

UNIVERSITY OF HELSINKI  
FACULTY OF SCIENCE  
DEPARTMENT OF MATHEMATICS AND STATISTICS

---

Bachelor's thesis

# **The Order of Euler's totient function**

Elli Kiiski

---

Bachelor's Programme in Mathematical Sciences

Supervisor: Eero Saksman

June 24, 2021

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Euler's totient function and its properties</b>	<b>2</b>
<b>3</b>	<b>Helpful functions and results</b>	<b>5</b>
3.1	Mertens' theorems . . . . .	5
3.2	Functions $\sigma$ and $\zeta$ . . . . .	11
<b>4</b>	<b>The growth rate of Euler's totient function</b>	<b>13</b>
4.1	Upper bound of Euler's totient function . . . . .	14
4.2	Lower growth rate of Euler's totient function . . . . .	14

## Summary in Finnish

Lukuteoriassa Eulerin  $\phi$ -funktio on merkittävä kuvaus, joka kertoo eräällä tavalla kokonaislukujen jaollisuudesta. Lukuteoreettisena funktiona se kuvaa luonnollisia lukuja toisiksi luonnollisiksi luvuiksi siten, että sen arvo luvulla  $n$  on sellaisten positiivisten kokonaislukujen määrä, jotka ovat sitä pienempiä ja joilla ei ole ykköstä suurempia yhteisiä tekijöitä sen kanssa.

Tässä kandidaatintutkielmassa keskitytään tarkastelemaan, millaisia arvoja Eulerin  $\phi$ -funktio voi saada hyvin suurilla luvuilla. Eritysen kiinnostavaa on, kuinka pieniä nämä arvot voivat olla suhteessa mielivaltaiseen lukuun  $n$ . Aloitamme teeman käsittelyn lukuteorian peruskäsitteistä ja jatkamme usean määritelmän ja aputuloksen kautta kohti  $\phi$ -funktion kasvuvauhdin alarajan todistusta, johon kaikki kulminoituu. Kyseinen todistus osoittautui kirjoitusvaiheessa yllättävän monikerroksiseksi ja vaati täten kokonaisen osan pelkälle avustavien funktioiden ja lemموjen esittelylle.

Eulerin  $\phi$ -funktio saa suurimmat arvonsa alkuluvuilla. Tämä on paitsi intuitiivista, on myös varsin triviaalia todistaa, että jokaisella alkuluvulla  $p$  funktio saa arvon  $\phi(p) = p - 1$ . Pienimpien arvojen löytäminen ja niiden suuruuden määrittäminen sen sijaan ei ole lainkaan yhtä suoraviivaista. Joistakin selvästi monilla luvuilla jaollisista luvuista, kuten 24 on toki helppo huomata, että  $\phi$ -funktion arvo kyseisessä kohdassa lienee verrattain pieni. Arvon suhteellisen suuruuden määrittäminen kuitenkin vaikeutuu, kun siirrytään tarkastelemaan yhä suurempia lukuja.

Tämän tutkielman rakenne on seuraavanlainen. Johdannossa kerrataan tärkeimpiä lukuteorian käsitteitä ja seuraavassa luvussa esitellään itse  $\phi$ -funktio muutamane ominaisuuksineen. Tämän jälkeen jatketaan tarvittavien aputulosten parissa. Oikeastaan vasta viimeisessä luvussa päästään otsikon aiheeseen, kun käsittelyyn otetaan  $\phi$ -funktion kasvuvauhti. Lukijan on siis kärsivällisesti maltettava pysyä mukana aivan loppuun saakka.

# 1 Introduction

Euler's totient function, also known as Euler's  $\phi$ -function, is one of the most fundamental functions in number theory. It is used broadly within the field and unlike most concepts in number theory, the totient function even has a significant practical application, namely the RSA encryption system [4].

The totient function is also interesting as such, since its values differ quite unpredictable as it grows. This becomes apparent, when taking a look at figures 1 and 2 presented later on. That is why the growth rate (i.e. the order) of the Euler's totient function is the question, on which will be concentrating in this thesis.

To talk about the notation, the variables ( $a, b, k, m, n, p$  etc.) denote integers if not stated otherwise. Particularly  $p$  is always a prime number. Also, we define the set of natural numbers  $\mathbb{N}$  to consist of positive integers, meaning  $0 \notin \mathbb{N}$ . In chapter 3 the notation  $\lfloor x \rfloor$  is used to denote the integer part and  $\{x\}$  the decimal part of a real number  $x$ . In other words,  $x = \lfloor x \rfloor + \{x\}$ .

It is beneficial to go through the basic definitions concerning the essential areas before getting to the totient function. So, let us start with that.

**Definition 1.1.** *Divisibility*

If  $b = ka$  for some integer  $k$ ,  $b$  is divisible by  $a$ . This is denoted by  $a \mid b$ .

**Theorem 1.2.** *Greatest common divisor*

Let  $a \in \mathbb{N}$  and  $b \in \mathbb{N}$ . There is a unique  $d \in \mathbb{N}$  with following properties:

1.  $d \mid a$  and  $d \mid b$
2. if  $c \mid a$  and  $c \mid b$ , then  $c \mid d$

The number  $d$  is called the greatest common divisor of  $a$  and  $b$ , denoted by  $\gcd(a, b) = d$ .

*Proof.* The existence of such number is proved in *Fundamentals of Number theory* [3] as Theorem 2.1 (ch. 2.1, p. 31).  $\square$

**Definition 1.3.** *Congruence*

Let  $m \neq 0$ . If  $m \mid (a - b)$ , we say  $a$  is congruent to  $b$  modulo  $m$ . It is denoted by  $a \equiv b \pmod{m}$ .

