# Euler's phi



**Author:** Jamal Abo Mokh
**Course:** 1040158 - Group Theory

## Question 1

---

**Lemma 1.1** let $(a, b) = 1$, let $x, y \in \mathbb{Z}$, then exists $Z \in \mathbb{Z}$ such that:

$$Z \bmod a = x$$

$$Z \bmod b = y$$

and it's unique.

*Proof.* since $(a, b) = 1$, then by bezouts identity, exist $\alpha, \beta \in Z$ such that:

$$a\alpha + b\beta = 1$$

hence, we have:

$$1 \equiv_a (a\alpha + b\beta) \equiv_a b\beta$$

applying the same with $b$, we obtain:

$$b\beta \equiv_a 1,\ a\alpha \equiv_b 1$$

therefore, we define:

$$Z = x(b\beta) + y(a\alpha)$$

hence,

$$Z \bmod a = x(b\beta) \bmod a = x \bmod a \cdot 1 = x \bmod a$$

and same with $b$.

Assume $Z'$ is another solution, therefore,

$$a, b \mid Z - Z'$$

hence since, $(a, b) = 1$, then:

$$ab \mid Z - Z'$$

since we assumed $Z, Z' < ab$, then we must have, $Z = Z'$ as required. □

let $\varphi$ be euler function.

**Definition 1.1**

$$R_n = \left\{ m : (n, m) = 1 \right\} \subset [n]$$

is the set of relative primes of $n$. note that we have:

$$\varphi(n) = |R_n|$$

**Lemma 1.2** let $(a, b) = 1$, then for any $c \in \mathbb{Z}$, we have:

$$\gcd(c, ab) = 1 \implies \gcd(c, a) = 1$$

*Proof.* assume otherwise, then exists $d > 1$ such that:

$$d \mid c, d \mid a$$

consequently,

$$d \mid c, d \mid ab$$

which means by the properties of the gcd:

$$1 < d \leq \gcd(c, ab)$$

in contradiction, hence, $\gcd(c, a) = 1$ as required. □

**Lemma 1.3** let $(a, b) = 1$, the function $f \colon R_{ab} \to R_a \times R_b$:

$$f(z) = (z \bmod a, z \bmod b)$$

is well-defined and bijective.

*Proof.* let $z \in R_{ab}$, therefore:

$$(z, ab) = 1$$

since we have:

$$x = z \bmod a, \ y = z \bmod b$$

therefore,

$$z = ma + x$$

consequently, by euclid theorem we have:

$$\gcd(z, a) = \gcd(ma + x, a) = \gcd(x, a)$$

hence, by lemma (1.2) we have:

$$\gcd(x, a) = \gcd(z, a) = \gcd(z, ab) = 1$$

same with $b$. as a result, $f$ is well-defined.

Let $(x, y) \in R_a \times R_b$, by lemma (1.1) (CRT), there exists a unique $z \leq ab$ such that:

$$f(z) = (x, y)$$

and we have:

$$\gcd(z, a) = \gcd(x, a) = 1$$

therefore, by a theorem, since $\gcd(z, a) = 1$, we have:

$$1 = \gcd(z, b) = \gcd(z, ab)$$

hence, $z \in R_{ab}$, therefore, $f$ is surjective.

and since if $z'$ is another number such that $z' < ab$ with:

$$f(z') = f(z)$$

then since by lemma (1.1) the solution is unique, we have:

$$z' = z$$

hence, $f$ is bijective as required.

□

**Corollary 1.1** for $a, b \in \mathbb{Z}$ such that $(a, b) = 1$:

$$\varphi(ab) = \varphi(a)\varphi(b)$$

*Proof.* take $(a, b) = 1$, then by the lemma (1.3) the function $f$ is bijective, therefore,

$$|R_{ab}| = |R_a||R_b|$$

since we have:

$$\varphi(x) = |R_x|$$

by definition, then:

$$\varphi(ab) = |R_{ab}| = |R_a||R_b| = \varphi(a)\varphi(b)$$

as required. □

**Claim 1.1** for $p \in \mathbb{P}$ we have:

$$\varphi(p) = p - 1$$

*Proof.* since $p$ is prime, then by definition, we have:

$$\forall 1 \leq x < p \;\; (x, p) = 1$$

therefore,

$$R_p = \{1, \ldots, p-1\} \implies \varphi(p) = p - 1$$

as required. □

**Lemma 1.4** let $p \in \mathbb{P}, k \in \mathbb{N}$, then:

$$(x, p) = 1 \iff (x, p^k) = 1$$

*Proof.* for the $\implies$ direction, let $d = (x, p^k)$, since we have:

$$d \mid p^k$$

then if $d \neq 1$, therefore,

$$p \mid d$$

hence,

$$p \mid x$$

which means $(x, p) = p$ in contradiction, therefore, $(x, p^k) = 1$.

