People's Democratic Republic Of Algeria
Ministry Of Higher Education And Scientific Research

Mohamed Boudiaf University Of M'sila
Faculty Of Mathematics And Computer Science
Department Of Mathematics

# *Master Thesis*

**Domaine** : Mathematics and Computer Science
**Track** : Mathematics
**Option** : Algebra and Discrete Mathematics

# Theme

## *Notes on Euler's phi function*

**Presented by :**
*REFICE* Habiba

**Before the jury composed of :**

| | | |
|---|---|---|
| AMROUNE Abdelaziz | University of M'sila | **President**. |
| BELLAOUAR Djamel | University of Guelma | **Supervisor**. |
| BOUDAOUD Abdelmadjid | University of M'sila | **Co-Supervisor**. |
| GHADBANE Nasser | University of M'sila | **Examiner**. |

University Year 2021/2022

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOHAMED BOUDIAF DE M'SILA
Faculté des Mathématiques et de l'Informatique
Département des Mathématiques
قسم الرياضيات

المسيلة في: / /

# تصريح بتصحيح مذكرة الماستر 2

أنا الممضي أسفله الأستاذ: بو داود عبد المجيد (نائب مؤطر)

مؤطر الطلبة الآتية أسماؤهم:

1- ارقيس حبيبة

2-

3-

أصرح بأنهم قد قاموا بتصحيح مذكرتهم المعنونة بـ:

Notes on Euler's phi function

وذلك تبعا للنصائح الموجهة لهم من طرف لجنة التقييم.

/

إمضاء الأستاذ المؤطر

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOHAMED BOUDIAF DE M'SILA
Faculté des Mathématiques et de l'Informatique
Département des Mathématiques
قسم الرياضيات
المسيلة في: / /
تصريح بتصحيح مذكرة الماستر 2
أنا الممضي أسفله الأستاذ: بو داود عبد المجيد (نائب مؤطر)
مؤطر الطلبة الآتية أسماؤهم:
1- ارقيس حبيبة
2-
3-
أصرح بأنهم قد قاموا بتصحيح مذكرتهم المعنونة بـ:
Notes on Euler's phi function
وذلك تبعا للنصائح الموجهة لهم من طرف لجنة التقييم.
/
إمضاء الأستاذ المؤطر

# Rremerciements

قال رسول لله صلى الله عليه وسلم "من لم يشكر الناس لم يشكر الله ومن اهدى إليكم معروفا فكافئوه فإن لم تستطيعوا فأدعو له "

- *I would like to thank my supervisor BELLAOUAR Djamel from University of Guelma who accompanied me throughout this research and provided me with valuable information and advice. I hope to God that he will pay his sins and achieve from us. May God reward him for all the good.*
- *I thank Assistant Co-supervisor BOUDAOUD Abdelmadjid at Mohamed Boudiaf University who instilled in me the hope and will to overcome the difficulties.*

- *I Also thank AMROUNE Abdelaziz and GHADBANE Nasser for agreeing to study this work and join this jury.*
- *Finally, I thank my family for their moral support and assistance. I also extend my sincere thanks and appreciation to all those who contributed to lighting my path with bright flag candles.*

# Dedicate

بسم الله الرحمان الرحيم

الى حجة الله على خلقه وسراجه في ارضه .....الى سليل الأخيار ونور الأنوار وزين الأبرار

الى ال محمد عليه أزكى الصلاة والسلام

الى من أفضلها على نفسي ولِما لا فلقد ضحت من أجلي

الى من ساندتني في صلاتها ودعائها .....الى من سهرت الليالي تنير دربي

الى من تشاركني افراحي وأساتي .....الى نبع العطف والحنان

الى أجمل ابتسامة في حياتي .....الى اروع أمرأه في الوجود

أمي الغالية حدة

الى من علمني أن الدنيا كفاح .....وسلاحها العلم والمعرفة

الى الذي لم يبخل علي بأي شيء .....الى من سعى لأجل راحتي ونجاحي

الى أعظم وأعز رجل في الكون

أبي العزيز العمراوي

الى الأعمدة الثابتة داخل قلبي .....وكل الأشياء التي أتباها بهم

كيف لا أحبهم ورب الكون قال فيهم ***"سنشد عضدك بأخيك "***

الى اخوتي وأخر العنقود مختار.....دون ان أنسى براعم العائلة أولاد اخوتي

الى كل عائلة ارفيس وقذيفة

الى من لقتني بهم الحياة صدفه فأسميتكم نصفي الثاني..... لأن احساسنا واحد وروحنا واحدة

ودموعنا واحدة صحيح انكم لستم ب أخوتي في دفتر العائلي انما انتم اخوتي في دفتر قلبي

صديقاتي فرح.سوسو.دودو. ميمي .لاتي .حسينة. فيفي.....

الى من له مكانة خاصة في قلبي

الى كل من تحمله ذاكرتي ولا تحمله مذكرتي

# Contents

# Résumé

L'objet de ce travail est d'étudier la fonction d'Euler $\varphi(n)$ et donner quelques relations avec les autres fonctions arithmétiques multiplicatives. Nous essayons de comprendre plusieurs équations Diophantiennes prouvées dans [1],[3],[6],[8] and [9]. Nous terminons notre travail en citant quelques problèmes ouverts faisant intervenir la fonction d'Euler.

**Mots clés.** Fonctions arithmétiques, Fonction d'Euler, équations Diophantiennes.

# Abstract

We say two numbers are relatively prime if they have no prime factors in common. For $n \geq 1$, the Euler's function $\varphi(n)$ denotes the number of positive integers not exceeding $n$ and relatively prime to $n$. In this work, we state some basic propertities of the Euler's function. That is, the behaviour of $\varphi(n)$, relations with other multiplicative functions and solving Diophantine equations involving the expression $\varphi(n)$.

**Keywords and phrases** Arithmetic functions, Euler's function, Diophantine equations and inequalities.

# Table of notations

| **Notation** | **Explanation** |
|---|---|
| $\mathbb{Z}$ | The set of integers |
| $\mathbb{N}$ | The set of positive integers |
| $n\|m$ | $n$ divides $m$ or $m$ is divisible by $n$ |
| $p^a \mid\mid n$ | $p^a$ divides $n$ but $p^{a+1}$ does not divide |
| $n \nmid m$ | $m$ is not divisible by $n$ or $n$ does not divide $m$ |
| $\pi(n)$ | The number of primes $\leq n$ |
| $d(n)$ or $\tau(n)$ | Number of positive divisors of $n$ |
| $\sigma(n)$ | Sum of positive divisors of $n$ |
| $\sigma_\alpha(n)$ | Generalized sum of divisors functions |
| $\varphi(n)$ | Euler's totient function |
| $\varphi_s$ | The generalized Euler's function |
| $\psi_s$ | The related Euler's function |
| $\omega(n)$ | The number of distinct prime factors of $n$ |
| $\Omega(n)$ | The total number of distinct prime factors of $n$ |
| $\Lambda(n)$ | Von Mangoldt function |
| $\lambda(n)$ | Liouville function |
| $id(n)$ | Identity function: $id(n)$; defined by $id(n) = n$ for all $n$ |
| $\mu(n)$ | Moebius function |
| $\gcd(m,n)$ or $(m,n)$ | The greatest common divisor of $m$ and $n$ |
| $\lfloor x \rfloor$ | The largest positive integer $\leq x$ |
| $\gamma(n)$ | The kernel of $n$ given by $\gamma(n) = \prod_{p\|n} p$. |
| $[m,n]$ | The least common multiple of $m$ and $n$. |

# Introduction

Fermat's little theorem tells us how to work with certain congruences involving exponents when the modulus is a prime [4, page 68]. How do we work with the corresponding congruences modulo a composite integer? For this purpose, we first define a special counting function called Euler's function, which counts the number of positive integers not exceeding $n$ and relatively prime to $n$. This number changes irregularly from a given number to another. For example, the number $n = 6$ has two positive integers $< 6$ and relatively prime to 6, while the number 7 has 6 positive integers $< 7$ and relatively prime to 7 and also the number 8 has 4 positive integers $< 8$ and relatively prime to 8. So, the expression which counts "*the number of positive integers not exceeding $n$ and relatively prime to $n$*" has a strange special behavior. In the case when $n$ is not a prime, is there a way to compute this expression? Recall that in the years 1750-1760 Euler [2] was the first who studied this expression and he gave it the notation $\varphi(n)$. By definition, it is clear that $\varphi(n) \leq n$. A similar definition, $\varphi(n)$ is the number of positive integers $\leq n$ and relatively prime to $n$, from which we have $\varphi(1) = 1$ or take this last equality as a convention.

An arithmetic function is an important function with many interesting properties frequently occurred in number theoretic investigations as well as

$\varphi(n)$ and many others. A multiplicative function is an arithmetic function $f(m)$ such that $f(mn) = f(m)f(n)$ for all pairs of relatively prime positive integers $m$ and $n$. If $f(m)$ is multiplicative, then it is easy to prove by induction on $k$ that if $m_1, ..., m_k$ are pairwise relatively prime positive integers, then $f(m_1...m_k) = f(m_1)...f(m_k)$. For details, see [5].

The goal of this work is to deal with important results about Euler's function. For example, we show that $\varphi$ is multiplicative and we give an explicit formula of $\varphi(n)$ in terms of the prime powers dividing $n$. We give examples on Fermat's Little Theorem and Euler's Theorem and we deal with some Diophantine equations and inequalities related to this function. Of course, based on the Fundamental Theorem of Arithmetic, we state with elementary proofs some classical results involving Euler's function and some other multiplicative functions. For further research, there are some open question at the end of this manuscript. Some other references, eg, see [1],[3],[6],[8] and [9].

# Chapter 1

# Elementary notions

## 1.1 Basic elements of arithmetic

Arithmetic Functions and the Fundamental Theorem of Arithmetic are two basic elements of arithmetic. Number-theoretic functions (or arithmetic functions) are the most fundamental functions in mathematics and computer science. For example, the computable functions studied in mathematical logic and computer science are actually arithmetic functions. In this chapter, we shall study some basic arithmetic functions that are useful in number theory [5]. But, in general, we shall present the most important properties of the Euler phi function. Recall that an *arithmetic function* is a function defined on the positive integers. Throughout this work we deal with arithmetic functions from $\mathbb{N}$ to itself.

**Definition 1.1** *Any nonzero function $f : \mathbb{N} \to \mathbb{C}$ (the set of complex numbers) is called an arithmetic function.*

**Example 1.1** *$f : \mathbb{N} \to \mathbb{N}$, $f(n) = n$ and $f(n) = n^2$ are arithmetic functions.*

**Definition 1.2** *An arithmetic function $f(n)$ is called multiplicative if*

$$f(mn) = f(m) f(n)$$

*for all positive integers $m$ and $n$ such that $(m, n) = 1$.*

In other words, a number-theoretic function $f$ is multiplicative if $f(mn) = f(m) f(n)$ whenever $m$ and $n$ are relatively prime. For example, the constant function $f(n) = 1$ is multiplicative, since $f(mn) = 1 = 1 \cdot 1 = f(m)f(n)$. So is the function $g(n) = n^k$, $k$ being a fixed integer, since $g(mn) = (mn)^k = m^k \cdot n^k = g(m)g(n)$.