**Definition 1.4.** *Complete residue system (mod  $m$ )*

The set  $a_0, a_1, \dots, a_{m-1}$  forms a complete residue system if

$$a_i \equiv i \pmod{m}$$

for all  $i \in \{0, 1, \dots, m-1\}$ .

**Definition 1.5.** *Prime number*

Integer  $p \in \mathbb{N}$  is a prime, if  $p \geq 2$  and for all  $k \in \mathbb{N}$  it holds that  $k|p$  implies  $k \in \{1, p\}$ . The set of prime numbers is denoted by  $\mathbb{P}$ .

It is a well known result that there are infinitely many primes.

**Definition 1.6.** *Co-prime*

If  $\gcd(a, b) = 1$ ,  $a$  and  $b$  are called co-primes or relative primes.

**Definition 1.7.** *Multiplicative number theoretic function*

Function  $f: \mathbb{N} \rightarrow \mathbb{R}$  is called number theoretic function. It is multiplicative if  $f(ab) = f(a)f(b)$  when  $\gcd(a, b) = 1$ .

## 2 Euler's totient function and its properties

Now that we have revised some of the basic concepts in number theory, let us introduce Euler's totient function itself. It is a number theoretic function that counts the positive co-primes of a given number that are less or equal to it. It is defined formally as follows.

**Definition 2.1.** *Euler's totient function  $\phi: \mathbb{N} \rightarrow \mathbb{N}$*

We set  $\phi(1) = 1$ . For all  $n \geq 2$ ,  $\phi(n)$  is the number of integers  $a \in \{1, 2, \dots, n\}$ , for which  $\gcd(a, n) = 1$ .

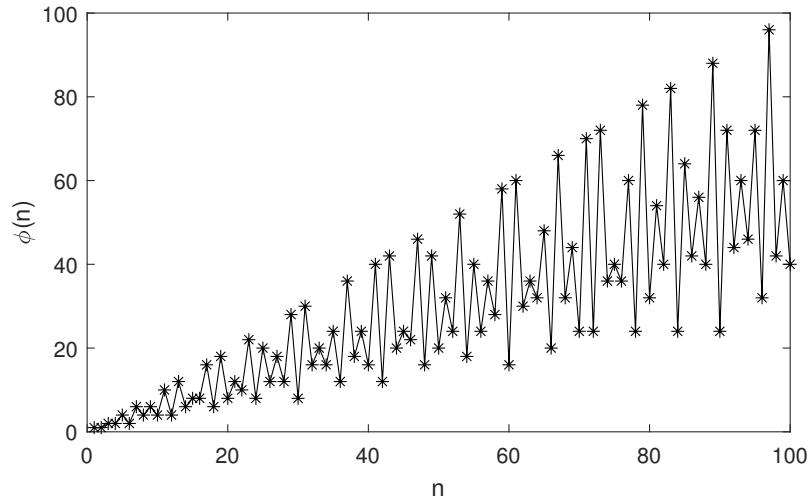


Figure 1: Graph of Euler's totient function when  $n \in \{1, 2, \dots, 100\}$ .

**Theorem 2.2.** *Euler's totient function is multiplicative, i.e.*

$$\gcd(m, n) = 1 \Rightarrow \phi(mn) = \phi(m)\phi(n).$$

*Proof.* Assume  $m > 1$ ,  $n > 1$  and  $\gcd(m, n) = 1$ . Consider the array

$$\begin{array}{ccccc} 0 & 1 & \dots & m-2 & m-1 \\ m & m+1 & \dots & m+(m-2) & m+(m-1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (n-2)m & (n-2)m+1 & \dots & (n-2)m+(m-2) & (n-2)m+(m-1) \\ (n-1)m & (n-1)m+1 & \dots & (n-1)m+(m-2) & (n-1)m+(m-1) \end{array}$$

which consists of integers from 0 to  $mn - 1$  forming a complete residue system  $(\text{mod } mn)$ .

Clearly, each row of the array forms a complete residue system  $(\text{mod } m)$  and all the elements of any column are congruent to each other  $(\text{mod } m)$ . Now there are two types of columns:  $\phi(m)$  columns containing only co-primes to  $m$  and the rest containing none of them.

Next consider the co-prime columns. Every column forms a complete residue system  $(\text{mod } n)$  [3, Thm. 3.5], meaning each includes  $\phi(n)$  elements co-prime to  $n$ . Counting  $\phi(n)$  elements from all the  $\phi(m)$  columns we get in total  $\phi(m)\phi(n)$  numbers that are relatively prime to both  $m$  and  $n$ .

On the other hand, since  $\gcd(m, n) = 1$ , an integer  $k$  is co-prime to  $mn$  if and only if both  $\gcd(m, k) = 1$  and  $\gcd(n, k) = 1$  are true. Hence there are  $\phi(m)\phi(n)$  numbers relatively prime to  $mn$ . Thus, by definition  $\phi(mn) = \phi(m)\phi(n)$ .

The case  $m = 1$  or  $n = 1$  is trivial, since  $\phi(1) = 1$  and hence  $\phi(mn) = \phi(m)\phi(n)$ .

□

As seen above, the definition of Euler's totient function is rather verbal, making it somewhat inconvenient to handle in computation. Fortunately, there is a simple formula to calculate the value as a product involving primes that divide  $n$ .

**Theorem 2.3.** *Euler's product formula*

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where  $\prod_{p|n} \left(1 - \frac{1}{p}\right)$  stands for the product over those distinct primes that divide  $n$ .

*Proof.* Assume first that  $n = p^k$ , where  $p \in \mathbb{P}$ . Integers  $b$  less or equal to  $p^k$ , for which  $\gcd(p^k, b) \neq 1$ , are exactly the numbers  $b = mp$  where  $m \in \{1, 2, \dots, p^{k-1}\}$ .