Proving $\Longleftarrow$ direction, we have:

$$(x, p^k) = 1$$

therefore, we have:

$$p \nmid x$$

since otherwise, $(x, p^k) > 1$, hence, since

$$(x, p) \in \{1, p\}$$

and

$$(x, p) \mid x \ \wedge \ (x, p) \neq p$$

we must have:

$$(x, p) = 1$$

as required.

□

**Lemma 1.5** let $p \in \mathbb{P}$, then:

$$\exists n \in \mathbb{N} \ \ (x, p^n) = 1 \implies \forall k \in \mathbb{N} \ \ (x, p^k) = 1$$

*Proof.* we'll show that $(x, p) = 1$, and the result follows from (1.4). assume otherwise, then we have:

$$(x, p) \neq 1$$

since $p$ is prime, then we must have:

$$\gcd(x, p) = p$$

(since $\gcd(x,p) \mid p$), hence, we have:

$$p \mid x$$

therefore, since we also have:

$$p \mid p^n$$

then:

$$p \mid \gcd(x, p^n)$$

which is a contradiction to $\gcd(x,p^n) = 1$. □

**Claim 1.2** for $p \in \mathbb{P}$ we have:

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

*Proof.* first, we'll count the non coprime to $p^n$, therefore we define the function $f\colon [p^{n-1}] \to R^c_{p^n}$:

$$f(x) = px$$

first, it's clear that,

$$p \mid f(x)$$

therefore by lemma (1.4).

$$\gcd(p, f(x)) \neq 1 \implies \gcd(p^n, f(x)) \neq 1$$

hence, $f(x) \in R^c_{p^n}$ hence the function is well defined.

let $y \in R^c_{p^n}$, therefore, we have:

$$\gcd(y, p^n) > 1$$

since we have:

$$\gcd(y,p^n) \mid p^n \implies p \mid \gcd(y,p^n)$$

we conclude that:

$$\gcd(y,p) = p$$

therefore,

$$y = p \cdot m$$

for $m \in [p^{n-1}]$, hence,

$$f(m) = pm = y$$

as required.

the function is trivially injective. as a result, $f$ is bijective, therefore:

$$p^{n-1} = |\left[p^{n-1}\right]| = |R^c_{p^n}|$$

therefore, since the universe is $[p^n]$, we have:

$$|R_{p^n}| = p^n - |R^c_{p^n}| = p^n - p^{n-1}$$

consequently,

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

as required. □

**Claim 1.3** for any $n \in \mathbb{N}$, such that:

$$n = \prod_{p \in \mathbb{P}} p^{\alpha_p} = p_1^{\alpha_{p_1}} \dots p_s^{\alpha_{p_s}}$$

we have:

$$\varphi(n) = \prod_{p \in \mathbb{P}} (p^{\alpha_p} - p^{\alpha_p - 1})$$

*Proof.* proof by induction on $s$.

**Base Case.** for $s = 1$, we have:

$$n = p^{\alpha_p}$$

therefore, by (1.2), we have:

$$\varphi(n) = \varphi(p^{\alpha_p}) = p^{\alpha_p} - p^{\alpha_p - 1}$$

as required.

**Inductive Step.** let

$$x = p_1^{\alpha_{p_1}} \dots p_{s-1}^{\alpha_{p_{s-1}}},\ y = p_s^{\alpha_{p_s}}$$

therefore:

$$n = xy$$

and we have:

$$\gcd(x, y) = 1$$

therefore, by claim (1.1) we have:

$$\varphi(n) = \varphi(x)\varphi(y)$$

by the induction assumption we have:

$$\varphi(x) = \prod_{p \in \mathbb{P} \setminus \{p_s\}} p^{\alpha_p} - p^{\alpha_p - 1}$$

$$\varphi(y) = p_s^{\alpha_{p_s}} - p_s^{\alpha_{p_s} - 1}$$

therefore, in total we have:

$$\varphi(n) = \varphi(x)\varphi(y) = \prod_{p \in \mathbb{P}} p^{\alpha_p} - p^{\alpha_p - 1}$$

as required.