**Example 1.2** *If $f(n) = n$, then $f(mn) = mn$ so $f$ is multiplicative. If $g(n) = 2n$, then $g(mn) = 2mn \neq g(m) g(n)$, and hence $g$ is not multiplicative.*

**Definition 1.3 (Totally multiplicative Arithmetic function)** *If $f(n)$ is an arithmetic function such that $f(mn) = f(m) f(n)$ for all $m, n$, then $f(n)$ is said to be totally multiplicative arithmetic function. For example, $f(n) = n^2$ is totally multiplicative.*

**Remark 1.1** *The following are two basic properties of multiplicative functions:*

1. *If $f$ and $g$ are multiplicative functions such that $f(p^a) = g(p^a)$ for all primes $p$ and all integers $a$, then $f(n) = g(n)$ for all positive integers. That is $f = g$.*

2. *If $f$ and $g$ are totally multiplicative functions such that $f(p) = g(p)$ for all primes $p$, then $f = g$.*

**Theorem 1.1 (The Fundamental Theorem of Arithmetic)** *Every integer $n \geq 2$ either is a prime or can be expressed as a product of primes. The factorization into primes is unique except for the order of the factors.*

The *canonical decomposition* of a positive integer $n$ is of the form $n = q_1^{a_1} q_2^{a_2} ... q_k^{a_k}$, where $q_1, q_2, ..., q_k$ are distinct primes with $q_1 < q_2 < ... < q_k$ and $a_1, a_2, ..., a_k$ are positive integers. For example, we find the canonical decomposition of 2020 and 2520. Simple computation, we get $2020 = 2^2 \cdot 5 \cdot 101$ and $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$. Moreover, note that any positive integer $n$ can be written as $n = 2^a \cdot m$, where $m \geq 1$ is odd. That is, $\gcd(2, m) = 1$. In this case, if we have a multiplicative function $f$, then $f(n) = f(2^a) \cdot f(m)$. Thus, $\varphi(2^a \cdot m) = \varphi(2^a) \cdot \varphi(m)$.

**Theorem 1.2** *If $f$ is a multiplicative function and if $n = q_1^{a_1} q_2^{a_2} ... q_k^{a_k}$, where $q_1, q_2, ..., q_k$ are distinct primes and $a_1, a_2, ..., a_k$ are positive integers, then*

$$f(n) = f(q_1^{a_1}) \cdot f(q_2^{a_2}) \cdot ... \cdot f(q_k^{a_k}).$$

**Proof.** Since $f$ is multiplicative and $\gcd(q_1^{a_1}, q_2^{a_2} ... q_k^{a_k}) = 1$, we see that

$$f(n) = f(q_1^{a_1} q_2^{a_2} ... q_k^{a_k}) = f(q_1^{a_1} \cdot q_2^{a_2} ... q_k^{a_k}) = f(q_1^{a_1}) \cdot f(q_2^{a_2} ... q_k^{a_k}).$$

Since $\gcd(q_2^{a_2}, q_3^{a_3} ... q_k^{a_k}) = 1$ we also have

$$f(q_2^{a_2} ... q_k^{a_k}) = f(q_2^{a_2}) \cdot f(q_3^{a_3} ... q_k^{a_k}),$$

so that $f(n) = f(q_1^{a_1}) \cdot f(q_2^{a_2}) \cdot f(q_3^{a_3} ... q_k^{a_k})$. Continuing in this way, we find that $f(n) = f(q_1^{a_1}) \cdot f(q_2^{a_2}) \cdot ... \cdot f(q_k^{a_k})$. ■

## 1.2 Definitions of some important arithmetic functions

We state the definition of basic arithmetic functions and we illustrate an example for each function. For details, one can see [2] and [5].

1. **Divisor function**[1]: $d(n)$, the number of positive divisors of $n$ (including the trivial divisors $d = 1$ and $d = n$). As usual, the notation "$d|n$" as the range for a sum or product means that $d$ ranges over the positive divisors of $n$. Thus, the number of divisors function is given by

$$\sum_{d|n} 1.$$

For example, the positive divisors of 15 are $1, 3, 5$, and 15. So $d(15) = 4$. Note that if $p$ is prime, $d(p) = 2$. Recall that if $n = q_1^{a_1} q_2^{a_2} ... q_k^{a_k}$, where $q_1, q_2, ..., q_k$ are distinct primes and $a_1, a_2, ..., a_k$ are positive integers, then

$$d(n) = (a_1 + 1)(a_2 + 1) ... (a_k + 1). \tag{1.1}$$

For example, we compute $d(36)$ and $\sigma(36)$. Because $36 = 2^2 \cdot 3^2$, where $(2^2, 3^2) = 1$, by (1.1), $d(36) = d(2^2) \cdot d(3^2) = 9$.

2. **Sum of divisors function:** $\sigma(n)$, the sum over all positive divisors of $n$; i.e.,

$$\sigma(n) = \sum_{d|n} d.$$

[1] Another common notation for the divisor function is $\tau(n)$.

For each integer $n \geq 2$ written in its canonical form $n = q_1^{a_1} q_2^{a_2} ... q_k^{a_k}$, as in (1.1), we have the following explicit formula:

$$\sigma(n) = \prod_{i=1}^{k} \frac{q_i^{a_i+1} - 1}{q_i - 1}.$$

3. **Generalized sum of divisors functions:** $\sigma_\alpha(n)$, defined by $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$. Here $\alpha$ can be any real or complex parameter. This function generalizes the divisor function ($\alpha = 0$) and the sum of divisors function ($\alpha = 1$).

4. **Number of distinct prime factors:** $\omega(n)$, defined by $\omega(1) = 0$ and $\omega(n) = k$ if $n \geq 2$ and $n = q_1^{\alpha_1} q_2^{\alpha_2} ... q_k^{\alpha_k}$. That is, $\omega(n) = \sum_{p|n} 1$. For example, if $n = 2021$, then $\omega(n) = 2$. Moreover, since $2022 = 2 \cdot 3 \cdot 337$ we have $\omega(2022) = 3$.

5. **Identity function:** $id(n)$; defined by $id(n) = n$ for all $n$.

6. **Moebius function:** $\mu(n)$, defined by $\mu(1) = 1$, $\mu(n) = 0$ if $n$ is not square-free (i.e., divisible by the square of a prime), and $\mu(n) = (-1)^k$ if $n$ is composed of $k$ distinct prime factors (i.e., $n = q_1 q_2 ... q_k$, where $q_1, q_2, ..., q_k$ are distinct primes. For example, $2020 = 2^2 \cdot 5 \cdot 101$, $2021 = 43 \cdot 47$, and so $\mu(2020) = 0$, $\mu(2021) = 1$ and $\mu(2022) = -1$.

7. **Liouville function:** $\lambda(n)$, defined by $\lambda(1) = 1$ and $\lambda(n) = (-1)^k$ if $n$ is composed of $k$ not necessarily distinct prime factors (i.e., if $n = q_1^{\alpha_1} q_2^{\alpha_2} ... q_k^{\alpha_k}$, then $\lambda(n) = \prod_{i=1}^{k} (-1)^{\alpha_i}$.

8. **Von Mangoldt function:** $\Lambda(n)$, defined by $\Lambda(n) = 0$ if $n$ is not a prime power, and $\Lambda(p^m) = \log p$ for any prime power $p^m$.

9. **Total number of prime divisors:** $\Omega(n)$, defined in the same way as $\omega(n)$, except that prime divisors are counted with multiplicity. Thus, $\Omega(1) = 0$ and $\Omega(n) = \sum_{i=1}^{k} \alpha_i$ if $n \geq 2$ and $n = q_1^{\alpha_1} q_2^{\alpha_2} ... q_k^{\alpha_k}$, i.e., $\Omega(n) = \sum_{p^m|n} 1$ For square-free integers $n$, the functions $\omega(n)$ and $\Omega(n)$ are equal and are related to the Moebius function by $\mu(n) = (-1)^{\omega(n)}$. For all integers $n$, $\lambda(n) = (-1)^{\Omega(n)}$.

10. $\pi(x)$: The number of primes $\leq x$. For example, $\pi(5.3) = 3$.

# Chapter 2

# On the properties of phi function

**Definition 2.1** *The Euler phi function $\varphi(n)$ is the arithmetic function that counts the number of integers in the set $1, 2, ..., n-1$ that are relatively prime to $n$.*

We can also write from the above definition

$$\varphi(n) = \sum_{\substack{1 \leq k < n \\ \gcd(k,n)=1}} 1.$$

Let us take the first numbers $1, 2, ..., 8$. We have:

- $\varphi(1) = 1$. The only number $n$ such that, $\gcd(n, 1) = 1$ is 1 itself.
- $\varphi(2) = 1$. The only number $n$ such that, $\gcd(n, 2) = 1$ is 1.
- $\varphi(3) = 2$. The only number $n$ such that, $\gcd(n, 3) = 1$ are $1, 2$.
- $\varphi(4) = 2$. The only number $n$ such that, $\gcd(n, 4) = 1$ are $1, 3$.
- $\varphi(5) = 4$. The only number $n$ such that, $\gcd(n, 5) = 1$ are $1, 2, 3, 4$.

- $\varphi(6) = 2$. The only number $n$ such that, $\gcd(n, 6) = 1$ are $1, 5$.
- $\varphi(7) = 6$. The only number $n$ such that, $\gcd(n, 7) = 1$ are $1, 2, 3, 4, 5, 6$.
- $\varphi(8) = 4$. The only number $n$ such that, $\gcd(n, 8) = 1$ are $1, 3, 5, 7$.

Moreover, by Definition 2.1, we also have

$$\begin{array}{lll} \varphi(9) = 6, & \varphi(13) = 12, & \varphi(17) = 16, \\ \varphi(10) = 4, & \varphi(14) = 6, & \varphi(18) = 6, \\ \varphi(11) = 10, & \varphi(15) = 8, & \varphi(19) = 18, \\ \varphi(12) = 4, & \varphi(16) = 8, & \varphi(20) = 8. \end{array}$$

We now start with some properties of Euler's function. First, we consider its values at primes[1] and then at prime powers. First, note that $\varphi(n) = n$ if and only $n = 1$. This follows from the fact that if $f$ is a multiplicative function, then $f(1) = 1$.

**Theorem 2.1** *Let $n$ be a positive integer. Then*

1. *If $n$ is a prime, namely $n = p$, then $\varphi(n) = \varphi(p) = p - 1$. Conversely, if $n$ is a positive integer with $\varphi(n) = n - 1$, then $n$ is prime. Thus, $\varphi(n) = n - 1$ if and only if $n$ is prime.*
2. *If $n$ is a prime power $p^a$ with $a \geq 1$, then*

$$\varphi(p^a) = p^{a-1}(p - 1). \tag{2.1}$$

**Proof.** We present the proof as follows:

[1] If $p$ is a prime number, then $(a, p) = 1$ for $a = 1, ..., p - 1$, and so $\varphi(p) = p - 1$. In addition, no composite number $m$ exists such that $\varphi(m) = m - 1$ and this was conjectured by Lehmer [3] more than half a century ago and it is yet to be established.

1. If $n$ is a prime, then every positive integer less than $n$ is relatively prime to $n$. Since there are $n-1$ such integers, we have $\varphi(n) = n-1$. Conversely, if $n$ is composite, then $n$ has a divisor $d$ with $1 < d < n$ and of course, $n$ and $d$ are not relatively prime. Since we know that at least one of the $n-1$ integers $1, 2, ..., n-1$, namely $d$, is not relatively prime to $n$, we have $\varphi(n) \leq n-2$. Hence, if $\varphi(p) = p-1$, then $p$ must be prime.

2. The positive integers less than $p^a$ that are not relatively prime to $p$ are those integers not exceeding $p^a$ that are divisible by $p$. That is, the numbers

$$p, 2 \cdot p, 3 \cdot p, ..., p^{a-1} \cdot p^a.$$

There are exactly $p^{a-1}$ such integers, so there are $p^a - p^{a-1}$ integers less than $p^a$ that are relatively prime to $p^a$. Hence, $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$.

The proof is finished. ■

**Remark 2.1** *$\varphi(p^a)$ = number of positive integers $\leq p^a$ and relatively prime to it =(number of positive integers $\leq p^a$) - (number of positive integers $\leq p^a$ and not relatively prime to it).*

Notice that the value $\varphi(p^a)$ can also be written as

$$\varphi(p^a) = p^a\left(1 - \frac{1}{p}\right). \tag{2.2}$$

We will find this version useful in Theorem 2.3.

