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 April 27, 2021

Contents

1 Introduction

Tähän pitää keksiä joku alkusepitys todellakin, KEKSI

It is beneficial to go through the basic definitions concerning the essential areas before considering the totient function itself.

Paremmat setit kiitos, MUOTOILE The variables k, m, n and p are usually natural numbers, p denoting particularly a prime number. Here the set of natural numbers $\mathbb{N}$ consists of positive integers, meaning $0 \notin \mathbb{N}$. Also, 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, $x = \lfloor x \rfloor + \{x\}$.

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. This is proved in *Fundamentals of Number theory* [4] as Theorem 2.1 (ch. 2.1, p. 31). □

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

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

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

Definition 1.5. *Prime number*

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

It is well known 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 $f : \mathbb{N} \to \mathbb{R}$ *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 (also known as Euler's ϕ-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. We start by formally defining the function and then showing a few of its properties.

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

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

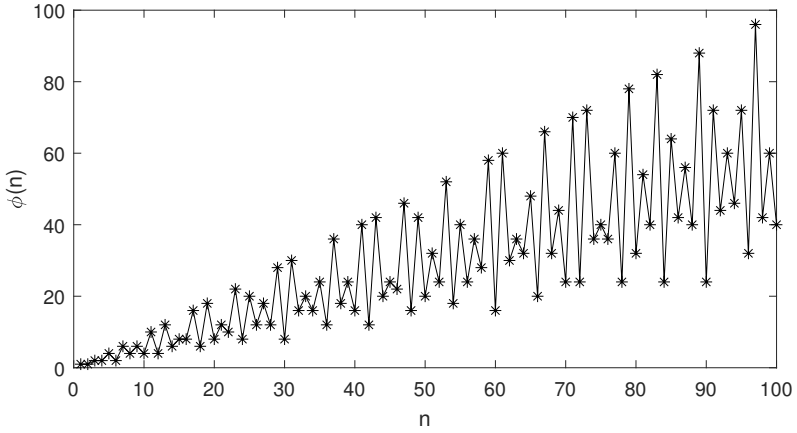

Figure 1: Graph of Euler's totient function when $n \in \{1, 2, \ldots, 100\}$

.

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

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

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 (mod mn).

Clearly, each row of the array forms a complete residue system (mod m) and all the elements of any column are congruent to each other (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. Tarviiks tää nyt jotain lähdettä vai ei, PÄÄTÄ

Next consider the co-prime columns. Every column forms a complete residue system (mod n) [4, 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 $\phi(mn)=\phi(m)\phi(n)$.

□

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 x, for which $gdc(p^k,x)>1$, are exactly the numbers $x=mp$ 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 $p_1, p_2, \ldots, p_r$ are distinct primes that divide n and $k_1, k_2, \ldots, k_r$ their powers respectively.

Now, since ϕ is a multiplicative function

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

□

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 themself and one, yielding the following lemma.

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

Proof. Vois lisää nopee suoranki todistuksen, LISÄÄ

Let $n \in \mathbb{P}$. We observe that the only prime that divides n is n itself. Hence by the Euler's product formula

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

□

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 the proof of the lower limit. Since all of the results of this chapter serve mainly as tools, we do not give details for some of them.

3.1 Mertens' theorems

The most important of the results is the Mertens' third theorem. We still need some lemmas before the proof of the theorem itself. First, we introduce few functions. The O-function, defined formally below, 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 $|f(x)| < Ag(x)$ 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 Λ-function, the partial sum of which has some useful properties keeping an eye on the Mertens' theorems.

Definition 3.2. *Von Mangoldt Λ-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.

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

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

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

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

$$\sum_{p^k \mid n} \log p = \sum a \log p = \sum \log p^a = \log \prod p^a = \log n \,.$$

□

Lemma 3.4.

