Elli Kiiski

2021 Kandikaatopaikka

1 Hardy-Wrightin todistuksen perkaamista

G. H. Hardyn 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 alkusepitykset nyt kun sigma joudutaankin ottamaan käyttöön

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

1. $\lim_{t\to\infty} F_1(t) = 1$ ja $\lim_{t\to\infty} F_2(t) = 1$
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 $n_2, n_3, ...$

”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: $f(n) \geq F_1(\log n)$

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

Nyt

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

mistä seuraa

$$\rho < \frac{\log n}{\log\log n}. \tag{2}$$

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

$$
\begin{aligned}
\frac{\phi(n)}{n} &= \prod_{i=1}^{r}(1-\frac{1}{p_i}) && (3)\\
&= \prod_{i=1}^{r-\rho}(1-\frac{1}{p_i})\prod_{i=r-\rho+1}^{r}(1-\frac{1}{p_i}) && (4)\\
&\geq \left(\prod_{i=1}^{r-\rho}(1-\frac{1}{p_i})\right)(1-\frac{1}{\log n})^{\rho} && (5)\\
&> \left(\prod_{i=1}^{r-\rho}(1-\frac{1}{p_i})\right)(1-\frac{1}{\log n})^{\frac{\log n}{\log\log n}}. && (6)
\end{aligned}
$$

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

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

Kuitenkin funktiolle F_1 pätee Mertenin kolmannen lauseen nojalla

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

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 **??**

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

Hence

$$\log\log n_j = \log Aje^j = \log A + \log j + \log e^j = \log A + \log j + j\,. \tag{7}$$

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

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

Also, by the lemma 5.2

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

Now we can define

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

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

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

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

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

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

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

Viel semmonen johtopäätös

2 Okei, sigma-funktio tarvitaan

Definition 2.1. *The σ-function*

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

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 $p_1, p_2, ..., p_r$ are distinct primes. Then

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

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

Theorem 2.2.

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

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

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 it 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:

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

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

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

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 (mod m) and (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

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

meaning

□

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 $gdc(p^k, x) > 1$, 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

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

□

5 The zeta-function

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 $s > 1$

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

6 Merten's (third) theorem

Theorem 6.1. *Merten's (third) theorem*

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

where γ is the Euler's constant.

Proof. Oh, this seems like a työmaa

□

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 $n \to \infty$. With more precise examination, we see that is indeed the case.