**Example 2.1** *Let* $n = 11$. *The numbers* $1, 2, 3, 4, 5, 6, 7, 8, 9$ *and* $10$ *are all relatively prime to* $11$. *Thus,* $\varphi(11) = 10$. *Also, applying* (2.1), *we find that* $\varphi(5^3) = 5^2(5-1) = 100$, $\varphi(2^x) = 2^{x-1}$ *and* $\varphi(11^x) = 2 \cdot 5 \cdot 11^{x-1}$.

- If $\varphi(p^a)$ is a square, then $p-1$ must be a square and $a$ must be odd. In fact, since $\varphi(p^a) = p^{a-1}(p-1)$ where $\gcd(p^{a-1}, p-1) = 1$, we deduce that $\varphi(p^a)$ is a square if and only if $a$ is odd and $p-1$ must be a square. But, if $p$ is odd then $p = 2^x + 1$.

## 2.1 Euler's function is multiplicative

Now, to present a formula for $\varphi(n)$ by using the prime factorization of $n$, we must show that $\varphi$ is *multiplicative*. Thus, by applying Theorem 1.2, we obtain the explicit expression of $\varphi(n)$. Let us start with the following example:

**Example 2.2** *Let* $m = 4$ *and* $n = 9$, *so that* $mn = 36$. *We list the integers from* $1$ *to* $36$ *in the following rectangular*

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **1** | **5** | 9 | **13** | **17** | 21 | **25** | **29** | 33 |
| 2 | 6 | 10 | 14 | 18 | 22 | 26 | 30 | 34 |
| 3 | **7** | **11** | 15 | **19** | **23** | 27 | **31** | **35** |
| 4 | 8 | 12 | 16 | 20 | 24 | 28 | 32 | 36 |

*Neither the second nor fourth row contains integers relatively prime to* $36$, *since each element in these rows is not relatively prime to* $4$, *and hence not relatively prime to* $36$. *In the other two rows, each elements of these rows is relatively prime to* $4$. *But, there are* $6$ *integers in each row relatively prime to* $9$. *Thus, there are* $12$ *integers in the list relatively prime to* $36$. *Hence,* $\varphi(36) = \varphi(4)\varphi(9) = 2 \cdot 6 = 12$. *As a conclusion, there are two rows where*

*their elements are relatively prime to* 4 *and each of these rows contains* 6 *integers relatively prime to* 9.

*Let* $m = 6$ *and* $n = 11$*, so that* $mn = 66 = 2 \times 3 \times 11$*. As above, we obtain*

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 7 | 13 | 19 | 25 | 31 | 37 | 43 | 49 | **55** | 61 |
| 2 | 8 | 14 | 20 | 26 | 32 | 38 | 44 | 50 | 56 | 62 |
| 3 | 9 | 15 | 21 | 27 | 33 | 39 | 45 | 51 | 57 | 63 |
| 4 | 10 | 16 | 22 | 28 | 34 | 40 | 46 | 52 | 58 | 64 |
| 5 | **11** | 17 | 23 | 29 | 35 | 41 | 47 | 53 | 59 | 65 |
| 6 | 12 | 18 | 24 | 30 | 36 | 42 | 48 | 54 | 60 | 66 |

*There are two rows where their elements are relatively prime to* 6 *and each of these rows contains* 10 *integers relatively prime to* 11*. Hence,* $\varphi(66) = \varphi(6)\varphi(11) = 2 \cdot 10 = 20$.

**Theorem 2.2** *Let* $m$ *and* $n$ *be relatively prime positive integers. Then* $\varphi(mn) = \varphi(m)\varphi(n)$*. That is, Euler's function is multiplicative.*

**Proof.** Let $m$ and $n$ be positive integers such that $(m, n) = 1$. We would like to show that $\varphi(mn) = \varphi(m)\varphi(n)$. We display the positive integers not exceeding $mn$ in the following way:

| | | | | |
|---|---|---|---|---|
| $1$ | $m+1$ | $2m+1$ | $\dots$ | $(n-1)m+1$ |
| $2$ | $m+2$ | $2m+2$ | $\dots$ | $(n-1)m+2$ |
| $3$ | $m+3$ | $2m+3$ | $\dots$ | $(n-1)m+3$ |
| $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ |
| $m-1$ | $2m-1$ | $3m-1$ | $\dots$ | $(n-1)m+m-1$ |
| $m$ | $2m$ | $3m$ | $\dots$ | $mn$ |

Let $r$ be a positive integer $\leq m$ such that $(r, m) > 1$. We will show that no element of the $r$th row in the array is relatively prime to $mn$. Let $d = (r, m)$.

Then $d \mid r$ and $d \mid m$, so $d \mid km + r$ for any integer $k$; that is, $d$ is a factor of every element in the $r$th row. Thus, no element in the $r$th row is relatively prime to $m$ and hence to $mn$ if $(r, m) > 1$; in other words, the elements in the array relatively prime to $mn$ come from the $r$th row only if $(r, m) = 1$. By definition, there are $\varphi(m)$ such integers $r$ and hence $\varphi(m)$ such rows.

Now let us concentrate on the $r$th row, where$(r, m) = 1$:

$$r, m + r, 2m + r, ..., (n - 1)m + r$$

So the least residues modulo $n$ are a permutation of $0, 1, 2, ..., (n-1)$ of which $\varphi(n)$ are relatively prime to $n$. Therefore, exactly $\varphi(n)$ elements in the $r$th row are relatively prime to $n$ and hence to $mn$. Thus, there are $\varphi(m)$ rows containing positive integers relatively prime to $mn$, and each row contains $\varphi(n)$ elements relatively prime to it. So the array contains $\varphi(n)\varphi(m)$ positive integers n $\leq mn$ and relatively prime to $mn$; that is, $\varphi(mn) = \varphi(m)\,\varphi(n)$.

■

Consider another example, let $m = 4$ and $n = 7$. Then $\gcd(m, n) = 1$ and $mn = 28$. To find $\varphi(mn) = \varphi(28)$, we list the positive integers $\leq 28$ in four rows of 7 each and then ignore the ones that are not relatively prime to 28 (see the following table):

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 5 | 9 | 13 | 17 | 21 | 25 |
| 2 | 6 | 10 | 14 | 18 | 22 | 26 |
| 3 | 7 | 11 | 15 | 19 | 23 | 27 |
| 4 | 8 | 12 | 16 | 20 | 24 | 28 |

Clearly, the first element in the second and fourth rows is not relatively prime to $m$; in fact, no element in either row is relatively prime to $m$. So none of them is relatively prime to $mn$. Consequently, the positive integers $\leq 28$ and

relatively prime to it must come from the $2 = \varphi(4)$ remaining rows:

$$\begin{array}{cccccccc} 1 & 5 & 9 & 13 & 17 & 21 & 25 \\ 3 & 7 & 11 & 15 & 19 & 23 & 27 \end{array}$$

Each of them is relatively prime tom. Each row contains $6 = \varphi(7)$ elements relatively prime to $n = 7$:

$$\begin{array}{cccccc} 1 & 5 & 9 & 13 & 17 & 25 \\ 3 & 11 & 15 & 19 & 23 & 27 \end{array}$$

The resulting array contains 12 elements and they are indeed relatively prime to 28. Thus, $\varphi(28) = 12 = 2 \cdot 6 = \varphi(4)\varphi(7)$.

**Theorem 2.3** *Let $n = q_1^{a_1} q_2^{a_2} ... q_k^{a_k}$, where $q_1, q_2, ..., q_k$ are distinct primes and $a_1, a_2, ..., a_k$ are positive integers. Then*

$$\varphi(n) = q_1^{a_1-1}(q_1 - 1)\, q_2^{a_2-1}(q_2 - 1) \dots q_k^{a_k-1}(q_k - 1) = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{2.3}$$

**Proof.** Since $\varphi$ is multiplicative, by Theorem 2.2, we obtain

$$\varphi(n) = \varphi(q_1^{a_1}) \cdot \varphi(q_2^{a_2}) \cdot ... \cdot \varphi(q_k^{a_k}).$$

In addition, from Theorem 2.1 we know that

$$\varphi(q_i^{a_i}) = q_i^{a_i} - q_i^{a_i-1} = q_i^{a_i}\left(1 - \frac{1}{q_i}\right), \text{ for } i = 1, 2, ..., k.$$

Hence,

$$\begin{aligned} \varphi(n) &= q_1^{a_1}\left(1 - \frac{1}{q_1}\right) \cdot q_2^{a_2}\left(1 - \frac{1}{q_2}\right) \cdot ... \cdot q_k^{a_k}\left(1 - \frac{1}{q_k}\right) \\ &= q_1^{a_1} q_2^{a_2} ... q_k^{a_k}\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) ... \left(1 - \frac{1}{q_k}\right) \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right). \end{aligned}$$

This is the desired formula for $\varphi(n)$. ■

We illustrate the use of Theorem 2.3 with the following example.

**Example 2.3** *Let* $n = 100 = 2^2 \cdot 5^2$. *Then* $\varphi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$. *For* $n = 2022 = 2 \cdot 3 \cdot 337$. *Then*

$$\varphi(n) = 2022\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{337}\right) = 672.$$

**Remark 2.2** *Note that if* $n$ *is square-free. That is,* $n = q_1 q_2 ... q_k$, *where* $q_1, q_2, ..., q_k$ *are distinct primes, then* $\varphi(n) = (q_1 - 1)(q_2 - 1)...(q_k - 1)$.

**Remark 2.3** *Let* $n \geq 2$. *We have* $2^{\omega(n)-1} \mid \varphi(n)$. *In fact, since* $2 \mid q_i - 1$ *for* $i = 2, ..., k$ *we deduce that* $2^{\omega(n)-1} \mid (q_2 - 1)...(q_k - 1)$ *and so* $2^{\omega(n)-1} \mid \varphi(n)$.

Also, we have:

- If $n \equiv 0\,(mod 4)$, then $\varphi(n/2) = \varphi(n)/2$.
- If $p \nmid n$, then $\varphi(pn) = (p-1)\varphi(n)$.
- If $\varphi(pn) = (p-1)\varphi(n)$, then $p \nmid n$.

**Corollary 2.1** *Let* $f(n) = \dfrac{\varphi(n)}{n}$. *Then* $f(p^a) = f(p)$ *for all primes* $p$ *and all positive integers* $a$.

**Proof.** In fact, by (2.2), we have

$$f(p^a) = \frac{\varphi(p^a)}{p^a} = \frac{p^a\left(1-\frac{1}{p}\right)}{p^a} = \left(1-\frac{1}{p}\right) = \frac{p-1}{p} = f(p).$$

The proof is finished. ■

**Theorem 2.4** *Let $m, n \in \mathbb{N}$, and let $d = \gcd(m, n)$. Then*

$$\varphi(mn) = \varphi(n)\,\varphi(m)\,\frac{d}{\varphi(d)}. \tag{2.4}$$

**Proof.** Suppose $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ and $m = q_1^{b_1} q_2^{b_2} ... q_s^{b_s}$. Then

$$\begin{aligned} \varphi(mn) &= \varphi\left(p_1^{a_1} p_2^{a_2} ... p_k^{a_k} \cdot q_1^{b_1} q_2^{b_2} ... q_s^{b_s}\right) \\ &= mn \prod_{p|mn} \left(1 - \frac{1}{p}\right). \end{aligned}$$

Or equivalently, we have

$$\frac{\varphi(mn)}{mn} = \prod_{p|mn} \left(1 - \frac{1}{p}\right) = \frac{\prod\limits_{p|m} \left(1 - \frac{1}{p}\right) \prod\limits_{p|n} \left(1 - \frac{1}{p}\right)}{\prod\limits_{p|d} \left(1 - \frac{1}{p}\right)},$$

where $d = \gcd(m, n)$. Therefore,

$$\frac{\varphi(mn)}{mn} = \frac{\frac{\varphi(m)}{m} \cdot \frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}} = \frac{1}{mn} \varphi(m)\,\varphi(n)\,\frac{d}{\varphi(d)}.$$

Thus, $\varphi(mn) = \varphi(m)\,\varphi(n)\,\dfrac{d}{\varphi(d)}$. This proves (2.4). ■

**Remark 2.4** *If $\gcd(m, n) = p$ with $p$ is prime, then $\varphi(mn) = \frac{p}{p-1} \varphi(m)\,\varphi(n)$. Thus, if $p$ is sufficiently large, then $\varphi(mn)$ and $\varphi(m)\,\varphi(n)$ are equivalent.*

Next, we present an important divisibility formula.