Hence

$$\phi(n) = \phi(p^k) = p^k - p^{k-1} = p^k - \frac{p^k}{p} = \left(1 - \frac{1}{p}\right) p^k = \left(1 - \frac{1}{p}\right) n.$$

Then, in the general case, assume  $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = \prod_{i=1}^r p_i^{k_i}$ , where  $p_1, p_2, \dots, p_r$  are distinct primes that divide  $n$  and  $k_1, k_2, \dots, k_r$  their powers respectively.

Now, since  $\phi$  is a multiplicative function

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

□

When it comes to primes, the value of the totient function is easy to deduce. By definition, primes are not divisible by any other number than themselves and one, yielding the following lemma.

**Lemma 2.4.** *For every  $p \in \mathbb{P}$  holds  $\phi(p) = p - 1$ .*

*Proof.* Let  $n \in \mathbb{P}$ . There are  $n$  elements in the set  $\{1, 2, \dots, n\}$ , only 1 and  $n$  of which divide  $n$ . Since also  $\gcd(1, n) = 1$ , there is only one number that is not coprime to  $n$ , namely  $n$  itself. Hence,  $\phi(n) = n - 1$ .

We could arrive to the same conclusion with Euler's product formula. That is, by making the same observation that the only prime dividing  $n$  is  $n$  itself. We get

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right) = n \left(1 - \frac{1}{n}\right) = n - 1.$$

□

### 3 Helpful functions and results

In order to determine the order of growth of the totient function, we must introduce a few functions and auxiliary results that are used in a proof later on. Since the results of this chapter serve mainly as tools, we do not give details for all of them.

#### 3.1 Mertens' theorems

The most important of the results is the Mertens' third theorem. Though, we still need some lemmas before the proof of the theorem itself. Let us introduce few functions: first the  $O$ -function, defined formally below, which describes the relative size of two expressions.

**Definition 3.1.**  *$O$ -function*

Let  $x$  be a real variable tending to infinity and  $f(x)$  and  $g(x)$  be functions of  $x$ . We say  $f(x) = O(g(x))$ , if  $|f(x)| < A g(x)$  for some constant  $A$ .

For example  $8x = O(x)$  and  $\sin x = O(1)$ . We can also do calculations with the function, for example  $O(x) + O(1) = O(x)$  and  $O(x) \cdot O(x) = O(x^2)$ .

Next up is the  $\Lambda$ -function, the partial sum of which has some useful properties keeping an eye on the Mertens' theorems.

**Definition 3.2.** *Von Mangoldt  $\Lambda$ -function*

Let  $p \in \mathbb{P}$  and  $k \geq 1$ .

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \\ 0 & \text{otherwise.} \end{cases}$$

**Theorem 3.3.**

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

*Proof.* Let us denote  $n = \prod p^k$ . By definition, we have

$$\sum_{d|n} \Lambda(d) = \sum_{p^k | n} \log p.$$

We notice that as the sum runs through all combinations of primes  $p$  and positive integer powers  $k$  such that  $p^k | n$ , each  $\log p$  occurs  $k$  times. Hence

$$\sum_{p^k | n} \log p = \sum k \log p = \sum \log p^k = \log \prod p^k = \log n.$$

□



**Lemma 3.4.**

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1).$$

*Proof.* First, we observe that

$$\begin{aligned} \left| \log n - \int_{n-1}^n \log t \, dt \right| &= \left| \log n - n \log n - \log(n-1) + n \log(n-1) + 1 \right| \\ &= \int_{n-1}^n \log \left( \frac{n}{t} \right) dt = \int_{n-1}^n \log \left( 1 + \frac{n-t}{t} \right) \\ &\leq \int_{n-1}^n \frac{n-t}{t} dt = n \log \left( 1 + \frac{1}{n-1} \right) - 1 \\ &\leq n \left( \frac{1}{n-1} \right) - 1 = \frac{1}{n-1}. \end{aligned}$$

Let  $x \in \mathbb{R}$ . From the inequality above we get

$$\left| \sum_{n \leq x} \log n - \int_1^x \log t \, dt \right| \leq \sum_{2 \leq n \leq x} \frac{1}{n-1} = O(\log x),$$

since the partial sums of harmonic series grow logarithmically.

Hence

$$\sum_{n \leq x} \log n = \int_1^x \log t \, dt + O(\log x) = x \log x - x + O(\log x).$$

On the other hand, by Theorem 3.3 we can deduce

$$\sum_{n \leq x} \log n = \sum_{n \leq x} \sum_{d|n} \Lambda(d) = \sum_{d \leq x} \Lambda(d) \left[ \frac{x}{d} \right] = x \cdot \sum_{d \leq x} \frac{\Lambda(d)}{d} + O(\psi(x)),$$

where  $\psi(x) = \sum_{d \leq x} \Lambda(d)$  as will be defined later on.

Now we have

$$x \log x - x + O(\log x) = x \cdot \sum_{d \leq x} \frac{\Lambda(d)}{d} + O(\psi(x))$$

and when we divide the equation by  $x$ , we get the result

$$\log x + O(1) = \sum_{d \leq x} \frac{\Lambda(d)}{d},$$

since  $\frac{O(\psi(x))}{x} = O(1)$  by Lemma 3.6 below. □

As we did in the previous proof, it is sometimes useful to denote the partial sum of the  $\Lambda$ -function with so called  $\psi$ -function. Along with it, let us introduce another similar function, the  $\vartheta$ -function, as we will need it soon too.

