Elli Kiiski

2021 Kandinalku - The order of Euler's totient function

1 Introduction

Placeholder for some introductory explaining about the subject of this thesis.

All introduced variables $a, b, c, ...$ are integers, unless stated otherwise. Here the set of natural numbers $\mathbb{N}$ consists of positive integers, meaning $0 \notin \mathbb{N}$.

LÄHDE näille kaikille määritelmille

Definition 1.1. *Divisibility*

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

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. $d|a$ and $d|b$
2. if $c|a$ and $c|b$, then $c|d$

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

Proof. LÄHDE W. J. LeVeque: Fundamentals of Number Theory, chapter 2.1, theorem 2.1 □

Definition 1.3. *Prime number*

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

In other words, all integers greater than 1, only divisible by themself and 1, are primes.

Definition 1.4. *Co-prime*

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

Definition 1.5. *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

Euler's totient function is a multiplicative number theoretic function...

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

Hardy-Wright: chapter 5.5, p.63

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

That is, the value of $\phi(n)$ is the number of positive co-primes of n less or equal to n.

Tuo sanallinen selitys on yhä hyvin onneton.

Theorem 2.2. Hardy-Wright: chapter 5.5, theorem 60, p. 64

Euler's totient function is multiplicative:

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

Proof. Placeholder for proof. □

Theorem 2.3. *Euler's product formula*

Hardy-Wright: chapter 5.5, theorem 62, p. 64
Oisko jossain parempi lähde

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

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

Proof. Assume first that $n = p^k$, where $p \in \mathbb{P}$. Now for every x, for which $gdc(p^k, x) > 1$, holds $x = mp^{k-1}$ for some $m \in \{1, 2, ..., p^{k-1}\}$.

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 $p_1, p_2, ..., p_r$ are distinct primes that divide n and $k_1, k_2, ..., k_r$ their powers respectively.

Now, since ϕ is a multiplicative function

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

□

Lemma 2.4. *Totient function and primes*

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

Proof. Let $n \in \mathbb{P}$. Now 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 Merten's theorem and other lemmas

Building up to the order of the totient function, we must introduce few functions and theorems that are used in the proof of the lower limit. Since all of the results of this chapter serve mostly as tools, proof for may of the is left untouched.

Theorem 3.1. *Merten's (third) theorem*

Hardy-Wright: chapter 22.8, theorem 429, p. 466 Oisko parempi lähde, jossa simppelimpi todistus

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

where γ is the Euler's constant.

Proof. Placeholder for a sketch of the proof or maybe even the whole proof.

□

Definition 3.2. *Euler-Mascheroni constant*

Wolfram MathWorld: Euler-Mascheroni constant Onkohan tarpeeks legit lähde

The Euler-Mascheroni constant γ equals the limit of the difference of the harmonic series and natural logarithm. It equals approximately $\gamma \approx 0.57722$. More detailed consideration is outside of the scope of this thesis.

Definition 3.3. *The sigma-function*

Hardy-Wright: chapter 16.7, p. 310

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

meaning the value of $\sigma(n)$ is the sum of the divisors of n.

Lemma 3.4. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime factorization of n, where $p_1, p_2, ..., p_r$ are distinct primes. Then

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{k_i+1} - 1}{p_i - 1} \,.$$

Proof. LÄHDE Theorem 275 in *Hardy & Wright: Introduction to the Theory of Numbers.* □

Theorem 3.5.

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

Proof. LÄHDE Theorem 329 in *Hardy & Wright: Introduction to the Theory of Numbers.* □

Definition 3.6. *Chebyshev function*

Hardy-Wright: chapter 22.1, p. 451

$$\vartheta(x) = \sum_{p \le x} \log p = \log \prod_{p \le x} p \,,$$

where $x \in \mathbb{R}$ and $p \in \mathbb{P}$.

Lemma 3.7. For the function $\vartheta(x)$ holds

$$\vartheta(x) < Ax \,,$$

where $x \ge 2 \in \mathbb{R}$, A is a real constant.

Proof. LÄHDE Theorem 414 in *Hardy & Wright: Introduction to the Theory of Numbers.* □

Definition 3.8. *Riemann zeta-function*

Hardy-Wright: chapter 17.2, p. 320

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

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

Lemma 3.9. For all $s > 1 \in \mathbb{R}$,

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

Proof. LÄHDE Theorem 280 in *Hardy & Wright: Introduction to the Theory of Numbers.* □

4 The limits of Euler's totient function

As shown in previous chapter, there is an exact formula for the rather verbally defined totient function $\phi(n)$. Though, using it requires factorization of n, which seems to cause the difficulty to estimate its size as n gets bigger.

For example, 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 $\phi(n)$.

4.1 Upper limit of Euler's totient function

The maximum value of $\phi(n)$ given n is easy to define by the theorem 2.4.

Theorem 4.2. *Upper limit of the totient function*

Hardy-Wright: chapter 18.4, theorem 326, p. 352

For every $n \geq 2$ holds $\phi(n) \leq n - 1$ and

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

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

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

Onkohan yllä oleva ensimmäinen yhtäsuuruusmerkki ihan legit? Myös: pitääkö infinitely many primes perustella?

□

4.3 Lower limit 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 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 limit inferior of the totient function.

Theorem 4.4. *Lower limit of the totient function*

Hardy-Wright: chapter 18.4, theorem 328, p. 352

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

where γ is the Euler's constant.

Proof. Hardy-Wright: chapter 22.9, p. 467

Let's prove the claim by showing $\liminf f(n) = 1$, when

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

and γ is the Euler's constant.

The proof is based on finding two functions $F_1(t)$ and $F_2(t)$, the limits of which are both $\lim_{t\to\infty} F_1(t) = 1$ and $\lim_{t\to\infty} F_2(t) = 1$. First we show that

$$f(n) \geq F_1(\log n) \text{ for all } n \geq 3 \tag{1}$$

and in the second part that

$$f(n_j) \leq \frac{1}{F_2(j)} \text{ for some infinite increasing sequence } n_2, n_3, \ldots \tag{2}$$

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)

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

Hence, we can define

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

because by the inequality above

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

and by the Merten's third theorem (theorem 3.1)

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

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

Next, to prove the part (2), let's 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 $n_2, n_3 \dots$. The desired result will follow from theorem 3.5.

Let

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

By the lemma 3.7

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

where A is a real constant.

Hence

$$\log\log n_j = \log A j e^j = \log A + \log j + \log e^j = \log A + \log j + j\,.$$

Since n_j is the product of all primes smaller than e^j to the power of j, by the lemma 3.4 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 3.9

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

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 a suitable 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 Merten's third theorem (theorem 3.1)

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

and hence

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

Zeta-funktion raja-arvo pitää käsitellä!

By the theorem 3.5

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

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

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

Thus we have proved the part (2) and showed that $\liminf f(n) \le 1$.

Altogether, from the parts (1) and (2), 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

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

$\square$