**Proposition 2.1** *If $d \mid n$, then $\varphi(d) \mid \varphi(n)$.*

**Proof.** Assume that $n = q_1^{a_1} q_2^{a_2} ... q_k^{a_k}$, where $q_1, q_2, ..., q_k$ are distinct primes and $a_1, a_2, ..., a_k$ are positive integers. Let $d = q_1^{b_1} q_2^{b_2} ... q_k^{b_k}$, where $0 \leq b_i \leq a_i$ for $i = 1, 2, ..., k$. Then

$$\varphi(n) = q_1^{a_1-1}(q_1 - 1) q_2^{a_2-1}(q_2 - 1) \dots q_k^{a_k-1}(q_k - 1)$$

and

$$\varphi(d) = q_1^{b_1-1}(q_1 - 1) q_2^{b_2-1}(q_2 - 1) \dots q_k^{b_k-1}(q_k - 1).$$

Since $0 \leq b_i \leq a_i$, we have

$$\begin{aligned} \frac{\varphi(n)}{\varphi(d)} &= \frac{q_1^{a_1-1}(q_1 - 1) q_2^{a_2-1}(q_2 - 1) \dots q_k^{a_k-1}(q_k - 1)}{q_1^{b_1-1}(q_1 - 1) q_2^{b_2-1}(q_2 - 1) \dots q_k^{b_k-1}(q_k - 1)} \\ &= q_1^{a_1-b_1} q_2^{a_2-b_2} ... q_k^{a_k-b_k}, \end{aligned}$$

which is a positive integer. The proof is finished. ■

**Example 2.4** *Let $n = 2022 = 2 \cdot 3 \cdot 337$ and let $d = 6$. Then*

$$\varphi(n) = (2-1) \cdot (3-1) \cdot (337-1) = 672.$$

*and $\varphi(d) = \varphi(6) = (2-1) \cdot (3-1) = 2$. Thus, $d \mid n$ and $\varphi(d) \mid \varphi(n)$.*

**Theorem 2.5 (Fermat's Little Theorem)** *If $p$ is prime, and $a$ is relatively prime to $p$, then $a^{p-1} \equiv 1 \pmod{p}$.*

For example, if $p = 11$ and $a = 6$ which is relatively prime to 11. By Theorem 2.5, $6^{10} \equiv 1 \pmod{11}$. In fact, $6^{10} = 2^{10} \cdot 3^{10} - 1 = 60466175 = 5^2 \cdot 7 \cdot 11 \cdot 101 \cdot 311$.

**Theorem 2.6 (Euler's Theorem)** *If $a$ and $n$ are relatively prime, then*

$$a^{\varphi(n)} \equiv 1 \,(\text{mod } n)\,.$$

For example, if $n = 8$ and $a = 9$ which is relatively prime to 8. By Theorem 2.6, $9^{\varphi(8)} \equiv 1 \,(\text{mod } 8)$. In fact, $9^{\varphi(8)} = 9^4 = 6561 - 1 = 6560 = 2^5 \cdot 5 \cdot 41$.

**Theorem 2.7** *Let $a$ and $m$ be positive integers such that $\gcd(a, m) = 1 = \gcd(a - 1, m)$. Then*

$$1 + a + a^2 + ... + a^{\varphi(m)-1} \equiv 0 \,(\text{mod } m)\,. \tag{2.5}$$

**Example 2.5** *Let $a = 3$ and $m = 11$. Then*

$$\begin{aligned} 1 + 3 + 3^2 + ... + 3^{\varphi(11)-1} &= 1 + 3 + 3^2 + ... + 3^9 \\ &= 29524 = 2^2 \cdot 11^2 \cdot 61 \\ &\equiv 0 \,(\text{mod } 11)\,. \end{aligned}$$

**Theorem 2.8** *Let $m_1, m_2, ..., m_k$ be any positive integers and $a$ any integer such that $\gcd(a, m_i) = 1$ for $1 \leq i \leq k$. Then*

$$a^{[\varphi(m_1),\varphi(m_2),...,\varphi(m_k)]} \equiv 1 \,(\text{mod } \ [m_1, m_2, ..., m_k])\,.$$

**Corollary 2.2** *Let $m_1, m_2, ..., m_k$ be pairwise relatively prime integers and $a$ any integer such that $\gcd(a, m_i) = 1$ for $1 \leq i \leq k$. Then*

$$a^{[\varphi(m_1),\varphi(m_2),...,\varphi(m_k)]} \equiv 1 \,(\text{mod } m_1 m_2 ... m_k)\,.$$

**Example 2.6** *Let* $m_1 = 3, m_2 = 4, m_k = 5$ *and* $a = 7$. *Then*

$$a^{[\varphi(m_1),\varphi(m_2),...,\varphi(m_k)]} = 7^{[2,2,4]} = 7^4 = 2401 = 1 + 2^5 \cdot 3 \cdot 5^2.$$

*That is,* $7^4 \equiv 1 \pmod{3 \cdot 4 \cdot 5}$.

**Proposition 2.2** *If* $n$ *has at most nine distinct prime factors, that is* $\omega(n) \leq 9$, *then* $\varphi(n) > \dfrac{n}{7}$.

**Proof.** Let $k$ be a positive integer with $k \leq 9$ and assume that $n = q_1^{a_1} q_2^{a_2} ... q_k^{a_k}$, where $q_1, q_2, ..., q_k$ are distinct primes and $a_1, a_2, ..., a_k$ are positive integers. Since $q_i \geq p_i$ for $i = 1, 2, ..., k$, we conclude that

$$\begin{aligned} \frac{\varphi(n)}{n} &= \prod_{i=1}^{k} \left(1 - \frac{1}{q_i}\right) \geq \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \geq \prod_{i=1}^{9} \left(1 - \frac{1}{p_i}\right) \\ &= \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) ... \left(1 - \frac{1}{23}\right) = \frac{110\,592}{676\,039} > \frac{1}{7}. \end{aligned}$$

The proof of Proposition 2.2 is finished. ■

**Corollary 2.3** *Let* $n \geq 2$. *Then* $\varphi(n) = n - 2$ *if and only if* $n = 4$.

**Proof.** If $n = 4$, then $\varphi(n) = 2 = n - 2$. Conversely, if $\varphi(n) = n - 2$, then

$n$ must have exactly one proper divisor, and it follows that $n = p^2$ for some prime $p$. Hence, $\varphi(n) = p(p-1)$. Assuming this equal to $p^2 - 2$, we obtain that $p = 2$, and so $n = 4$. ■

**Example 2.7** *Let* $n = 28$ *and* $d \mid 28$. *Let* $C_d$ *denote the class of those positive integers* $m \leq n$, *where* $(m, n) = d$. *Since* 28 *has six positive factors* $1, 2, 4, 7, 14$, *and* 28, *there are six such classes:*

- $C_1 = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$,
- $C_2 = \{2, 6, 10, 18, 22, 26\}$,
- $C_4 = \{4, 8, 12, 16, 20, 24\}$,
- $C_7 = \{7, 21\}$,
- $C_{14} = \{14\}$,
- $C_{28} = \{28\}$.

*In fact, these classes contain* $12 = \varphi(28) = \varphi(28/1)$, $6 = \varphi(14) = \varphi(28/2)$, $6 = \varphi(7) = \varphi(28/4)$, $2 = \varphi(4) = \varphi(28/7)$, $1 = \varphi(2) = \varphi(28/14)$, *and* $1 = \varphi(1) = \varphi(28/28)$ *elements, respectively. Also, they form a partitioning of the set of positive integers* $\leq 28$. *Therefore, the sum of the numbers of elements in the various classes must equal* 28*; that is,* $12+6+6+2+1+1 = 28$. *In other words,*

$$\varphi(28) + \varphi(14) + +\varphi(7) + \varphi(4) + \varphi(2) + \varphi(1) = 28,$$

*that is* $\sum_{d|28} \varphi(d) = 28$.

More generally, we have the following result.

**Theorem 2.9** *Let* $n$ *be a positive integer. Then*

$$\sum_{d|n} \varphi(d) = n. \tag{2.6}$$

**Proof.** We partition the set of positive integers 1 through $n$ into various classes $C_d$ as follows, where $d|n$. Let $m$ be a positive integer $\leq n$. Then $m$ belongs to class $C_d$ if and only if $(m,n) = d$; that is, if and only if $(m/d, n/d) = 1$. The number of elements in $C_d$ equals the number of positive integers $\leq n/d$ and relatively prime to it, namely, $\varphi(n/d)$, thus, each class $C_d$ contains $\varphi(n/d)$ elements.

Since there is a class corresponding to every factor $d$ of $n$ and every integer $m$ belongs to exactly one class, the sum of the elements in the various classes must yield the total number of elements. That is,

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) = n.$$

But as $d$ runs over the divisors of $n$, so does $n/d$. Consequently,

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d) = n.$$

The proof is finished. ■

The following example illustrates this theorem. Let $n = 12$. we compute $\varphi(d)$ for every divisor $d$ of $n$, and check that $\sum_{d|12} \varphi(d) = 12$. In fact, we have

$$\begin{aligned} \sum_{d|12} \varphi(d) &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) \\ &= 1 + 1 + 2 + 2 + 2 + 4 = 12. \end{aligned}$$

Also, we use the proof by induction to show that $\sum_{d|n} \varphi(d) = n$. Let $n$ have only one distinct prime factor with some positive power i.e., suppose, $n = p^a$

with $a \geq 1$. We have

$$\begin{aligned}\sum_{d|p^a} \varphi(d) &= \varphi(1) + \varphi(p) + \varphi\left(p^2\right) + ... + \varphi\left(p^a\right) \\ &= 1 + (p-1) + p(p-1) + ... + p^{a-1}(p-1) \\ &= 1 + (p-1)\left[1 + p + ... + p^{a-1}\right] = p^a = n.\end{aligned}$$

i.e., the result is true when $n$ is a power of a prime.

Let us assume that the theorem is true when $n$ has $k$ distinct prime factors. Then consider an integer $N$, which has $(k+1)$ distinct prime factors. Let $p^a \mid\mid N$, that is, $p^a \mid N$ and $p^{a+1} \nmid N$. We put $N = p^a \cdot n$, where $n$ has $k$ distinct prime factors. Now if $d$ runs through the divisor of $n$, then $p^i d$ $(0 \leq i \leq a)$ runs through the divisors of $N$. Hence

$$\begin{aligned}\sum_{d|N} \varphi(d) &= \varphi(d_1) + \varphi(pd_1) + \varphi\left(p^2 d_1\right) + ... + \varphi\left(p^a d_1\right) + \\ &\quad \varphi(d_2) + \varphi(pd_2) + \varphi\left(p^2 d_2\right) + ... + \varphi\left(p^a d_2\right) + \\ &\quad ... + \\ &\quad \varphi(d_r) + \varphi(pd_r) + \varphi\left(p^2 d_r\right) + ... + \varphi\left(p^a d_r\right) \\ &= \sum_{d|n} \varphi(d) + \sum_{d|n} \varphi(pd) + \sum_{d|n} \varphi\left(p^2 d\right) + ... + \sum_{d|n} \varphi\left(p^a d\right) \\ &= \sum_{d|n} \varphi(d) + \sum_{d|n} \varphi(p)\varphi(d) + \sum_{d|n} \varphi\left(p^2\right)\varphi(d) + ... + \sum_{d|n} \varphi\left(p^a\right)\varphi(d) \\ &= \sum_{d|n} \varphi(d) + \varphi(p) \sum_{d|n} \varphi(d) + \varphi\left(p^2\right) \sum_{d|n} \varphi(d) + ... + \varphi\left(p^a\right) \sum_{d|n} \varphi(d) \\ &= \sum_{d|n} \varphi(d)\left(1 + \varphi(p) + \varphi\left(p^2\right) + ... + \varphi\left(p^a\right)\right) \\ &= n \cdot p^a \\ &= N.\end{aligned}$$

Hence by the principle of induction the result follows.