**Definition 3.5.** *Chebyshev functions  $\vartheta$  and  $\psi$*

Let  $x \in \mathbb{R}$ .

$$\begin{aligned}\vartheta(x) &= \sum_{p \leq x} \log p = \log \prod_{p \leq x} p \\ \psi(x) &= \sum_{p^k \leq x} \log p = \sum_{n \leq x} \Lambda(n)\end{aligned}$$

**Lemma 3.6.**

$$\psi(x) = O(x) \quad \text{and} \quad \vartheta(x) = O(x)$$

i.e.

$$\psi(x) < Ax \quad \text{and} \quad \vartheta(x) < Ax$$

for some constant  $A$ .

*Proof.* The proof of Chebyshev's upper bound is nontrivial yet not long. It can be found in *An introduction to the Theory of Numbers* [2] as Theorem 414 (ch. 22.2, p. 453).  $\square$

The following lemma, so called Abel's partial summation formula, presents a convenient way to combine a partial sum of a sequence and a continuous function, which will be useful later.

**Lemma 3.7.** *Abel's partial summation formula*

Let  $c_1, c_2, \dots$  be a sequence of real numbers such that  $c_i = 0$  for  $i < 2$  and

$$C(t) = \sum_{n \leq t} c_n$$

and function  $f(t)$  have continuous derivative for  $t \geq 2 \in \mathbb{R}$ . Then

$$\sum_{n \leq x} c_n f(n) = C(x) f(\lfloor x \rfloor) - \int_2^x C(t) f'(t) dt,$$

where  $x \in \mathbb{R}$ .

*Proof.* First we notice that  $C(n) = C(t)$  and  $f(n) = f(\lfloor t \rfloor)$ , when  $n \leq t < n+1$ .

We have

$$\begin{aligned}
\sum_{n \leq x} c_n f(n) &= c_1 f(1) + c_2 f(2) + \cdots + c_n f(n) \\
&= C(1) f(1) + (C(2) - C(1)) f(2) + \cdots + (C(n) - C(n-1)) f(n) \\
&= C(1) (f(1) - f(2)) + C(2) (f(2) - f(3)) + \cdots \\
&\quad + C(n-1) (f(n-1) - f(n)) + C(n) f(n) \\
&= \sum_{n \leq x-1} C(n) (f(n) - f(n+1)) + \underbrace{C(n) f(n)}_{C(x) f(\lfloor x \rfloor)}.
\end{aligned}$$

On the other hand, since  $f(t)$  is continuously differentiable when  $t \geq 2$  and  $C(t) = 0$  elsewhere, we have

$$C(n) (f(n) - f(n+1)) = - \int_n^{n+1} C(t) f'(t) dt.$$

Finally, by combining these we get

$$\begin{aligned}
\sum_{n \leq x} c_n f(n) &= C(x) f(\lfloor x \rfloor) + \sum_{n \leq x-1} C(n) (f(n) - f(n+1)) \\
&= C(x) f(\lfloor x \rfloor) - \int_2^x C(t) f'(t) dt.
\end{aligned}$$

□

Next we present two of Mertens' theorems. The third theorem is the one actually used later on, however, we settle for thoroughly proving only the second. That is, the proof of the third (the part where a mysterious constant  $\gamma$  pops up) would unfortunately steal too much space from the actual subject of this thesis.

**Theorem 3.8.** *Mertens' second theorem*

For some constant  $B$ ,

$$\sum_{p \leq n} \frac{1}{p} = \log \log n + B + O\left(\frac{1}{\log n}\right).$$

*Proof.* We observe that

$$\begin{aligned}
\sum_{d \leq n} \frac{\Lambda(d)}{d} &= \sum_k \sum_{p^k \leq n} \frac{\log p}{p^k} \\
&= \sum_{p \leq n} \frac{\log p}{p} + \sum_{p \leq \sqrt{n}} \frac{\log p}{p^2} + \sum_{p \leq \sqrt[3]{n}} \frac{\log p}{p^3} + \dots \\
&= \sum_{p \leq n} \frac{\log p}{p} + O\left(\sum_p \left(\frac{1}{p^2} + \frac{1}{p^3} + \dots\right) \log p\right) \\
&= \sum_{p \leq n} \frac{\log p}{p} + O\left(\sum_p \frac{\log p}{p(p-1)}\right) \\
&= \sum_{p \leq n} \frac{\log p}{p} + O\left(\sum_{m \geq 2}^{\infty} \frac{\log m}{m(m-1)}\right) \\
&= \sum_{p \leq n} \frac{\log p}{p} + O(1).
\end{aligned}$$

We get

$$\sum_{p \leq n} \frac{\log p}{p} = \sum_{d \leq n} \frac{\Lambda(d)}{d} + O(1) = \log n + O(1)$$

by Lemma 3.4.

Let us then apply the Abel's partial summation formula (Lemma 3.7) with the sequence  $(c_k)$  such that  $c_p = \frac{\log p}{p}$  with prime indices and  $c_k = 0$  otherwise. We then have

$$C(n) = \sum_{k \leq n} c_k = \sum_{p \leq n} c_p = \sum_{p \leq n} \frac{\log p}{p}.$$

