

Elli Kiiski

2021 Kandikaatopaikka

1 Hardy-Wrightin todistuksen perkaamista

G. H. Hardy ja *E. M. Wrightin* kirjan *An Introduction to the theory of numbers* sivulla 469 olevan ϕ -funktion alarajan todistuksen läpikäyntiä.

1.1 Määrittely: mitä todistetaan

Aloitetaan määrittelemällä kuvaus

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

missä γ on Eulerin vakio.

Halutaan todistaa, että $\liminf f(n) = 1$, mikä on yhtäpitävää sen kanssa, että ϕ -funktion alaraja on $\frac{n}{e^\gamma \log \log n}$.

1.2 Määrittely: miten todistetaan

Pitää kirjoittaa kokonaan uusiksi alkuseitykset nyt kun sigma joudutaankin ottamaan käyttöön

Riittää löytää funktiot $F_1(t)$ ja $F_2(t)$, joille pätee

1. $\lim_{t \rightarrow \infty} F_1(t) = 1$ ja $\lim_{t \rightarrow \infty} F_2(t) = 1$
2. $f(n) \geq F_1(\log n)$ kaikilla $n \geq 3$
3. $f(n_j) \leq \frac{1}{F_2(j)}$ äärettömällä kasvavalla jonolla n_2, n_3, \dots

”Tämä tarkoittaa, että on löydetty funktio $F_1(\log n)$, jonka on sama limes infimum on yksi, mutta funktio on kaikkialla suurempi kuin $f(n)$. Tällöin funktion $f(n)$ limes infimum on enintään yksi. Vastaavasti alapuolen kanssa.”

1.3 Todistus osa 1: $f(n) \geq F_1(\log n)$

Olko $p_1, p_2, \dots, p_{r-\rho} \leq \log n$ ja $p_{r-\rho+1}, \dots, p_r > \log n$ luvun n alkutekijöitä. Siis luvulla n on yhteensä r alkutekijää, joista $\log n$:ää suurempia on ρ kappaletta.

Nyt

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

mistä seuraa

$$\rho < \frac{\log n}{\log \log n}. \quad (2)$$

Eli $\log n$:ää suurempia alkulukutekijöitä on alle $\frac{\log n}{\log \log n}$ kappaletta. Nyt tulokaavaa käyttäen ϕ -funktion suhde n :ään voidaan ilmaista seuraavasti

$$\frac{\phi(n)}{n} = \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \quad (3)$$

$$= \prod_{i=1}^{r-\rho} \left(1 - \frac{1}{p_i}\right) \prod_{i=r-\rho+1}^r \left(1 - \frac{1}{p_i}\right) \quad (4)$$

$$\geq \left(\prod_{i=1}^{r-\rho} \left(1 - \frac{1}{p_i}\right) \right) \left(1 - \frac{1}{\log n}\right)^\rho \quad (5)$$

$$> \left(\prod_{i=1}^{r-\rho} \left(1 - \frac{1}{p_i}\right) \right) \left(1 - \frac{1}{\log n}\right)^{\frac{\log n}{\log \log n}}. \quad (6)$$

Näin ollen voidaan valita

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

jolloin

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

Kuitenkin funktiolle F_1 pätee Mertenin kolmannen lauseen nojalla

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

Täten funktion f limes infimum on korkeintaan 1.

1.4 Todistus osa 2: $f(n_j) \leq \frac{1}{F_2(j)}$

Next, to prove the part (??), 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. By theorem 2.2 the desired result will follow.

Let

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

By the lemma ??

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

Hence

$$\log \log n_j = \log A j e^j = \log A + \log j + \log e^j = \log A + \log j + j. \quad (7)$$

Since n_j is the product of the primes smaller than e^j to the power of j , by the lemma 2.1.1 we have

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

and

$$\frac{\sigma(n_j)}{n_j} = \prod_{p \leq e^j} \frac{p^{j+1} - 1}{(p - 1)p^j} = \prod_{p \leq e^j} \frac{p^{j+1} \left(1 - \frac{1}{p^{j+1}}\right)}{p^{j+1} \left(1 - \frac{1}{p}\right)} = \prod_{p \leq e^j} \frac{1 - \frac{1}{p^{j+1}}}{1 - \frac{1}{p}}. \quad (8)$$

Also, by the lemma 5.2

$$\prod_{p \leq e^j} \left(1 - \frac{1}{p^{j+1}}\right) > \prod_{p \leq e^j} \left(1 - \frac{1}{p^{j+1}}\right) = \frac{1}{\zeta(j+1)}. \quad (9)$$

Now we can define

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

because by combining the results (7), (8) and (9)

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

By the Merten's third theorem (theorem ??)

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

By the theorem 2.2

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

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

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

Viel semmonen johtopäätös

2 Okei, sigma-funktio tarvitaan

Definition 2.1. *The σ -function*

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

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

Lemma 2.1.1. 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, \dots, p_r are distinct primes. Then

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

also denoted by

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

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

Theorem 2.2.

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

Proof. By the Euler's product formula and lemma 2.1.1 we get

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

Equivalently

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

\square

3 Multiplikatiivisuustodistus

Tarttetaan alkuun modulomääritelmät ja muut (jippii lisää määriteltävää ja todistettavaa)

Definition 3.1. *Congruence*

Let $m \neq 0$. We say that a is congruent to b modulo m if $m|(a - b)$. It is denoted by

$$a \equiv b \pmod{m}.$$

Lemma 3.1.1. Joku lemma on varmaan tarpeen

Theorem 3.2. Euler's totient function is multiplicative:

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

Proof. (Theorem 59+60 in *Hardy & Wright: Introduction to the Theory of Numbers*.)