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

Proof. First, we have a weak form of so called Stirling's formula [3]

Ei tästä ees ymmärrä mitä tässä tapahtuu, TODISTUS UUTEEN USKOON

$$\begin{aligned}\sum_{n\le x}\log n &= \int_1^x \log t\, d\lfloor t\rfloor \\ &= \lfloor x\rfloor \log x - \int_1^x \frac{\lfloor t\rfloor}{t}\, dt \\ &= x\log x - \{x\}\log x - x + 1 + \int_1^x \frac{\{t\}}{t}\, dt \\ &= x\log x - x + O(\log x)\,.\end{aligned}$$

On the other hand, by Theorem 3.3 we can deduce

$$\sum_{n\le x}\log n = \sum_{n\le x}\sum_{d\,|\,n}\Lambda(d) = \sum_{d\le x}\Lambda(d)\,\left\lfloor\frac{x}{d}\right\rfloor = x\cdot\sum_{d\le x}\frac{\Lambda(d)}{d} + O(\psi(x))\,,$$

where $\psi(x) = \sum_{d\le x}\Lambda(d)$ as defined before.

Now we have

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

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

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

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

It is sometimes useful to denote the partial sum of the Λ-function with another function, so called ψ-function. Let us also introduce another similar function, the ϑ-function, as we will need it too.

Definition 3.5. *Chebyshev functions ϑ and ψ*

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

Lemma 3.6.

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

i.e.

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

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). □

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* [2]

If $c_1, c_2, \ldots$ is a sequence of real numbers such that $c_i = 0$ for $i < 2$ and

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

and $f(t)$ has continuous derivative for $t \ge 2 \in \mathbb{R}$, then

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

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

We have

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

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

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

Finally, by combining these we get

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

□

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

Theorem 3.8. *Mertens' second theorem* [3]

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

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

proving the claim.

□

Theorem 3.9. *Mertens' third theorem* [2]

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

and especially

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

where γ 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

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

where γ is the Euler-Masheroni constant.

Let us take the value of B as given and deduce

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

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 $e^{O\left(\frac{1}{\log n}\right)} = 1 + O\left(\frac{1}{\log n}\right)$ [6, p. 9]

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

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

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

□

Remark 3.10. *About the Euler-Mascheroni constant.* [8]

The Euler-Mascheroni constant γ equals the limit of the difference of the harmonic series and natural logarithm,

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

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

3.2 Functions σ and ζ

The σ-function is also a number theoretical and it is quite closely related to the ϕ-function itself, 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 $n = p_1^{k(p_1)} p_2^{k(p_2)} \cdots p_r^{k(p_r)}$ be the prime factorization of n, where $p_1, p_2, \ldots, p_r$ 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. Ei ois varmaan vaikea todistaa, KOITAS 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). □

Lemma 3.13.

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

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

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

Equivalently

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

□

We also need the ζ-function briefly later on.

Definition 3.14. *Riemann ζ-function* [2]

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

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). □

Lemma 3.16.

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

Proof. By Lemma 3.15, we have

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

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

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

Altogether,

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

□

4 The limits 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 prsents the totient function in a more computable form. 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. [5] *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 $\phi(n+1) = \phi(2^p) = 2^p(1-\frac{1}{2}) = \frac{2^p}{2} = \frac{n+1}{2}$.*

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

All this in our mind, next we will prove the exact growth rate of the totient function, starting with the fairly 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 $\phi(n)$ 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*

$$\limsup \frac{\phi(n)}{n} = 1\,.$$

Proof. By definition, $\phi(n) \leq n$ because there are n elements in the set $\{1, 2, \ldots, n\}$. 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 $p \in \mathbb{P}$. Hence, because there are infinitely many primes

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

□

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.

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

where γ is the Euler-Mascheroni constant.

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

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

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

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

Let $p_1, p_2, \ldots, p_{r-\rho} \leq \log n$ and $p_{r-\rho+1}, \ldots, p_r > \log n$ be the prime factors of n. In other words, the number n has r prime factors, ρ 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)

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

The last limit was seen by observing that... LISÄÄ

Now we have proved the part (4.4) and showed that $\liminf f(n) \ge 1$.