Let  $f(t) = \frac{1}{\log t}$ . Now by the Abel's partial summation formula we get

$$\begin{aligned}
\sum_{p \leq n} \frac{1}{p} &= \sum_{p \leq n} c_p f(p) = \sum_{k \leq n} c_k f(k) \\
&= \frac{C(n)}{\log n} + \int_2^n \frac{C(t)}{t \log^2 t} dt \\
&= \frac{\log n + O(1)}{\log n} + \int_2^n \frac{\log t + O(1)}{t \log^2 t} dt \\
&= 1 + \frac{O(1)}{\log n} + \int_2^n \frac{dt}{t \log t} + \int_2^n \frac{O(1)}{t \log^2 t} dt \\
&= 1 + O\left(\frac{1}{\log n}\right) + \log \log n - \log \log 2 + \int_2^\infty \frac{O(1)}{t \log^2 t} dt - \int_n^\infty \frac{O(1)}{t \log^2 t} dt \\
&= \log \log n + \underbrace{\left( \int_2^\infty \frac{O(1)}{t \log^2 t} dt + 1 - \log \log 2 \right)}_{=: \text{constant } B} + O\left(\frac{1}{\log n}\right),
\end{aligned}$$

proving the claim. □

**Theorem 3.9.** *Mertens' third theorem*

$$e^{-\gamma} = \log n \prod_{p \leq n} \left(1 - \frac{1}{p}\right) \left(1 + O\left(\frac{1}{\log n}\right)\right)$$

and especially

$$\lim_{n \rightarrow \infty} \log n \prod_{p \leq n} \left(1 - \frac{1}{p}\right) = e^{-\gamma},$$

where  $\gamma$  is the Euler-Mascheroni constant.

*Proof.* To reach the form of Mertens' third theorem, it is shown in *An Introduction to the Theory of Numbers* [2] as Theorem 428 (ch. 22.8, p. 466) that

$$B = \gamma + \sum_{p \leq n} \left( \log \left(1 - \frac{1}{p}\right) + \frac{1}{p} \right).$$

Let us take the value of  $B$  as given and deduce

$$\begin{aligned}
\sum_{p \leq n} \frac{1}{p} &= \log \log n + B + O\left(\frac{1}{\log n}\right) \\
&= \log \log n + \gamma + \sum_{p \leq n} \left( \log \left(1 - \frac{1}{p}\right) + \frac{1}{p} \right) + O\left(\frac{1}{\log n}\right)
\end{aligned}$$

or equivalently

$$\begin{aligned} 0 &= \log \log n + \gamma + \sum_{p \leq n} \log \left(1 - \frac{1}{p}\right) + O\left(\frac{1}{\log n}\right) \\ &= \log \log n + \gamma + \log \prod_{p \leq n} \left(1 - \frac{1}{p}\right) + O\left(\frac{1}{\log n}\right). \end{aligned}$$

Thus, since  $e^{O(\frac{1}{\log n})} = 1 + O\left(\frac{1}{\log n}\right)$  [5, p. 9], we get

$$1 = \log n \cdot e^\gamma \cdot \prod_{p \leq n} \left(1 - \frac{1}{p}\right) \cdot \left(1 + O\left(\frac{1}{\log n}\right)\right)$$

and finally

$$e^{-\gamma} = \log n \prod_{p \leq n} \left(1 - \frac{1}{p}\right) \left(1 + O\left(\frac{1}{\log n}\right)\right).$$

Hence also

$$\lim_{n \rightarrow \infty} \log n \prod_{p \leq n} \left(1 - \frac{1}{p}\right) = e^{-\gamma}.$$

□

**Remark 3.10.** *About the Euler-Mascheroni constant.*

The Euler-Mascheroni constant  $\gamma$  equals the limit of the difference of the harmonic series and natural logarithm [6],

$$\gamma = \lim_{n \rightarrow \infty} \left( \sum_{k=1}^n \frac{1}{k} - \log n \right) \approx 0,57721566.$$

The constant appears in many connections in mathematics, including here in the Mertens' third theorem and later in the lower growth rate of the totient function.

### 3.2 Functions $\sigma$ and $\zeta$

The  $\sigma$ -function is also a number theoretical function and it is quite closely related to the  $\phi$ -function, as we will soon see. The value of  $\sigma(n)$  is the sum of the divisors of  $n$ , or formally defined as:

**Definition 3.11.** *The  $\sigma$ -function*

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

**Lemma 3.12.** Let  $n = p_1^{k_{p1}} p_2^{k_{p2}} \cdots p_r^{k_{pr}}$  be the prime factorization of  $n$ , where  $p_1, p_2, \dots, p_r$  are distinct primes and  $k_{p_i} \geq 0$  is the power of each  $p_i$ . Then

$$\sigma(n) = \prod_{p|n} \frac{p^{k_p+1} - 1}{p - 1}.$$

*Proof.* The proof is fairly easy and it can be found in *An introduction to the Theory of Numbers* [2] as Theorem 275 (ch. 16.7, p. 311).  $\square$

**Lemma 3.13.**

$$\frac{\phi(n) \sigma(n)}{n^2} < 1$$

*Proof.* By the Euler's product formula and Lemma 3.12 we get

$$\begin{aligned} \phi(n) \sigma(n) &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \cdot \prod_{p|n} \frac{p^{k_p+1} - 1}{p - 1} \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \cdot \prod_{p|n} p_p^{k_p} \cdot \prod_{p|n} \frac{p - \frac{1}{p^{k_p}}}{p - 1} \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right) \cdot n \prod_{p|n} \frac{1 - \frac{1}{p^{k_p+1}}}{1 - \frac{1}{p}} \\ &= n^2 \prod_{p|n} \left(1 - \frac{1}{p^{k_p+1}}\right) < n^2. \end{aligned}$$

Equivalently

$$\frac{\phi(n) \sigma(n)}{n^2} < 1.$$

$\square$

Lastly, let us define the  $\zeta$ -function. We will need it briefly later on.

**Definition 3.14.** *Riemann  $\zeta$ -function*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

where  $s > 1 \in \mathbb{R}$ .