**Example 2.8** *Let $n = 12$. Compute $\sum_{d|12} (-1)^{\frac{12}{d}} \varphi(d)$. In fact, we see that*

$$\begin{aligned}\sum_{d|12} (-1)^{\frac{12}{d}} \varphi(d) &= (-1)^{\frac{12}{1}} \varphi(1) + (-1)^{\frac{12}{2}} \varphi(2) + (-1)^{\frac{12}{3}} \varphi(3) + (-1)^{\frac{12}{4}} \varphi(4) + \\ &\quad (-1)^{\frac{12}{6}} \varphi(6) + (-1)^{\frac{12}{12}} \varphi(12) \\ &= 1 + 1 + 2 - 2 + 2 - 4 \\ &= 0.\end{aligned}$$

**Remark 2.5** *We ask whether*

$$\varphi(\gcd(m,n)) = \gcd(\varphi(m), \varphi(n)),$$

*and*

$$\varphi([m,n]) = [\varphi(m), \varphi(n)].$$

*For example, for $m = 6$ and $n = 4$. Then $\gcd(m,n) = 2$ and $[m,n] = 12$. Thus,*

$$\varphi(\gcd(m,n)) = \varphi(2) = 1 \neq \gcd(\varphi(m), \varphi(n)) = \gcd(2,2) = 2.$$

**Proposition 2.3** *Let $n$ be a positive integer. If $\varphi(n)$ divides $n-1$, then there exists no prime $p$ such that $p^2$ divides $n$.*

**Proof.** Suppose that $n = p^a \cdot m$, where $p$ is prime, $a \geq 2$ and $m \geq 1$. That is $p^2$ divides $n$. We have $\varphi(p^a) = p^a - p^{a-1} = p(p^{a-1} - p^{a-2})$ and so

$$p \mid \varphi(p^a) \mid \varphi(n) \mid n - 1.$$

Thus, $p \mid n - 1 = p^a \cdot m - 1$. This is impossible since $p \nmid 1$. ■

**Remark 2.6** *If $\varphi(n)$ divides $n-1$, then $n$ must be square-free.*

**Theorem 2.10** *Let $n$ be a composite number. If $\varphi(n)$ divides $n-1$, then $n$ has at least three distinct prime factors.*

**Proof.** Suppose $n$ has two distinct prime factors and since $\varphi(n) \mid n-1$, by the preceding proposition $n = pq$, where $p$ and $q$ are primes. Then

$$\begin{aligned}\frac{n-1}{\varphi(n)} &= \frac{pq-1}{(p-1)(q-1)} = \frac{pq-p-q+1+p+q-2}{(p-1)(q-1)} \\ &= \frac{(p-1)(q-1)}{(p-1)(q-1)} + \frac{p-1}{(p-1)(q-1)} + \frac{q-1}{(p-1)(q-1)} \\ &= 1 + \frac{1}{q-1} + \frac{1}{p-1}.\end{aligned}$$

As $\varphi(n) \mid n-1$, then $\frac{n-1}{\varphi(n)}$ is an integer. Moreover, we see that

$$1 < 1 + \frac{1}{q-1} + \frac{1}{p-1} \leq 3,$$

where $p$ and $q$ are primes. Thus, $\frac{1}{q-1} + \frac{1}{p-1} = 1$ or $2$ which is possible only when $p = q = 2$ or $p = q = 3$; but our assumption says that $p$ and $q$ are distinct. Hence $n$ cannot have two distinct primes. So $n$ must have at least three distinct primes. ■

**Example 2.9** *We solve for $x, y, z$ the equation*

$$\varphi(x-5) + \varphi(3y-5) + \varphi(5z-18) = 3, \tag{2.7}$$

*where $\varphi$ is the Euler's function.*

**Solution.** We know that $\varphi(n) =$ number of $a$ $(< n)$ such that $\gcd(a, n) = 1$ where $\varphi(1) = 1$. Since $\varphi(n) \in \mathbb{N}$, therefore (2.7) will be satisfied if and

only if $\varphi(x-5)=1$, $\varphi(3y-5)=1$ and $\varphi(5z-18)=1$. Now, $\varphi(x-5)=1$ implies $x=6$ or 7, $\varphi(3y-5)=1$ implies $y=2$ and $\varphi(5z-18)=1$ implies $z=4$. The solutions are $(x,y,z)=(6,2,4)$ or $(x,y,z)=(7,2,4)$.

**Example 2.10** *We solve the simultaneous equations*

$$\begin{cases} \varphi(x)+\varphi(y)=2, \\ \varphi(2x-1)+\varphi(2y)=3. \end{cases} \tag{2.8}$$

**Solution.** From the first equation of (2.8) we get $\varphi(x)=1$ implies $x=1$ or 2 and $\varphi(y)=1$ implies $y=1$ or 2. Then putting $x=1$, $y=1$ in the second equation of (2.8), $\varphi(11)+\varphi(2)=3$ which is not possible. However, for $x=1$, $y=2$ we have $\varphi(1)+\varphi(4)=3$ is true. Thus $(x,y)=(1,2)$ is a solution. Also $(x,y)=(2,1)$ is a solution since $\varphi(3)+\varphi(2)=3$.

Next, we prove the following result.

**Theorem 2.11** *Let $n\geq 2$. We have*

$$\sum_{\substack{\gcd(a,n)=1\\ 1\leq a<n}}^{n} a=\frac{n\cdot\varphi(n)}{2}. \tag{2.9}$$

**Proof.** We have $\gcd(a,n)=1$ gives $\gcd(n-a,n)=1$. Thus, if $a$ is a set of integers such that $\gcd(a,n)=1$, $1\leq a<n$ then, $n-a$ is also the same set as $a$. That is,

$$\begin{aligned} \sum_{\substack{\gcd(a,n)=1\\ 1\leq a<n}}^{n} a &= a_1+a_2+\ldots+a_{\varphi(n)} \\ &= (n-a_1)+(n-a_2)+\ldots+\left(n-a_{\varphi(n)}\right) \end{aligned}$$

Therefore,

$$2\sum_{\substack{\gcd(a,n)=1\\1\leq a<n}}^{n} a=\underbrace{n+n+...+n}_{\varphi(n)\text{-times}}=n\varphi\left(n\right).$$

This proves (2.9). ■

**Example 2.11** *Let* $n=12=2^2\cdot 3$. *Then*

$$\sum_{\substack{\gcd(a,12)=1\\1\leq a<12}}^{12} a=1+5+7+11=24$$

*and* $n\varphi\left(n\right)/2=12\cdot 4/2=24$.

**Corollary 2.4** *We have the following properties*

1. *Let* $n\geq 1$. *Then* $\varphi\left(n^2\right)=n\varphi\left(n\right)$. *In particular,* $\varphi\left(p^2\right)=p\left(p-1\right)$.
2. *Let* $n\geq 1$. *Then* $\varphi\left(n^3\right)=n^2\varphi\left(n\right)$,
3. *Let* $n\geq 1$. *Then* $\varphi\left(n^a\right)=n^{a-1}\varphi\left(n\right)$.

**Proof.** Indeed, we have

$$\frac{\varphi\left(n^a\right)}{n^{a-1}}=\frac{n^a\prod\limits_{p|n^a}\left(1-\frac{1}{p}\right)}{n^{a-1}}=n\prod_{p|n}\left(1-\frac{1}{p}\right)=\varphi\left(n\right).$$

That is, $\varphi\left(n^a\right)=n^{a-1}\varphi\left(n\right)$. ■

As an example, using the third property of Corollary 2.4, $\varphi\left(16\right)=\varphi\left(2^4\right)=2^3\varphi\left(2\right)=8$, $\varphi\left(2401\right)=\varphi\left(7^4\right)=7^3\varphi\left(7\right)=7^3\cdot 6$ and $\varphi\left(1728\right)=\varphi\left(2^6\cdot 3^3\right)=\varphi\left(\left(2^2\cdot 3\right)^3\right)=\left(2^2\cdot 3\right)^2\varphi\left(2^2\cdot 3\right)=2^4\cdot 3^2\varphi\left(2^2\cdot 3\right)=2^6\cdot 3^2$.

## 2.2 Some other properties and examples

Suppose that $n$ is known to be the product of two distinct primes $p$ and $q$. Then knowledge of $p$ and $q$ is equivalent to knowledge of $\varphi(n)$, since $\varphi(n) = (p-1)(q-1)$. However, there is no known efficient method to compute $\varphi(n)$ if the prime factorization of $n$ is not known.

1. *For every* $n \geq 3$, $\varphi(n)$ *is even.* Let $n \geq 3$. There are two cases:

   Case 1. Assume that $n$ is not divisible by an odd prime, that is, $n = 2^a$ with $a \geq 2$. In this case, $\varphi(n) = 2^{a-1}$ which is even.

   Case 2. Assume that $n$ is divisible by at least one odd prime, namely $p$. By (2.3), $p-1$ divides $\varphi(n)$. This proves the result.

2. Let $n \geq 1$. Then $\varphi(n) \mid n$ if and only if $n = 2^a \cdot 3^b$ with $a \geq 1$ and $b \geq 0$.

3. If $d \mid n$ and $k \geq 0$, then $\varphi\left(n \cdot d^k\right) = d^k \varphi(n)$. Moreover, $\varphi\left(n^k\right) = n^{k-1}\varphi(n)$ for all positive integers $n$ and $k$. The result follows from the prime factorization of $n$ and $d$.

4. Let $p$ and $2p+1$ be two primes. If $n = 4p$, then $\varphi(n+2) = \varphi(n) + 2$. In fact, we have

   $$\varphi(n+2) = \varphi(2(2p+1)) = \varphi(2p+1) = 2(p-1)+2 = 2p = \varphi(n)+2.$$

5. Let $n = 2(2p-1)$, where $p$ and $2p-1$ are prime. Then, $\varphi(n) = \varphi(n+2)$.

6. $\varphi(n)$ is a power of 2 if and only if $n = 2^a F_1 ... F_k$, where $a \geq 0$ and $F_i = 2^{y_i} + 1$, $i = 1, 2, ..., k$ are primes[2]. We see that if $n = p^a$, then by (2.1) $\varphi(n) = p^{a-1}(p-1)$. Thus $\varphi(n) = 2^x$ for some $x \geq 1$ if and only if $p = 2$ or $a = 1$ and $p - 1 = 2^y$ for some $y \geq 1$. Hence, $p = 2^y + 1$. The result follows since $\varphi$ is multiplicative.

7. Let $m, n \geq 1$. Then $\varphi\left(\frac{m}{n}\right) = \frac{\varphi(m)}{\varphi(n)}$ if and only if $m = nk$, where $\gcd(n, k) = 1$. Clearly, if $m = nk$, where $\gcd(n, k) = 1$, then

$$\varphi\left(\frac{m}{n}\right) = \varphi(k) = \frac{\varphi(n)\varphi(k)}{\varphi(n)} = \frac{\varphi(m)}{\varphi(n)}.$$

8. We can easily prove that $\varphi(n) = 14$ has no solutions using the standard factorization of $n$.

**Corollary 2.5** *Let $a \geq 2$. There are no positive integers $n$ such that $2^a \varphi(n) = n$. In particular, there are no positive integers $n$ such that $\varphi(n) = n/4$.*

**Proof.** By (2.3), we have

$$\frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right) = \frac{1}{2^a},$$

where $a \geq 2$. Or equivalently,

$$2^a \prod_{p|n} (p-1) = \prod_{p|n} p. \tag{2.10}$$

Since $4 \nmid \prod_{p|n} p$, we deduce that (2.10) is not valid. ■

[2] A number of the form $2^{2^n} + 1$ is said be Fermat number, denoted by $F_n$. In addition, if $F_n$ is prime, then $F_n$ is said to be Fermat prime. The only known Fermat primes are $F_i$ $(0 \leq i \leq 4)$.

