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 $0 \notin \mathbb{N}$.

Notation 1.0.1. *Divisibility*

Let a and b be such that b is divisible by a. This is denoted by $a|b$.

Definition 1.0.2. *Greatest common divisor*

Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$. It can be shown that 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 $gcd(a, b) = d$.

However, the existence of the greatest common divisor is non-trivial. Proof can be found in *LeVeque: Fundamentals of Number Theory, chapter 2.1.*

Definition 1.0.3. *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, which are only divisible by themself and 1, are primes.

Definition 1.0.4. *Co-prime*

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

Definition 1.0.5. *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 2.0.1. *Euler's totient function* $\phi : \mathbb{N} \to \mathbb{N}$

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 the totient function at $n \in \mathbb{N}$ is the number of co-primes of n smaller than it.

Theorem 2.0.2. Euler's totient function is multuplicative.

Proof. Placeholder for proof. □

Theorem 2.0.3. *Euler's product formula*

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

where $\prod_{p|n}(1 - \frac{1}{p})$ 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

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

□

Theorem 2.0.4. *Totient function and primes*

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

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

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

□

3 Merten's theorem and other lemmas

Before starting with the order of the totient function, we must introduce few theorems that are used in the proof of the lower limit.

Theorem 3.0.1. *Merten's (third) theorem*

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

where γ is the Euler's constant.

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

□

Definition 3.0.2. *The σ-function*

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

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

Lemma 3.0.3. Placeholder for a lemma that would explain some things in the proof of the lower limit...

Definition 3.0.4. *Chebyshev function*

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

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

Lemma 3.0.5. For the function $\vartheta(x)$ holds

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

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

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

Definition 3.0.6. *Riemann zeta-function*

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

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

Lemma 3.0.7. For all $s > 1 \in \mathbb{R}$,

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

Proof. 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 2.0.4 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 2.0.4.

Theorem 4.1.1. *Upper limit of the totient function*

For every $n \geq 2$

$$\phi(n) \leq n - 1\,.$$

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 2.0.4, $\phi(p) = p - 1$ 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?

$\square$

4.2 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, the following lower limit exists.

Theorem 4.2.1. *Lower limit of the totient function*

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

where γ is the Euler's constant.

Proof. 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

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

Let $p_1, p_2, ..., p_{r-\rho} \leq \log n$ and $p_{r-\rho+1}, ..., p_r > \log n$ 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 2.0.3)

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

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

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

and by the Merten's third theorem (theorem 3.0.1)

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

Now we have proved the part (1) and showed that the limit inferior of the function $f(n)$ is greater or equal to 1.

Next, to prove the part (2), let

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

By the lemma 3.0.5

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

Hence

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

Sit hei väännetään tää todistus loppuun eiksje

$\square$