**Lemma 3.15.** For all  $s > 1 \in \mathbb{R}$ ,

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}.$$

*Proof.* This is not difficult to prove using unique decomposition of primes. See *Riemann's Zeta Function* [1] (ch. 1.2, p. 6).  $\square$

**Lemma 3.16.**

$$\lim_{s \rightarrow \infty} \zeta(s) = 1$$

*Proof.* By Lemma 3.15, we have

$$\lim_{s \rightarrow \infty} \zeta(s) = \lim_{s \rightarrow \infty} \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

and since  $\lim_{s \rightarrow \infty} \frac{1}{k^s} = 0$  when  $k > 1$ , we get

$$\lim_{s \rightarrow \infty} \prod_p \frac{1}{1 - \frac{1}{p^s}} = \prod_p \lim_{s \rightarrow \infty} \frac{1}{1 - \frac{1}{p^s}} = \prod_p 1 = 1.$$

Altogether,

$$\lim_{s \rightarrow \infty} \zeta(s) = 1.$$

$\square$

## 4 The growth rate of Euler's totient function

Finally reaching the point, in which we are equipped to start dealing with the order of the totient function, let us still consider, why it is interesting at all. As pondered before, the Euler's product formula presents the totient function in a more computable form than the mere definition. However, using it requires factorization of  $n$ , which still makes it difficult to estimate the size of  $\phi(n)$  as  $n$  gets bigger.

Let us amuse ourselves with a quick example.

**Example 4.1.** Let  $n = 2^p - 1 \in \mathbb{P}$  be so called *Mersenne prime*, meaning also  $p \in \mathbb{P}$ . By Theorem 2.4 we know  $\phi(n) = n - 1$ . On the other hand, from Euler's product formula follows that  $\phi(n + 1) = \phi(2^p) = 2^p(1 - \frac{1}{2}) = \frac{2^p}{2} = \frac{n+1}{2}$ .

We see that while  $n$  and  $n+1$  differ from each other only insignificantly,  $\phi(n+1)$  is half the size of  $\phi(n)$ .

Next, all this in our mind, we will prove the exact growth rate of the totient function, starting with the obvious upper bound and then diving into a detailed proof of the lower growth rate.



## 4.1 Upper bound of Euler's totient function

The maximum value of  $\phi(n)$  for given  $n$  is easy to deduce with Theorem 2.4.

**Theorem 4.2.** *For every  $n \geq 2$  holds  $\phi(n) \leq n - 1$  and*

$$\limsup_{n \rightarrow \infty} \frac{\phi(n)}{n} = 1.$$

*Proof.* By definition,  $\phi(n) \leq n$  because there are  $n$  elements in the set  $\{1, 2, \dots, n\}$ . Also, for every  $n \geq 2$  holds  $\gcd(n, n) = n \neq 1$ . Thus,  $\phi(n) \leq n - 1$ .

On the other hand, according to Theorem 2.4,  $\phi(p) = p - 1$  for every  $p \in \mathbb{P}$ . Since there are infinitely many primes,

$$\limsup_{n \rightarrow \infty} \frac{\phi(n)}{n} = \lim_{n \rightarrow \infty} \frac{n - 1}{n} = 1.$$

□

## 4.2 Lower growth rate of Euler's totient function

How small  $\phi(n)$  can be as  $n$  grows, is much less trivial a question to answer. However, it can be shown that there are arbitrary large  $n$  such that the value of  $\phi(n)$  is proportional to  $\frac{n}{\log \log n}$ . The rest of this paper will cover the proof of the exact lower growth rate of the totient function, following the proof of Theorem 328 in *An Introduction to the Theory of Numbers* [2] (ch. 22.9, p. 469).

**Theorem 4.3.**

$$\liminf_{n \rightarrow \infty} \frac{\phi(n) \log \log n}{n} = e^{-\gamma},$$

where  $\gamma$  is the Euler-Mascheroni constant.

*Proof.* It is enough to show that  $\liminf_{n \rightarrow \infty} f(n) = 1$ , when

$$f(n) = \frac{\phi(n) e^{\gamma} \log \log n}{n}.$$

The proof is based on finding auxiliary functions  $F_1$  and  $F_2$ , which are used to estimate  $f$ , and such that  $\lim_{t \rightarrow \infty} F_1(t) = 1$  and  $\lim_{t \rightarrow \infty} F_2(t) = 1$ . First we show that

$$f(n) \geq F_1(\log n) \text{ for all } n \geq 3 \tag{4.4}$$

and in the second part that

$$f(n_j) \leq \frac{1}{F_2(j)} \text{ for some infinite increasing sequence } n_2, n_3, \dots \tag{4.5}$$

Let  $p_1, p_2, \dots, p_{r-\rho} \leq \log n$  and  $p_{r-\rho+1}, \dots, p_r > \log n$  be the prime factors of  $n$ . In other words, the number  $n$  has  $r$  prime factors,  $\rho$  of which are greater than  $\log n$ .

Now

$$(\log n)^\rho < p_{r-\rho+1} \cdot p_{r-\rho+2} \cdots p_r \leq n,$$

which yields

$$\rho < \frac{\log n}{\log \log n}.$$

Thus, there are less than  $\frac{\log n}{\log \log n}$  prime factors greater than  $\log n$ .