- Let $n$ be an odd integer. Since $(2,n)=1$, we conclude that $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$. Also, $\varphi(4n) = 2\varphi(n)$.

- Let $n$ be an even integer. We put $n = 2^a \cdot m$, where $(2,m)=1$. Then $\varphi(2n) = 2^a\varphi(m) = 2\varphi(n)$. Therefore,

$$\varphi(2n) = \begin{cases} \varphi(n), \text{ if } n \text{ is odd} \\ 2\varphi(n), \text{ if } n \text{ is even} \end{cases}$$

- If $n$ is an even *perfect number, that* $\sigma(n) = 2n$, then $\varphi(n) = 2^{k-1}\left(2^{k-1}-1\right)$ for some positive integer $k$. In fact, there is a result state that $n$ is even perfect number if and only if $n = 2^{p-1}(2^p-1)$, where $p$ and $2^p-1$ are both primes. For example, $n = 6 = 2^{2-1}(2^2-1)$ which is perfect since $\sigma(6) = 2 \cdot 6$.

**Proposition 2.4** *Let $n \geq 1$. Then $\varphi(3n) = 3\varphi(n)$ if and only if $3 \mid n$.*

**Proof.** Assume that $n = 3^a \cdot m$, where $(3,m)=1$. Clearly, $\varphi(3n) = 2 \cdot 3^a\varphi(m) = 3 \cdot 2 \cdot 3^{a-1}\varphi(m) = 3\varphi(n)$. Conversely, assume that $\varphi(3n) = 3\varphi(n)$ and $3 \nmid n$. We put $n = q_1^{a_1}q_2^{a_2}...q_k^{a_k}$, where $q_1, q_2, ..., q_k$ are distinct primes and $a_1, a_2, ..., a_k$ are positive integers. Then

$$\varphi(3n) = 2\varphi(n) \neq 3\varphi(n).$$

A contradiction. ■

**Corollary 2.6** *Let $n \geq 1$. Then $\varphi(3n) = 2\varphi(n)$ if and only if $3 \nmid n$.*

**Proposition 2.5** *Let $n \geq 1$. Then $\varphi(n) = \dfrac{n}{2}$ if and only if $n = 2^k$ for some $k \geq 1$.*

**Proof.** Write $n = 2^k \cdot m$, where $k \geq 1$ and $(2, m) = 1$. We have $\varphi(n) = 2^{k-1}\varphi(m) = 2^{k-1} \cdot m$ if and only if $\varphi(m) = m$ and so $m = 1$. ■

**Proposition 2.6** *There are infinitely many positive integers $n$ such that $\varphi(n) = \frac{n}{3}$.*

**Proof.** Let $n = 3^a \cdot m$, where $(3, m) = 1$. We have $\varphi(n) = 2 \cdot 3^{a-1}\varphi(m)$. If $\varphi(n) = 3^{a-1} \cdot m$, then $\varphi(m) = \frac{m}{2}$. By Proposition , $m = 2^k$ for some $k \geq 1$. Thus, if $n = 2^a \cdot 3^b$ with $a \geq 1$ and $b \geq 0$, then $\varphi(n) = \frac{n}{3}$. ■

We conclude the following result:

**Proposition 2.7** *Let $n \geq 1$. Then $\varphi(n) = \frac{n}{3}$ if and only if $n = 2^a \cdot 3^b$ with $a, b \geq 1$.*

**Proposition 2.8** *The only solution of the equation $\varphi(a \cdot b) = \varphi(a) + \varphi(b)$ are $(a, b) = (2, 2), (3, 4)$ and $(4, 3)$.*

**Proof.** In fact, from the relation $\varphi(ab) = d\varphi(a)\varphi(b)/\varphi(d)$, where $d = \gcd(a, b)$ (see Theorem 2.4). This gives,

$$\frac{\varphi(a) + \varphi(b)}{\varphi(a)\varphi(b)} = \frac{d}{\varphi(d)},$$

or equivalently

$$\frac{1}{\varphi(a)} + \frac{1}{\varphi(b)} = \frac{d}{\varphi(d)} \Rightarrow \frac{\varphi(d)}{\varphi(a)} + \frac{\varphi(d)}{\varphi(b)} = d.$$

or

$$\frac{1}{m} + \frac{1}{n} = d, \text{ where } m = \frac{\varphi(a)}{\varphi(d)} \text{ and } n = \frac{\varphi(b)}{\varphi(d)}.$$

Since $m, n$ and $d$ are positive integers, the only possible values of $m$, $n$ and $d$ are:

$$d = 2, m = n = 1 \tag{2.11}$$

or

$$d = 1, m = n = 2. \tag{2.12}$$

For the case (2.11), $\varphi(a) = \varphi(b) = 2$ and then, $a = b = 2$. For the case (2.12), $\varphi(a) = \varphi(b) = 2$, then one of $a, b$ is 3 and the other is 4. Thus the possible values are $(2, 2)$, $(3, 4)$ and $(4, 3)$. The proof is finished. ■

# Chapter 3

# Relations between $\varphi$ and other multiplicative functions

In this chapter we present some notes involving relations between the Euler's function and the other multiplicative functions as well as the sum of divisors $\sigma$, the number of divisor $d$ and the kernel function $\gamma$.

Clearly, for any prime $p$ we have $\varphi(p)+\sigma(p) = 2p$, and if $\varphi(p^a)+\sigma(p^a) = 2p^a$, then $a = 1$. In fact, if

$$(p-1)\,p^{a-1} + 1 + p + ... + p^{a-1} + p^a = 2p^a,$$

then we must have $1 + p + ... + p^{a-1} = p^{a-1}$ and so $a = 1$.

Simple computation, we can verify the following example:

**Example 3.1** *Let $n = 568 \cdot 3^k$ and $m = 638 \cdot 3^k$, where $k \geq 0$. Then*

$$\varphi(n) = \varphi(m),\ d(n) = d(m),\ \sigma(n) = \sigma(m). \tag{3.1}$$

We can say that (3.1) holds infinitely often.

**Proposition 3.1** *Let $n \geq 1$. Then $\dfrac{\varphi(n)+\sigma(n)}{\gamma(n)^2}$ is an integer for infinitely many positive integers $n$.*

**Proof.** Consider the numbers

$$n = 32 \cdot 3^{2k+1},\ k \geq 1 \tag{3.2}$$

Note that $\gamma(n) = 2 \cdot 3$. Thus, we must prove that $(\gamma(n))^2$ divides $\varphi(n) + \sigma(n)$. In fact, we prove that if $n$ is as in (3.2), then $\varphi(n) + \sigma(n) = 16 \cdot 3^{2r} + 63 \cdot \frac{3^{2r+2}-1}{2}$ is divisible by 36, where $63 = 3^2 \cdot 7$. It remains to prove that $\frac{3^{2r+2}-1}{2}$ is divisible by 4, or equivalently $3^{2r+2} - 1$ is divisible by 8. On the other hand, we see that $9 \equiv 1 \pmod 8$, and so

$$3^{2r+2} = 9^{r+1} \equiv 1 \pmod 8.$$

Thus, $\frac{3^{2r+2}-1}{2}$ is divisible by 4 and hence $\frac{\varphi(n)+\sigma(n)}{\gamma(n)^2}$ is an integer infinitely many times. ■

## 3.1 Diophantine equations and related inequalities involving $\varphi(n)$

Now, recall that a *Diophantine equation* is an equation of the form:

$$f(x_1, x_2, ..., x_k) = b$$

that we want to solve in integers or nonnegative integers. This means that the values of the variables $x_1, x_2, ..., x_k$ will be integers or nonnegative integers. Usually the function $f(x_1, x_2, ..., x_k)$ is a is a polynomial with integer coefficients or a real-valued function whose domain is the set $\mathbb{N}$. Let us start with some simple Diophantine equations involving the divisor function and Euler's function.

**1. The equation** $d(n) = \varphi(n)$, $n \geq 1$. Here, we give a comparison between the value $d(n)$ and Euler's function at the same point $n$. Computing the values of functions $\varphi(n)$ and $d(n)$ for $n \leq 30$ from the well-known formulas for these functions, i.e., if $n = q_1^{a_1} q_2^{a_2} ... q_k^{a_k}$, then

$$\varphi(n) = q_1^{a_1-1}(q_1 - 1) q_2^{a_2-1}(q_2 - 1) ... q_k^{a_k-1}(q_k - 1),$$

and

$$d(n) = (a_1 + 1)(a_2 + 1) ... (a_k + 1).$$

we easily see that the only values $n \leq 30$ for which $\varphi(n) = d(n)$ are $n = 1$, 3, 8, 10, 18, 24 and 30. We have here $\varphi(1) = d(1) = 1$, $\varphi(3) = d(3) = 2$, $\varphi(8) = d(8) = 4$, $\varphi(10) = d(10) = 4$, $\varphi(18) = d(18 = 6$, $\varphi(24) = d(24) = 8$ and $\varphi(30) = d(30) = 8$.

In [5, pages 110-111], it was proved that there are no other solutions of the equation $\varphi(n) = d(n)$ in positive integers $n$. It can be shown that for $n > 30$ we have $\varphi(n) > d(n)$. For example, for $n = 31$ we see that $\varphi(n) = 30$, while $d(n) = 2$.

**Theorem 3.1** *The numbers* $1, 3, 8, 10, 24$ *and* $30$ *are the only solutions of* $d(n) = \varphi(n)$. *Moreover, we have* $\varphi(n) > d(n)$ *for* $n > 30$.

**Proof.** Clearly, $n = 1$ is a solution. Next, let $n > 1$ with $n = \prod p^{\alpha}$ (for simplicity we do not use indices), where $p$ is prime and $\alpha \geq 1$. Then

$$\frac{\varphi(p^{\alpha})}{d(p^{\alpha})} = \frac{p^{\alpha-1}(p-1)}{\alpha+1}.$$

For $p \geq 3$ we see that $p^{\alpha-1} \cdot (p-1) \geq 3^{\alpha-1} \cdot 2 \geq \alpha + 1$ for all $\alpha$ (which can be proved easily by induction on $\alpha$) with equality only for $\alpha = 1$ and $p = 3$.

One gets

$$\varphi(n) \geq d(n) \text{ for all odd,} \tag{3.3}$$

with equality for $n \in \{1, 3\}$.