Assume $\gcd(m, n) = 1$ and $a \in \{1, 2, \dots, m\}$ and $b \in \{1, 2, \dots, n\}$.

Let C be a set containing all the numbers of the form $bm + an$. Since m and n are co-prime and a and b run through a complete set of residues $(\text{mod } m)$ and $(\text{mod } n)$ respectively, there is exactly mn numbers in the set C .

Let $b_1m + a_1n \in C$ and $b_2m + a_2n \in C$ be congruent to each other modulo mn . Now

$$b_1m + a_1n \equiv b_2m + a_2n \pmod{mn}$$

then

$$b_1m \equiv b_2m \pmod{m} \quad \text{and} \quad a_1n \equiv a_2n \pmod{n}$$

and furthermore

$$b_1 \equiv b_2 \pmod{m} \quad \text{and} \quad a_1 \equiv a_2 \pmod{n}.$$

This yields $a_1 = a_2$ and $b_1 = b_2$, since a and b **En osaa sanoo tätä että a ja b sisältää menee vaan yhden kerran kaikki jäännökset läpi**. Thus all of the mn numbers in C are incongruent to each other and therefore C forms a complete residue system modulo mn .

Now

$$\begin{aligned} \gcd(bm + an, mn) = 1 &\Leftrightarrow \gcd(bm + an, m) = 1 \text{ and } \gcd(bm + an, n) = 1 \\ &\Leftrightarrow \gcd(an, m) = 1 \text{ and } \gcd(bm, n) = 1 \\ &\Leftrightarrow \gcd(a, m) = 1 \text{ and } \gcd(b, n) = 1, \end{aligned}$$

meaning

TÄÄ TODISTUS JOUTAA ROSKIIN

□

PAREMPI TODISTUS (EHKÄ)

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

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

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: $\phi(n)$ columns containing only co-primes to m and the rest containing none of them.

Now consider the co-prime columns. Every column forms a complete residue system (mod n) ([LeVeque: chapter 3.2, theorem 3.5, p. 52](#)), 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 $\gcd(n, k) = 1$. 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 thus $\phi(mn) = \phi(m)\phi(n)$.

□

4 Tulokaavan todistus

Eulerin tulokaava arvon $\phi(n)$ laskemiseksi on hyvinkin tärkeä palanen eli todistetaan se nyt suoraan englanniksi niin ei tarvitse erikseen kääntää.

4.1 Eulers's product formula

Theorem 4.2. *Euler's product formula*

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

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 $\gcd(p^k, x) > 1$, holds $x = mp^{k-1}$ for some $m \in \{1, 2, \dots, p^{k-1}\}$.

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 ϕ is a multiplicative function

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

□

5 Funktioita ja muita

Definition 5.1. The zeta-function

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

The zeta-funtion converges, when $s > 1$.

Theorem 5.2. For all $s > 1$

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

Definition 5.3. Von Mangoldt 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 5.4.

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

Proof. Let us denote $n = \prod p^k$. Now, 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

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

□

Lemma 5.4.1.

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

Proof. By theorem 5.4 we can deduce

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

Hiffaispa mikä homma ääää

□

6 Merten's theorem

Lemma 6.0.1. If c_1, c_2, \dots is a sequence of real numbers such that $c_i = 0$ for $i < 2$ and

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

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

$$\sum_{n \leq x} c_n f(n) = C(x) f([x]) - \int_2^x C(t) f'(t) dt .$$

Proof. First we observe that $C(t) = C(n)$ and $f(n) = f([t])$, when $n \leq t \leq n+1$.

We have

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

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

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

Finally, by combining these we get

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

□

Theorem 6.1. *Merten's theorem*

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

where γ is the Euler's constant.

Proof. In this proof we show that

$$\lim_{n \rightarrow \infty} \left(\sum_{p \leq n} \left(\frac{1}{p} \right) - \log \log n + B \right) = 0,$$

which is known as Mertens' second theorem. The final form follows from theorem 428 in Hardy-Wright

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

proof of which is outside of the scope of this thesis.

Let us use the lemma 6.0.1 with the sequence, where $c_p = \frac{\log p}{p}$ with prime indices and $c_n = 0$ otherwise.

Now we have

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

TODISTUS TOKALLE YHTÄSUURUUSMERKILLE PUUTTUU

Now, with $f(t) = \frac{1}{\log t}$, as $x \rightarrow \infty$, we get

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} &= \sum_{p \leq x} \frac{c_p}{f(p)} \\ &= \frac{C(x)}{\log[x]} + \int_2^x \frac{C(t)}{t \log^2 t} dt \\ &= \frac{\log x + O(1)}{\log[x]} + \int_2^x \frac{\log t + O(1)}{t \log^2 t} dt \\ &= 1 + \int_2^x \frac{dt}{t \log t} + \frac{O(1)}{\log x} + \int_2^x \frac{O(1)}{t \log^2 t} dt \\ &= 1 + \log \log x - \log \log 2 + \frac{O(1)}{\log x} + \int_2^x \frac{O(1)}{t \log^2 t} dt \end{aligned}$$

□

7 Edellisestä versiosta poistettua paskaa

7.0.1 Are there such integers n that $\phi(n) < \sqrt{n}$?

Let's begin with \sqrt{n} . Is there such large number n that $\phi(n) < \sqrt{n}$? When checking the values of $\phi(n)$ for smaller n , we see that at least with $n = 6$ the statement is true, as $\phi(6) = 2 < \sqrt{6}$. After that, however, the values seem to be consistently above the corresponding squareroot value.

Reasonable guess would be to assume that \sqrt{n} is a lower limit for $\phi(n)$ when $n \rightarrow \infty$. With more precise examination, we see that is indeed the case.