By the Euler's product formula (Theorem 2.3)

$$\begin{aligned} \frac{\phi(n)}{n} &= \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \\ &= \prod_{i=1}^{r-\rho} \left(1 - \frac{1}{p_i}\right) \prod_{i=r-\rho+1}^r \left(1 - \frac{1}{p_i}\right) \\ &= \prod_{p \leq \log n} \left(1 - \frac{1}{p}\right) \prod_{p > \log n} \left(1 - \frac{1}{p}\right) \\ &\geq \left(1 - \frac{1}{\log n}\right)^\rho \prod_{p \leq \log n} \left(1 - \frac{1}{p}\right) \\ &> \left(1 - \frac{1}{\log n}\right)^{\frac{\log n}{\log \log n}} \prod_{p \leq \log n} \left(1 - \frac{1}{p}\right). \end{aligned}$$

Hence, we can define

$$F_1(t) = e^\gamma \log t \left(1 - \frac{1}{t}\right)^{\frac{t}{\log t}} \prod_{p \leq t} \left(1 - \frac{1}{p}\right),$$

because by the inequality above

$$\begin{aligned} F_1(\log n) &= e^\gamma \log \log n \left(1 - \frac{1}{\log n}\right)^{\frac{\log n}{\log \log n}} \prod_{p \leq \log n} \left(1 - \frac{1}{p}\right) \\ &\leq \frac{\phi(n)}{n} e^\gamma \log \log n = f(n) \end{aligned}$$

and by the Mertens' third theorem (Theorem 3.9)

$$\begin{aligned}
\lim_{t \rightarrow \infty} F_1(t) &= \lim_{t \rightarrow \infty} e^\gamma \log t \left(1 - \frac{1}{t}\right)^{\frac{t}{\log t}} \prod_{p \leq t} \left(1 - \frac{1}{p}\right) \\
&= \lim_{t \rightarrow \infty} e^\gamma \left(1 - \frac{1}{t}\right)^{\frac{t}{\log t}} \left( \log t \prod_{p \leq t} \left(1 - \frac{1}{p}\right) \right) \\
&= \lim_{t \rightarrow \infty} e^\gamma \left(1 - \frac{1}{t}\right)^{\frac{t}{\log t}} e^{-\gamma} \\
&= \lim_{t \rightarrow \infty} \left(1 - \frac{1}{t}\right)^{\frac{t}{\log t}} \\
&= \lim_{t \rightarrow \infty} \frac{(t-1)^{\frac{t}{\log t}}}{t^{\frac{t}{\log t}}} \\
&= 1.
\end{aligned}$$

The last limit was seen by observing that

$$\begin{aligned}
\lim_{t \rightarrow \infty} \log \left( \frac{(t-1)^{\frac{t}{\log t}}}{t^{\frac{t}{\log t}}} \right) &= \lim_{t \rightarrow \infty} \frac{t}{\log t} \log \left( \frac{t-1}{t} \right) \\
&= \lim_{t \rightarrow \infty} t \log \left( 1 - \frac{1}{t} \right) \cdot \lim_{t \rightarrow \infty} \frac{1}{\log t} \\
&= \lim_{t \rightarrow \infty} -\frac{1}{\log t} = 0
\end{aligned}$$

since

$$\lim_{t \rightarrow \infty} t \log \left( 1 - \frac{1}{t} \right) = \lim_{t \rightarrow \infty} \frac{\log \left( 1 - \frac{1}{t} \right)}{\frac{1}{t}} = \lim_{t \rightarrow \infty} \frac{\frac{1}{t(t-1)}}{-\frac{1}{t^2}} = \lim_{t \rightarrow \infty} -\frac{t}{t-1} = -1$$

by l'Hôpitals rule.

Now we have proved the part (4.4) and shown that  $\liminf_{n \rightarrow \infty} f(n) \geq 1$ .

Next, to prove the part (4.5), let us define

$$g(n) = \frac{\sigma(n)}{n e^\gamma \log \log n}$$

and show that  $g(n_j) \geq F_2(j)$  for an infinite increasing sequence  $n_2, n_3, \dots$ . In the end we will see that the desired result follows from Theorem 3.13.

Let us define

$$n_j = \prod_{p \leq e^j} p^j, \text{ where } j \geq 2.$$

By the Lemma 3.6

$$\log n_j = \log \prod_{p \leq e^j} p^j = j \log \prod_{p \leq e^j} p = j \vartheta(e^j) \leq A j e^j ,$$

where  $A$  is a positive real constant.

Hence

$$\log \log n_j \leq \log(A j e^j) = \log A + \log j + j .$$

Since  $n_j$  is the product of all primes smaller than  $e^j$  to the power of  $j$ , by Lemma 3.12 we have

$$\sigma(n_j) = \prod_{p \leq e^j} \frac{p^{j+1} - 1}{p - 1}$$

and

$$\frac{\sigma(n_j)}{n_j} = \prod_{p \leq e^j} \frac{p^{j+1} - 1}{(p - 1)p^j} = \prod_{p \leq e^j} \frac{p^{j+1} \left(1 - \frac{1}{p^{j+1}}\right)}{p^{j+1} \left(1 - \frac{1}{p}\right)} = \prod_{p \leq e^j} \frac{1 - \frac{1}{p^{j+1}}}{1 - \frac{1}{p}} .$$

Also, by the Lemma 3.15

$$\prod_{p \leq e^j} \left(1 - \frac{1}{p^{j+1}}\right) > \prod \left(1 - \frac{1}{p^{j+1}}\right) = \frac{1}{\zeta(j+1)} .$$

Now we can define

$$F_2(t) = \frac{1}{e^\gamma \zeta(t+1)(B + t + \log t)} \prod_{p \leq e^t} \left(\frac{1}{1 - \frac{1}{p}}\right) ,$$

where  $B = \log A$  is again a real constant.