Let now be $n$ even, i.e, $n = 2^{\alpha} \cdot m$ with $m$ is odd and $\alpha \geq 1$. For $\alpha \geq 3$ one can write

$$\varphi(n) = \varphi(2^{\alpha}) \cdot \varphi(m) \geq 2^{\alpha-1} d(m)$$

on base of (3.3). But $2^{\alpha-1} \geq \alpha + 1$, with equality for $\alpha = 3$, so

$$\varphi(n) \geq d(n) \text{ for } n \text{ is even and } 8 \mid n. \tag{3.4}$$

In the above inequality we must have $m = 1$ or $m = 5$, so in (3.4) we can have equality only for $n = 1 \cdot 8 = 8$, $n = 3 \cdot 8 = 24$. We have to study the remaining cases $\alpha = 1$ and $\alpha = 2$. For $\alpha = 1$ one obtains the equation

$$\varphi(m) = 2d(m), \ m = \text{odd}, \tag{3.5}$$

while for $\alpha = 3$ we have

$$2\varphi(m) = 3d(m), \ m = \text{odd}. \tag{3.6}$$

Let $m = \prod_{p \geq 3} p^{\beta}$. Then (3.5) becomes

$$\prod_{p \geq 3} \frac{p^{\beta-1}(p-1)}{\beta+1} = 2$$

with equality only for $\beta = 1$, thus $m = 5$ or $m = 3 \cdot 5$ are the single possibilities. From here, as solutions we get $n = 2 \cdot 5 = 10$ and $n = 2 \cdot 3 \cdot 5 = 30$. In the same manner, (3.6) becomes

$$\prod_{p \geq 3} \frac{p^{\beta-1}(p-1)}{\beta+1} = \frac{3}{2}.$$

But, $\dfrac{2\cdot 3^{\beta-1}}{\beta+1}\geq 1$ and $\dfrac{4\cdot 5^{\beta-1}}{\beta+1}>\dfrac{3}{2}$. Thus, we cannot have equality. Therefore, this case doe not provide solutions. By summing, all solutions of the initial equations are:

$$n\in\{1,3,8,10,24,30\}.$$

As a consequence, we can write $\varphi(n)>d(n)$ for $n>30$. ■

**2. The equation** $\varphi(d(n))=d(\varphi(n))$.

**Proposition 3.2** *The equation* $\varphi(d(n))=d(\varphi(n))$ *has infinitely many solutions.*

**Proof.** Consider the numbers $n=2^k$, where $k\geq 1$. For such a number to be a solution of $\varphi(d(n))=d(\varphi(n))$, we must have $\varphi(k+1)=d\left(2^{k-1}\right)=k$, which is solvable only when $k+1$ is a prime number. Thus, $k=p-1$, with $p$ is prime. Then for $n=2^{p-1}$ with $p$ is prime, we have $\varphi(d(n))=d(\varphi(n))$.

■

**3. The equation** $d(n)+\varphi(n)=n+1$.

**Proposition 3.3** *The only solutions of* $d(n)+\varphi(n)=n+1$ *are* $1,4$ *and* $p$ *with* $p$ *is prime.*

**Proof.** One can remark that $n=p$ with $p$ is prime and $n=1$ are solutions. Let $n=p^\alpha$ be a prime power such that $d(n)+\varphi(n)=n+1$. Then $\alpha=p^{\alpha-1}$, or equivalently, $\alpha=p$ and $\alpha-1=1$. Hence, $n=4$.

Now, let $n>1$ be composite with $n\neq 4$ and let $d\neq 1$ be a divisor of $n$. Then $\gcd(d,n)\neq 1$. Therefore, clearly $\varphi(n)\leq n-d(n)$ from the definitions of $d$ and $\varphi$ (which is the number of couples $(i,n)$ such that $\gcd(i,n)=1$, $i<n$), and so $d(n)+\varphi(n)<n+1$. Therefore, $n$ cannot be a solution. ■

A *Diophantine inequality* is an inequality whose solutions are required to be integers of natural numbers. Let us consider the following Diophantine inequalities. Also, there are some Diophantine inequalities defined by using the Euler's function and some other arithmetic functions.

**Proposition 3.4** *Let $n \geq 1$. Then $\varphi(n) \geq \dfrac{n}{d(n)}$.*

**Proof.** Let $k$ be the number of distinct prime factors of $n$. Suppose that $n = q_1^{a_1} q_2^{a_2} ... q_k^{a_k}$, where $q_1, q_2, ..., q_k$ are distinct primes and $a_1, a_2, ..., a_k$ are positive integers. Then

$$\begin{aligned} \varphi(n) \cdot d(n) &= n\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)...\left(1-\frac{1}{q_k}\right)\cdot(a_1+1)(a_2+1)...(a_k+1) \\ &\geq n\left(\frac{1}{2}\right)^k \cdot 2^k = n. \end{aligned}$$

This gives the result. ■

**Proposition 3.5** *Let $n \geq 1$. Then*

$$\varphi(n) \leq \frac{n^2}{\sigma(n)}. \tag{3.7}$$

**Proof.** Assume that $n = q_1^{a_1} q_2^{a_2} ... q_k^{a_k}$, where $q_1, q_2, ..., q_k$ are distinct primes

and $a_1, a_2, ..., a_k$ are positive integers. We have

$$\begin{aligned}
\varphi(n)\sigma(n) &= \prod_{i=1}^{k} q_i^{a_i}\left(1-\frac{1}{q_i}\right)\prod_{i=1}^{k}\frac{q_i^{a_i+1}-1}{q_i-1} \\
&= \prod_{i=1}^{k} q_i^{a_i}\left(1-\frac{1}{q_i}\right)\prod_{i=1}^{k}\frac{q_i^{a_i+1}\left(1-\frac{1}{q_i^{a_i+1}}\right)}{q_i-1} \\
&= \prod_{i=1}^{k} q_i^{2a_i}\left(1-\frac{1}{q_i}\right)\prod_{i=1}^{k}\frac{q_i}{q_i-1}\left(1-\frac{1}{q_i^{a_i+1}}\right) \\
&= \prod_{i=1}^{k} q_i^{2a_i}\prod_{i=1}^{k}\left(1-\frac{1}{q_i^{a_i+1}}\right) \leq \prod_{i=1}^{k} q_i^{2a_i} = n^2.
\end{aligned}$$

The proof of (3.7) is finished. ■

## 3.2 Diophantine inequalities involving the generalized Euler's function

The generalized Euler's function is given by a similar argument as in (2.3). In fact, we have:

$$\varphi_k(n) = n^k \prod_{p|n}\left(1-\frac{1}{p^k}\right),\ k \geq 1.$$

The related Dedikind function is defined by

$$\psi_k(n) = n^k \prod_{p|n}\left(1+\frac{1}{p^k}\right),\ k \geq 1$$

In the present section we study several Diophantine inequalities formed by the product and the sum of certain multiplicative arithmetic functions on the left side as well as the generalized Euler's function and its related Dedikind function, and by integer-valued polynomials whose leading coefficients are positive on the right side. Recall that the following result is from the paper [1].

**Theorem 3.2** *Let $s$ and $n$ be positive integers with $n \geq 2$. Then,*

$$\varphi_s(n)^{d(n)} \psi_s(n) \sigma(n) \geq n^{3s+1} + n^{3s} - n^{2s+1} - n^{2s} - n^{s+1} - n^s + n + 1. \quad (3.8)$$

**Proof.** Firstly, for $s = 1$, we note that

$$\varphi(n)^{d(n)} \psi(n) \sigma(n) - \left(n^4 - 2n^2 + 1\right) = \begin{cases} 0, \text{ for } n = p, \\ 111, \text{ for } n = 4. \end{cases}$$

Next, it suffices to show that if $\varphi(n)^{d(n)} \psi(n) \sigma(n) \geq n^4 - 2n^2 + 1$ for some $n \geq 3$, then it is also true for $pn$ with $p \geq 2$ is prime. Indeed, for each such integer $n$ and for any prime $p \geq 2$ we distinguish two cases.

1. When $p$ does not divide $n$. Since $\varphi(n) \geq 2$ and $d(n) \geq 2$, it follows that

$$\begin{aligned} \varphi(pn)^{d(pn)} \psi(pn) \sigma(pn) &= (p-1)^{2d(n)} \varphi(n)^{2d(n)} (1+p)^2 \psi(n) \sigma(n) \\ &= (p-1)^{2d(n)} \varphi(n)^{\tau(n)} (1+p)^2 \left[\varphi(n)^{d(n)} \psi(n) \sigma(n)\right] \\ &\geq (p-1)^{2d(n)} \varphi(n)^{d(n)} (1+p)^2 \left(n^4 - 2n^2 + 1\right) \\ &\geq (p-1)^4 2^2 (1+p)^2 \left(n^4 - 2n^2 + 1\right) \\ &= n^4 \left(4p^6 - 8p^5 - 4p^4 + 16p^3 - 4p^2 - 8p + 4\right) + \\ &\quad n^2 \left(-8p^6 + 16p^5 + 8p^4 - 32p^3 + 8p^2 + 16p - 8\right) + \\ &\quad 4p^6 - 8p^5 - 4p^4 + 16p^3 - 4p^2 - 8p + 4. \end{aligned}$$

   Thus,

$$\begin{aligned} &\varphi(pn)^{\tau(pn)} \psi(pn) \sigma(pn) - \left((pn)^4 - 2(pn)^2 + 1\right) \quad (3.9) \\ \geq\ & n^4 \left(4p^6 - 8p^5 - 5p^4 + 16p^3 - 4p^2 - 8p + 4\right) + \\ & n^2 \left(-8p^6 + 16p^5 + 8p^4 - 32p^3 + 10p^2 + 16p - 8\right) + \\ & 4p^6 - 8p^5 - 4p^4 + 16p^3 - 4p^2 - 8p + 3. \end{aligned}$$

Using the graph of the function $x \mapsto 4x^6-8x^5-4x^4+16x^3-4x^2-8x+3$, we have

$$4p^6 - 8p^5 - 4p^4 + 16p^3 - 4p^2 - 8p + 3 > 0. \tag{3.10}$$

In fact, we see that

$$4p^6-8p^5-4p^4+16p^3-4p^2-8p = 4p^4\left(p^2-2p-1\right)+4p\left(4p^2-p-2\right),$$

where $p^2-2p-1>0$ holds for every $p \geq 3$ and $4p^2-p-2>0$ holds for every $p \geq 2$. This proves (3.10) for every $p \geq 2$, since its value at $p=2$ is 35. Moreover, from the graph of the function:

$$x \mapsto \frac{8x^6-16x^5-8x^4+32x^3-10x^2-16x+8}{4x^6-8x^5-5x^4+16x^3-4x^2-8x+4},$$

by using the same manner as those of the proof of (3.10) we can prove that

$$0 < \frac{8p^6-16p^5-8p^4+32p^3-10p^2-16p+8}{4p^6-8p^5-5p^4+16p^3-4p^2-8p+4} \leq 3.2.$$

Since $n \geq 2$, then

$$n^2 > \frac{-\left(-8p^6+16p^5+8p^4-32p^3+10p^2+16p-8\right)}{4p^6-8p^5-5p^4+16p^3-4p^2-8p+4} > 0. \tag{3.11}$$

Setting

$$\begin{aligned} A &= 4p^6-8p^5-4p^4+16p^3-4p^2-8p+3, \\ B &= -8p^6+16p^5+8p^4-32p^3+10p^2+16p-8, \\ C &= 4p^6-8p^5-5p^4+16p^3-4p^2-8p+4. \end{aligned}$$

Since $A>0$ and $n^2 > \dfrac{-B}{C}$, it follows from the inequality (3.9) that

$$\varphi(pn)^{d(pn)}\,\psi(pn)\,\sigma(pn) - \left((pn)^4 - 2(pn)^2 + 1\right) > n^4C + n^2B + A > 0.$$

2. When $p$ divides $n$. Since $\psi(pn) = p\psi(n)$, $\varphi(pn) = p\varphi(n)$, $\sigma(pn) > p\sigma(n)$ and $d(pn) \geq d(n)+1$, then

$$\begin{aligned}
\varphi(pn)^{d(pn)}\psi(np)\sigma(np) &= (p\varphi(n))^{d(pn)}\psi(pn)\sigma(pn) \\
&> p^{d(pn)+2}\varphi(n)^{d(pn)}\psi(n)\sigma(n) \\
&\geq p^{d(n)+3}\varphi(n)^{d(n)+1}\psi(n)\sigma(n) \\
&= p^{d(n)+3}\varphi(n)\left[\varphi(n)^{d(n)}\psi(n)\sigma(n)\right] \\
&\geq p^{d(n)+3}\varphi(n)\left(n^4-2n^2+1\right) \\
&\geq 2n^4p^5-4n^2p^5+2p^5.
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\varphi(pn)^{d(pn)}\psi(pn)\sigma(pn)-\left((pn)^4-2(pn)^2+1\right) \\
\geq\ & 2n^4p^5-n^4p^4-4n^2p^5+2n^2p^2+2p^5-1 \\
=\ & n^4\left(2p^5-p^4\right)+n^2\left(-4p^5+2p^2\right)+2p^5-1. \qquad (3.12)
\end{aligned}$$

Since $p \geq 2$, then $2p^5-1>0$. Using the graph of the function $x \mapsto \dfrac{4x^5-2x^2}{2x^5-x^4}$ and the proof of (3.10), we can also prove that

$$0 < \frac{4p^5-2p^2}{2p^5-p^4} \leq \frac{5}{2}.$$

Since $n \geq 2$, then

$$n^2 > \frac{-\left(-4p^5+2p^2\right)}{2p^5-p^4} > 0. \qquad (3.13)$$

It follows from (3.12),(3.13) that

$$\varphi(pn)^{d(pn)}\psi(pn)\sigma(pn)-\left((pn)^4-2(pn)^2+1\right)>0.$$

Hence, for $s=1$, we have proved that the inequality $\varphi(n)^{d(n)}\psi(n)\sigma(n) \geq n^4-2n^2+1$ is true for every $n \geq 2$.