□

**Definition 1.2** for any $n \in \mathbb{N}$, define the set $P(n)$ as:

$$P(n) = \left\{ p : p \mid n \right\} \subset \mathbb{P}$$

which is the set of prime components of $n$.

**Lemma 1.6** if $d \mid p$, then:

$$P(d) \subset P(n)$$

*Proof.* assume otherwise, then exists $p \mid d$ prime, where,

$$p \notin P(n)$$

which means,

$$p \nmid n$$

which is a contradiction to $d \mid n$. hence:

$$P(d) \subset P(n)$$

as required. □

**Corollary 1.2** for each $n \in \mathbb{N}$, we have:

$$\varphi(n) = n \prod_{p \in P(n)} \left(1 - \frac{1}{p}\right)$$

*Proof.* by claim (1.3) we have:

$$\varphi(n) = \prod_{p \in P(n)} p^{\alpha_p} - p^{\alpha_p - 1}$$

therefore, we have:

$$\begin{aligned}
\varphi(n) &= \prod_{p \in P(n)} p^{\alpha_p} - p^{\alpha_p - 1} \\
&= \prod_{p \in P(n)} p^{\alpha_p}(1 - \frac{1}{p}) \\
&= \prod_{p \in P(n)} p^{\alpha_p} \prod_{p \in P(n)} (1 - \frac{1}{p}) \\
&= n \prod_{p \in P(n)} \left(1 - \frac{1}{p}\right)
\end{aligned}$$

as required. □

## Question 2

---

**Claim 2.1** let $N \in \mathbb{N}$, then:

$$|\varphi(N)^{-1}| \in \mathbb{N}$$

*Proof.* let $n \in \mathbb{N}$ such that:

$$\varphi(n) = N$$

since $n$ can be written as:

$$n = \prod_{p \in P} p^{\alpha_p}$$

where $P = P(n)$, then by claim (1.3), we have:

$$\begin{aligned} N = \varphi(n) &= \prod_{p \in P} (p^{\alpha_p} - p^{\alpha_p - 1}) \\ &= \prod_{p \in P} p^{\alpha_p - 1} \prod_{p \in P} (p - 1) \end{aligned}$$

therefore, we conclude that:

$$\forall p \in P(n) \;\; (p-1) \mid N$$

therefore, we must have:

$$\forall p \in P(n) \;\; p - 1 \leq N \implies p \leq N + 1$$

which means that the number of primes in the "pool" is finite.

since $N$ has a unique prime factorization, we have:

$$N = \prod_{p \in P(N)} p^{\beta_p}$$

therefore, since

$$p^{\beta_p + 1} \nmid N$$

then for each $p \in P(n)$, we must have:

$$\alpha_p \leq \beta_p + 1$$

hence, we take the following set:

$$S = \left\{ p : p - 1 \mid N \right\}$$

we conclude that, for the set:

$$T = \left\{ \prod_{p \in S} p^{k_p} : 0 \leq k_p \leq \beta_p + 1 \right\}$$

we have $n \in T$, moreover, it has the size:

$$|T| = \prod_{p \in S} \left( \beta_p + 1 \right)$$

hence, it's finite, as a result:

$$\varphi(N)^{-1} \subset T \implies |\varphi(N)| \in \mathbb{N}$$

as required. □

## Question 3

---

**Claim 3.1** let $n, d \in \mathbb{N}$, therefore:

$$d \mid n \implies \varphi(d) \mid \varphi(n)$$

*Proof.* by the assumption:

$$d \mid n$$

therefore,

$$P(d) \subset P(n)$$

and in particular,

$$\alpha_p(d) \leq \alpha_p(n)$$

as a result:

$$\forall p \in P(d) \;\; p^{\alpha_p(d)} - p^{\alpha_p(d)-1} \mid p^{\alpha_p(n)} - p^{\alpha_p(n)-1}$$

therefore, by claim (1.3) we have:

$$\varphi(d) = \prod_{p \in P(d)} \left( p^{\alpha_p(d)} - p^{\alpha_p(d)-1} \right) \mid \prod_{p \in P(n)} \left( p^{\alpha_p(n)} - p^{\alpha_p(n)-1} \right) = \varphi(n)$$

as required.

□