This is, by combining the results above

$$\begin{aligned} F_2(j) &= \frac{1}{e^\gamma \zeta(j+1)(B + j + \log j)} \prod_{p \leq e^j} \left(\frac{1}{1 - \frac{1}{p}}\right) \\ &\leq \frac{1}{e^\gamma \log \log n_j} \prod_{p \leq e^j} \frac{1 - \frac{1}{p^{j+1}}}{1 - \frac{1}{p}} \\ &= \frac{\sigma(n_j)}{n_j e^\gamma \log \log n_j} = g(n_j) . \end{aligned}$$

By the Mertens' third theorem (Theorem 3.9)

$$\lim_{t \rightarrow \infty} \frac{1}{t} \cdot \prod_{p \leq e^t} \left( \frac{1}{1 - \frac{1}{p}} \right) = \lim_{t \rightarrow \infty} \frac{1}{\log e^t \prod_{p \leq e^t} \left( 1 - \frac{1}{p} \right)} = \frac{1}{e^{-\gamma}} = e^{\gamma}$$

and since  $\zeta(t+1) \rightarrow 1$  when  $t \rightarrow \infty$  (Lemma 3.16), we have

$$\begin{aligned} \lim_{t \rightarrow \infty} F_2(t) &= \lim_{t \rightarrow \infty} \frac{1}{e^{\gamma} \zeta(t+1)(B+t+\log t)} \prod_{p \leq e^t} \left( \frac{1}{1 - \frac{1}{p}} \right) \\ &= \lim_{t \rightarrow \infty} \frac{e^{\gamma} t}{e^{\gamma} \zeta(t+1)(B+t+\log t)} \\ &= \lim_{t \rightarrow \infty} \frac{t}{\zeta(t+1)(B+t+\log t)} \\ &= \lim_{t \rightarrow \infty} \frac{t}{B+t+\log t} \\ &= 1. \end{aligned}$$

By Theorem 3.13

$$f(n) g(n) = \frac{\phi(n) e^{\gamma} \log \log n}{n} \cdot \frac{\sigma(n)}{n e^{\gamma} \log \log n} = \frac{\phi(n) \sigma(n)}{n^2} < 1$$

yielding

$$f(n_j) \leq \frac{1}{F_2(j)},$$

since  $g(n_j) \geq F_2(j)$

Thus we have proved part (4.5) and shown that  $\liminf_{n \rightarrow \infty} f(n) \leq 1$ .

Altogether, from the parts (4.4) and (4.5), we get

$$\liminf_{n \rightarrow \infty} \frac{\phi(n) e^{\gamma} \log \log n}{n} = \liminf_{n \rightarrow \infty} f(n) = 1$$

and equivalently

$$\liminf_{n \rightarrow \infty} \frac{\phi(n) \log \log n}{n} = e^{-\gamma}.$$

□

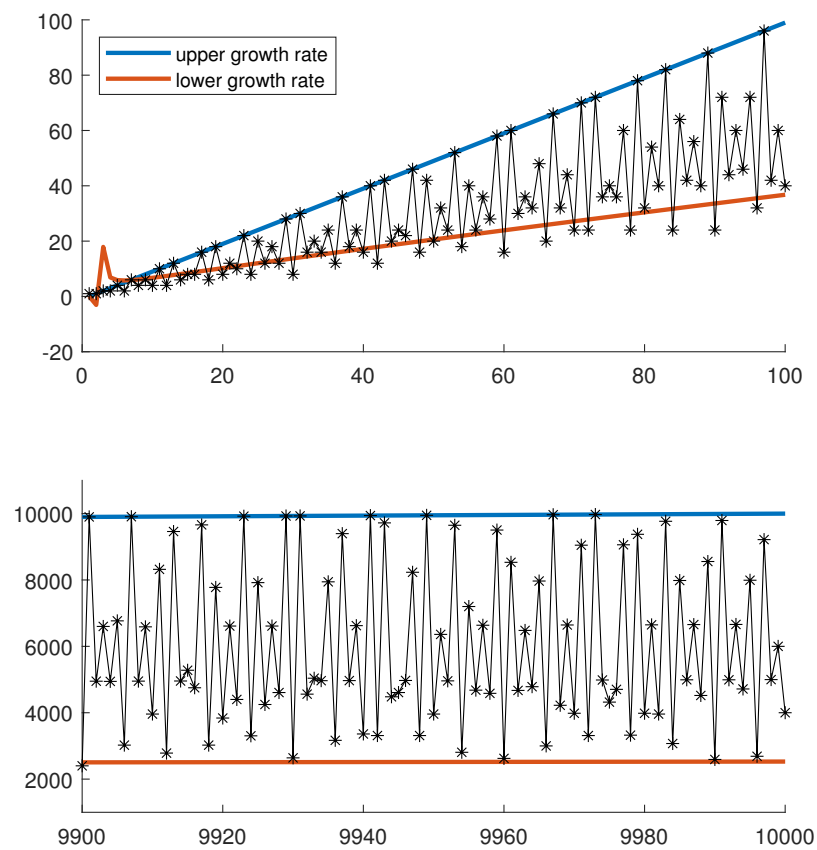


Figure 2: Upper and lower growth rate of Euler's totient function with small and relatively large  $n$ . We see that the lower bound only begins to hold when  $n \rightarrow \infty$ .

## References

- [1] H. M. Edwards. *Riemann's Zeta function*. Academic Press, 1974, pp. 6–7.
- [2] E. M. Wright G. H. Hardy. *An Introduction to the Theory of Numbers*. Oxford University Press, 2008, pp. 310–353, 451–471.
- [3] W. J. LeVeque. *Fundamentals of Number Theory*. Addison-Wesley Publishing Company, 1977, pp. 31–54.
- [4] R. L. Rivest, A. Shamir, and L. Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. In: *Commun. ACM* (1983), p. 7.
- [5] Michael Rosen. “A generalization of Mertens’ theorem”. In: *Journal of the Ramanujan mathematical society* (1999).
- [6] E. W. Weisstein. *Euler-Mascheroni Constant*. URL: <https://mathworld.wolfram.com/Euler-MascheroniConstant.html>.