Now, assume for some $s \geq 1$ that the desired inequality holds for any composite positive integer $n$. We distinguish two cases:

*Case 1.* Suppose that $n$ is not the square of a prime number. Then

$$\begin{aligned}
& \varphi_{s+1}(n)^{d(n)} \psi_{s+1}(n) \sigma(n) \\
= & \left( n^{s+1} \prod_{p|n} \left(1 - \frac{1}{p^{s+1}}\right) \right)^{d(n)} n^{s+1} \prod_{p|n} \left(1 + \frac{1}{p^{s+1}}\right) \sigma(n) \\
= & \; n^{d(n)} \left( n^{s} \prod_{p|n} \left(1 - \frac{1}{p^{s+1}}\right) \right)^{d(n)} n^{s+1} \prod_{p|n} \left(1 + \frac{1}{p^{s+1}}\right) \sigma(n) \\
\geq & \; n^{d(n)} \left( n^{s} \prod_{p|n} \left(1 - \frac{1}{p^{s}}\right) \right)^{d(n)} n^{s} \prod_{p|n} \left(1 + \frac{1}{p^{s}}\right) \sigma(n) \\
= & \; n^{d(n)} \left[ \varphi_s(n)^{d(n)} \psi_s(n) \sigma(n) \right] \\
\geq & \; n^{d(n)} \left( n^{3s+1} + n^{3s} - n^{2s+1} - n^{2s} - n^{s+1} - n^{s} + n + 1 \right)
\end{aligned}$$

Therefore,

$$\begin{aligned}
\varphi_{s+1}(n)^{d(n)} \psi_{s+1}(n) \sigma(n) & \geq n^4 \left( n^{3s+1} + n^{3s} - n^{2s+1} - n^{2s} - n^{s+1} - n^{s} + n + 1 \right) \quad (3.14) \\
& = n^{3s+5} + n^{3s+4} - n^{2s+5} - n^{2s+4} - n^{s+5} - n^{s+4} + n^5 + n^4,
\end{aligned}$$

where (3.14) holds because $n$ is not of the form $p^2$ with $p$ is prime, and therefore $d(n) \geq 4$. Since $n \geq 6$, it follows that

$$\begin{aligned}
&\varphi_{s+1}(n)^{d(n)} \psi_{s+1}(n) \sigma(n) - \left(n^{3s+4} + n^{3s+3} - n^{2s+3} - n^{2s+2} - n^{s+2} - n^{s+1} + n + 1\right) \\
\geq\ & n^{3s+5} - n^{3s+3} - n^{2s+4} + n^{2s+3} - n^{2s+5} + n^{2s+2} - n^{s+5} - n^{s+4} + n^{s+2} + \\
& n^{s+1} + n^5 + n^4 - n - 1 \\
\geq\ & 6^{3s+5} - 6^{3s+3} - 2^{2s+4} + 6^{2s+3} - 6^{2s+5} + 6^{2s+2} - 6^{s+5} - 6^{s+4} + 6^{s+2} + \\
& 6^{s+1} + 6^5 + 6^4 - 6 - 1 \\
=\ & 7560 \times 6^{3s} - 8820 \times 6^{2s} - 9030 \times 6^s + 9065 \\
\geq\ & 1270\,325.
\end{aligned}$$

Note that when $n$ is prime, the inequality (3.8) becomes

$$\begin{aligned}
\varphi_s(n)^{d(n)} \psi_s(n) \sigma(n) &= (n^s - 1)^2 (n^s + 1)(n + 1) \\
&= n^{3s+1} + n^{3s} - n^{2s+1} - n^{2s} - n^{s+1} - n^s + n + 1.
\end{aligned}$$

*Case 2.* Suppose that $n = p^2$ for some prime number $p \geq 2$. We also have

$$\begin{aligned}
\varphi_s(n)^{d(n)} \psi_s(n) \sigma(n) &= \left(p^{2s} - p^s\right)^3 \left(p^{2s} + p^s\right) \left(1 + p + p^2\right) \\
&= p^{8s+2} + p^{8s+1} + p^{8s} - 2p^{7s+2} - 2p^{7s+1} - 2p^{7s} + \\
&\quad 2p^{5s+2} + 2p^{5s+1} + 2p^{5s} - p^{4s+2} - p^{4s+1} - p^{4s}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\varphi_s(n)^{d(n)} \psi_s(n) \sigma(n) - \left(n^{3s+1} + n^{3s} - n^{2s+1} - n^{2s} - n^{s+1} - n^s + n + 1\right) \\
\geq\ & p^{8s+2} + p^{8s+1} + p^{8s} - 2p^{7s+2} - 2p^{7s+1} - 2p^{7s} - p^{6s+2} - p^{6s} + 2p^{5s+2} + \\
& 2p^{5s+1} + 2p^{5s} + p^{2s+2} - p^{4s+1} + p^{2s} - p^2 - 1 \\
\geq\ & 7 \times 2^{8s} - 14 \times 2^{7s} - 5 \times 2^{6s} + 14 \times 2^{5s} - 2 \times 2^{4s} + 5 \times 2^{2s} - 5 \\
\geq\ & 111,
\end{aligned}$$

since $p \geq 2$. Hence, (3.8) is true for $n = p^2$ with $p$ is prime.

Thus, our assertion is proved by induction on $s$. This completes the proof of Theorem 3.2. ■

**Remark 3.1** *In the case when $n = p^2$ with $p$ is prime, then (3.14) becomes*

$$\varphi_{s+1}(n)^{d(n)} \psi_{s+1}(n) \sigma(n) \geq n^{3s+4}+n^{3s+3}-n^{2s+3}-n^{2s+4}-n^{s+4}-n^{s+3}+n^4+n^3,$$

*since $\tau(n) = 3$. Hence,*

$$\begin{aligned} & \varphi_{s+1}(n)^{d(n)} \psi_{s+1}(n) \sigma(n) - \left(n^{3s+4} + n^{3s+3} - n^{2s+3} - n^{2s+2} - n^{s+2} - n^{s+1} + n + 1\right) \\ \geq \; & -n^{2s+4} + n^{2s+2} - n^{s+4} - n^{s+3} + n^{s+2} + n^{s+1} + n^4 + n^3 - n - 1, \end{aligned} \tag{3.15}$$

*where the leading coefficient of (3.15) is negative. Therefore, in this case, the inequality (3.8) can not be easily deduced for $s + 1$.*

# Chapter 4

# Conclusion and unsolved problems

Number Theory is a field where the problems to solve are *very easy* to formalize and to understand, but *very hard* to prove. In this chapter, we state some famous open problems involving Euler's function and we give examples to understand them. Some of these problems are found in [3] and [9]. Clearly, if $n$ is prime, then $\varphi(n) = n - 1$; while Lehmer asked whether $\varphi(n)$ divides $n$ implies that $n$ is prime, but this question is still open. Moreover, there are several other questions:

1. Does $\varphi(n) = \varphi(n+1)$ have infinitely many solutions? The first few terms with this property (see [7]) are:

$$1, 3, 14, 104, 164, 194, 255, 495, 584, 975, ...$$

   - For $n = 975$, we have $\varphi(n) = \varphi(3 \cdot 5^2 \cdot 13) = 2^5 \cdot 5 \cdot 3 = 480$ and $\varphi(n+1) = \varphi(976) \quad = \varphi(2^4 \cdot 61) = 2^5 \cdot 3 \cdot 5 = 480$.
   - The number $n = 1405845 = 3^2 \cdot 5 \cdot 7 \cdot 4463$ satisfies $\varphi(n) = \varphi(n+1)$.

2. Erdös asked the question: Does $\varphi(n) = \varphi(n+1) = ... = \varphi(n+k)$ have solutions for every $k$? In particular, for $k = 2$ we have the first solution $n = 5186$. That is, we have:

**Example 4.1** *The equation* $\varphi(n) = \varphi(n+1) = \varphi(n+2)$ *holds when* $n = 5186 = 2 \cdot 2593$.

1. Moser asked the question: Is $\varphi(x) = \varphi(y) = 2n$ solvable for every $n$?

2. Erdös asked the question: Are there infinitely many numbers not of the form $\varphi(n) + n$?

3. Moser asked whether the only solutions of $\varphi(n) = \pi(n)$ are $n = 2, 3, 4, 8, 14, 20, 90$ or not.

4. Note that the equation $14 = \varphi(x)$ has no solutions. Instead of $2^x 7^y$ with $x, y \geq 1$, are there infinitely many such positive integers?

5. Let $a = 665 = 5 \cdot 7 \cdot 19$, $b = 666 = 2 \cdot 3^2 \cdot 37$, $c = 667 = 23 \cdot 29$ and $d = 668 = 2^2 \cdot 167$. We can easily verify the following equations.

   $\cdot\ \varphi(a) = 2\varphi(b)$,

   $\cdot\ \varphi(\sigma(a)) = 2\varphi(a)$,

   $\cdot\ \sigma(a) = 2\sigma(\varphi(a))$,

   $\cdot\ \sigma(\varphi(a)) = 2\sigma(a)$.

   It remains to give information on each of the above equation and we ask if there are infinitely many solutions.

6. An important general Diophantine equation related to the Euler's function is given by

$$f(\varphi(n)) = \varphi(g(n)),$$

where $f$ and $g$ are two multiplicative functions. Does the above equation has infinitely many solutions?

**Conjecture 4.1 (Carmichael, see [9])** *There is no $n$ for which $\varphi(x) = n$ has a unique solution. In general, for every positive integer $k > 1$, there exist infinitely many $n$ for which $\varphi(x) = n$ has exactly $k$ solutions.*

# Bibliography


[1] S. Boudaoud, D. Bellaouar, A. Boudaoud, *Nonclassical Study on certain Diophantine Inequalities involving Multiplicative Arithmetic Functions*. Malaysian Journal of Mathematical Sciences, 14(1) (2020), 17-39.

[2] J. M. De Koninck and A. Mercier, *1001 problems in classical number theory*. Ellipses Edition Marketing S.A, Paris, 2007.

[3] R. K. GUY, *Unsolved problems in number theory*, Springer-Verlag, New York, 2 edition, 1994.

[4] M. B. Nathanson, *Elementary methods in number theory*, Springer-Verlag, New York, 2000.

[5] J. Sándor, *Geometric theorems, Diophantine equations, and arithmetic functions*. American Research Press. Rehoboth, 2002.

[6] J. Sándor, D. S. Mitrinovic and B. Crstici, *Handbook of number theory I*. Springer Science & Business Media, 2005.

[7] R. Baillie, Table of $\varphi(n) = \varphi(n+1)$, Math. Comput., 30(1976) 189-190

[8] T. Koshy, *Elementary Number Theory with Applications*, Second Edition, Elsevier, 2007.

[9] L. Moser, *An Introduction to the theory of numbers*, The Trillia Lectures on Mathematics, 2007.