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

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

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

The desired result will follow from Theorem 3.13.

Let us define

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

By the Lemma 3.6

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

where A is a positive real constant.

Hence

$$\log\log n_j = \log(Aje^j) = \log A + \log j + j\,.$$

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

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

and

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

Also, by the Lemma 3.15

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

Now we can define

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

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

This is, by combining the results above

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

By the Mertens' third theorem (Theorem 3.9)

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

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

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

By Theorem 3.13

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

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

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

Thus we have proved part (4.5) and shown that $\liminf f(n) \leq 1$.

Altogether, from the parts (4.4) and (4.5), we get that the limit inferior of $f(n)$ must be

$$\liminf \frac{\phi(n)\,e^{\gamma}\log\log n}{n} = \liminf f(n) = 1$$

and equivalently

$$\liminf \frac{\phi(n)\,\log\log n}{n} = e^{-\gamma}\,.$$

□

- Kuvia voisi kommentoida jotenkin väliselityksissä
- Lähteet ja viittaukset kuntoon
- Väliselitykset minttiin: limit-check, now-check, marian oikoluku
- Johdonmukaisuus ja eheys: muuttuja-check
- Kypsyysnäyte

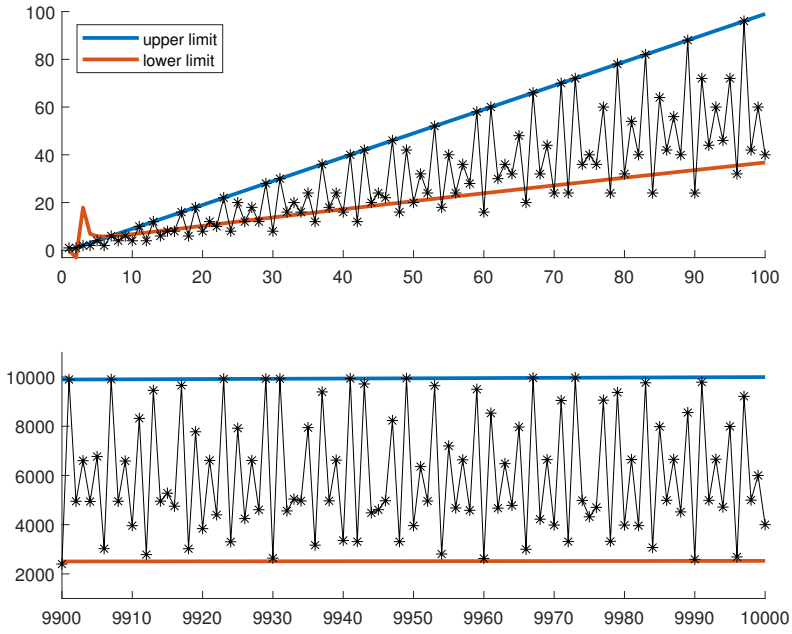

Figure 2: KORJAA KUVAN SELITTEET "growth rate" Upper and lower growth rate of Euler's totient function with small and relatively large n. We see that the lower bound only holds when $n \to \infty$.

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] Leo Goldmakher. "A Quick Proof of Mertes' Theorem".

[4] W. J. LeVeque. *Fundamentals of Number Theory*. Addison-Wesley Publishing Company, 1977, pp. 31–54.

[5] Carl Pomerance. "Arithmetical Functions III: Orders of Magnitude".

[6] Michael Rosen. "A generalization of Mertens' theorem". In: (1999).

[7] M. B. Villarino. "Mertens' proof of Mertens' theorem". In: (2005).

[8] E. W. Weisstein. *Euler-Mascheroni Constant*. URL: `https://mathworld.wolfram.com/Euler-MascheroniConstant.html`.