

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

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

Kirjan todistuksessa todistetaan myös sigmafunktion $\sigma(n)$ yläraja ja käytetään sitä hyväksi funktion F_2 löytämiseksi. Kysymys kuuluu, että tarvitaanko sigmafunktion välttämättä, että saadaan ϕ -funktion alaraja todistetuksi. Se on kuitenkin vasta todistuksen toisen osan ongelma, joten jätetään se hetkeksi sikseen.

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

Olkoot $p_1, p_2, \dots, p_{r-\rho} \leq \log n$ 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

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

(tähän tarvitaan todistus!! kirjassa viitattu todistukseen nro. 429),

Täten ensimmäinen osa on toidstettu.

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

Tämä ei lienekään ihan niin iisi keissi.

2 Tulokaavan todistus

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

2.1 Eulers's product formula

Theorem 2.2. *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

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

□

3 Mertenin kolmas lause

Mertenin kolmas lause

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

näyttää hyvin paljon siltä, että sitä voisi hyödyntää. Pidetään mielessä ja todistetaan tarvittaessa.