argument in the proof is key to a result to come so we express it as a corollary:

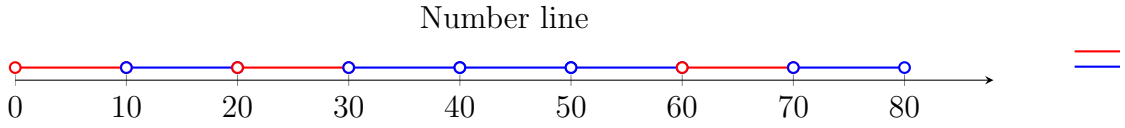
**Corollary.** *Define $G = \{r \in \mathbb{N} \mid (k-1)n < r \leq kn \ \ and \ \ gcd(r, n) = 1\}$, then $|G| = \phi(n)$.*

Consider $n = 10$, then $gcd(r, 10) = gcd(r+10, 10)$. Whichever the value of $r$, the left hand side will tell what the right hand side will be. Using this approach counting the number of relatively prime numbers between any consecutive multiples of 10 will be reduced to counting the number of relatively prime numbers to 10, namely $\phi(10)$.

For example, for 10 the numbers $1, 3, 7, 9$ share no factors with 10 and are less than 10. So we have $\phi(10) = 4$. Looking at the next interval, between 10 and 20, we can see that adding ten to the previously relatively prime numbers yield $\{11, 13, 17, 19\}$. These are exactly the numbers relatively prime to ten in that interval. The same holds true for the following interval, $\{21, 23, 27, 29\}$, and so on.

## Counting the Special Cases

Two cases will be considered for $\phi(pn)$, where $p$ could be any prime: when $gcd(p,n) = 1$ and when $gcd(p,n) = p$. To this end the intervals of our example have been colored. The red lines end with multiples $k$ of 10 where $gcd(k,10) = 1$ and the blue ones end where $gcd(k,10) > 1$. The lines that end in 30 and 70 are multiple 3 and multiple 7 of 10 respectively, hence red.




**Lemma 3.1.** *Let $p$ be a prime and $p|n$, then $\phi(pn) = p\phi(n)$.*

*Proof.* Notice that all the numbers that are relatively prime to $pn$ are also relatively prime to $n$. Since $gcd(pn,n) = n$ and $p|n$ the following result follows: $gcd(n,r) = 1$ if and only if $gcd(pn,r) = 1$ for any natural number $r$.

There are $p$ intervals, each with $\phi(n)$ numbers relatively prime to pn, hence by Lemma 2.1 the set $G_p = \{r \in \mathbb{N} | 0 < r < pn \ \ and \ \ gcd(n,r) = 1\}$ has $|G_p| = p\phi(n)$ elements. □

For our example we choose 10, so let's consider $2 \cdot 10$; $\phi(2 \cdot 10) = 2\phi(10) = 2(4) = 8$. Putting together the two sets mentioned in our previous example we have $\{1,3,7,9,11,13,17,19\}$, exactly all 8 numbers relatively prime to 20.

For 80 it holds, but care must be taken; we begin with $\phi(2 \cdot 40) = 2 \cdot \phi(40)$. Now we can apply the same argument again since 40 has a factor of 2, so $2 \cdot \phi(2 \cdot 20) = 2 \cdot 2 \cdot \phi(20)$. Repeating the same argument again $2 \cdot 2 \cdot \phi(2 \cdot 10) = 2 \cdot 2 \cdot 2 \cdot \phi(10) = 2 \cdot 2 \cdot 2 \cdot 4 = 32$. This can be checked by adding 10 to the set of four numbers relatively prime to 10 mentioned in the previous section. This will give the entire set relatively prime to 80, which has 32 elements in it.

Let's now examine $\phi(pn)$ when $p$ is not a factor of $n$.

**Lemma 3.2.** *Let $p$ be a prime and $p \nmid n$, then $\phi(pn) = (p-1)\phi(n)$.*

*Proof.* By Lemma 2.1 we know that $p\phi(n)$ is the number of numbers relatively prime to $n$ and less than $pn$. Notice that all the multiples of $p$ whose factors are relatively prime to $n$ are counted, since $gcd(p,n) = 1$. Notice the conditions imply $gcd(pn,r) = 1$ if and only if $gcd(n,r) = 1$ and $gcd(p,r) = 1$.

Suppose the list of multiples is $\{r_1p, r_2p, r_3p, ..., r_{\phi(n)}p\}$, where all the $r$'s are relatively prime to $n$. The set has $\phi(n)$ numbers relatively prime to $n$ and 0 relatively prime to $p$, because they are all multiples of $p$. We substract this many from our orignal count and we have $\phi(pn) = p\phi(n) - \phi(n) = (p-1)\phi(n)$. □

Pick 10, for example, and consider $3 \cdot 10$; $\phi(3 \cdot 10) = (3-1)\phi(10) = 2(4) = 8$. The set relatively prime to 10 is $\{1, 3, 7, 9\}$ and extending it three times we have $\{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29\}$. Notice the subset {3,9,21,27}; these numbers are all relatively prime to 10 and not relatively prime to 3. Excluding this subset we are left with $\{1, 7, 11, 13, 17, 19, 23, 29\}$, exactly all the 8 numbers relatively prime to 30.

# The General Case

We now have everything we need to prove the formula in the general case.

**Theorem.** *If the integer $n \geq 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

*Proof.* Applying Lemma 3.1 to all prime factors allows us to have the following formula: $\phi(p^{k_1} \cdots p_r^{k_r}) = p_1^{k_1-1} p_2^{k_2-1} \cdots p_r^{k_r-1} \phi(p_1 p_2 \cdots p_r)$.

Applying Lemma 3.2 we obtain $\phi(p_1 p_2 \cdots p_r) = (p_1 - 1)(p_2 - 1)...(p_r - 1)$. Therefore we have:

$$\phi(n) = p_1^{k_1-1} p_2^{k_2-1} \cdots p_r^{k_r-1}(p_1 - 1)(p_2 - 1)\cdots(p_r - 1)$$

Now we clean up by multiplying by 1 in the form of $\frac{p_s}{p_s}$ for all $1 \leq s \leq r$.

$$\begin{aligned}
\phi(n) &= \left(\frac{p_1}{p_1}\right)\left(\frac{p_2}{p_2}\right)...\left(\frac{p_r}{p_r}\right) p^{k_1-1} p^{k_2-1} \cdots p^{k_r-1}(p_1 - 1)(p_2 - 1)\cdots(p_r - 1) \\
&= p^{k_1} p^{k_2} \cdots p^{k_r}\left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right)\cdots\left(\frac{p_r - 1}{p_r}\right) \\
&= p^{k_1} p^{k_2} \cdots p^{k_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).
\end{aligned}$$

□

# References


[1] The Euler Archive, "E271 – Theorematа Arithmetica Nova Methodo Demonstrata". http://eulerarchive.maa.org/pages/E271.html, April, 2013.

[2] The Euler Archive, "E54 – Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio". http://eulerarchive.maa.org/pages/E054.htmll, April, 2013.

[3] Elementary Number Theory, David M. Burton, $7^{th}$ Edition, pg. 133-134.