TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Marita Riihiranta

# Multiplikatiivisista funktioista

Matematiikan ja tilastotieteen laitos
Matematiikka
Toukokuu 2008

Tampereen yliopisto

Matematiikan ja tilastotieteen laitos

RIIHIRANTA, MARITA: Multiplikatiivisista funktioista

Pro gradu -tutkielma, 24 s.

Matematiikka

Toukokuu 2008

---

## Tiivistelmä

Tutkielman tarkoituksena on esitellä jotain multiplikatiivisia funktioita ja niiden ominaisuuksia.

Ensimmäisessä luvussa määritellään multiplikatiivinen ja täydellisesti multiplikatiivinen funktio sekä tutustutaan Eulerin phi-funktioon. Luvussa myös todistetaan, että tämä $\phi$-funktio on multiplikatiivinen.

Toisessa luvussa tutustutaan tekijäfunktioihin ja niiden ominaisuuksiin. Aluksi määritellään luvun $n$ positiivisten tekijöiden lukumäärä ja summa sekä osoitetaan, että molemmat ovat multiplikatiivisia funktioita. Luvun $n$ tekijöiden lukumäärästä käytetään merkintään $\tau(n)$ ja luvun $n$ tekijöiden summasta merkintää $\sigma(n)$. Luvussa tutustutaan myös yleisemmin multiplikatiivisen funktion $f$ summafunktioon $F$. Summafunktio $F(n) = \Sigma_{d|n} f(d)$ on myös multiplikatiivinen.

Kolmannessa luvussa käsitellään Möbiuksen funktiota. Aluksi Möbiuksen funktio määritellään ja sen jälkeen se osoitetaan multiplikatiiviseksi. Luvussa tutustutaan myös Möbiuksen funktion summafunktioon $F(n) = \Sigma_{d|n} \mu(d)$ ja käänteiskaavaan $f(n) = \Sigma_{d|n} \mu(d) F(n/d)$. Möbiuksen käänteiskaavan avulla saadaan myös aritmeettinen lauseke ensimmäisessä luvussa mainitulle Eulerin phi-funktiolle.

Tutkielman päälähteinä on käytetty sekä Thomas Koshyn teosta Elementary Number Theory with Applications että Kenneth H. Rosenin teosta Elementary Number Theory and Its Applications.

# Sisältö

# Johdanto

Tämä tutkielma käsittelee lukuteorian alaan kuuluvia multiplikatiivisia funktioita ja niiden ominaisuuksia. Näitä funktioita on ääretön määrä ja tässä työssä on tutustuttu vain muutamiin niistä.

Ensimmäisessä luvussa määritellään käsitteet multiplikatiivinen ja täydellisesti multiplikatiivinen funktio sekä tutustutaan Eulerin phi-funktioon. Luvussa myös todistetaan, että tämä $\phi$-funktio on multiplikatiivinen.

Toisessa luvussa tutustutaan tekijäfunktioihin ja niiden ominaisuuksiin. Aluksi määritellään luvun $n$ positiivisten tekijöiden lukumäärä ja summa sekä osoitetaan, että molemmat ovat multiplikatiivisia funktioita. Luvussa tutustutaan myös yleisemmin multiplikatiivisen funktion $f$ summafunktioon $F$ ja osoitetaan, että se on multiplikatiivinen.

Kolmannessa luvussa määritellään Möbiuksen funktio ja osoitetaan, että se on multiplikatiivinen. Luvussa tutustutaan myös Möbiuksen funktion summafunktioon ja käänteiskaavaan. Möbiuksen käänteiskaavan avulla saadaan myös täsmällinen lauseke ensimmäisessä luvussa mainitulle Eulerin phi-funktiolle.

Tässä tutkielmassa lukijan oletetaan tuntevan lukuteorian peruskäsitteet. Tutkielmassa esitetyt lemmat ja lauseet on otettu lähdeteoksista todistuksineen. Esimerkit on itse keksittyjä ellei erikseen toisin mainita. Pääteosten (ks. lähdeluettelo) lisäksi on tutustuttu sekä David M. Burtonin teokseen Elementary Number Theory että Gareth A.Jonesin ja J. Mary Jonesin teokseen Elementary Number Theory. Näitä kahta ei kuitenkaan löydy lähdeluettelosta, sillä kaikki halutut asiat oli esitetty tarpeeksi selkeästi päälähdeteoksissa.

# Luku 1

# Eulerin phi-funktio

Tässä työssä tutustutaan tärkeimpiin multiplikatiivisiin funktioihin. Niistä valitaan ensimmäisenä Eulerin phi-funktio. Aluksi käsitellään multiplikatiivisuutta yleisesti ja sen jälkeen osoitetaan, että funktio $\phi$ on multiplikatiivinen.

## 1.1 Multiplikatiivinen ja täydellisesti multiplikatiivinen funktio

Määritellään ensin multiplikatiivinen ja täydellisesti multiplikatiivinen funktio.

**Määritelmä 1.1** Aritmeettinen funktio $f$ on multiplikatiivinen, jos $f(mn) = f(m)f(n)$ aina, kun $m$ ja $n$ ovat keskenään jaottomia positiivisia kokonaislukuja. Funktio $f$ on täydellisesti multiplikatiivinen, jos $f(mn) = f(m)f(n)$ kaikilla positiivisilla kokonaisluvuilla $m$ ja $n$.

**Esimerkki 1.1** Vakiofunktio $f(n) = 0$ on multiplikatiivinen, koska $f(mn) = 0 = 0 \cdot 0 = f(m)f(n)$.

Edellisessä esimerkissä ei tarvinnut edes olettaa, että $m$ ja $n$ ovat keskenään jaottomia positiivisia kokonaislukuja eli $(m, n) = 1$. Siitä huolimatta niillä on toivottu ominaisuus.

Seuraava lause (engl. fundamental theorem for multiplicative functions) mahdollistaa multiplikatiivisen funktio $f$ arvon laskemisen millä tahansa positiivisella kokonaisluvulla, kun tiedetään sen arvot alkuluvun potensseilla.

**Lause 1.1** *Olkoon $f$ multiplikatiivinen funktio ja $n$ positiivinen kokonaisluku, jonka kanoninen esitys on muotoa $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} = \Pi_{i=1}^{s} p_i^{a_i}$. Silloin $f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_s^{a_s}) = \Pi_p f(p^{n(p)})$.*

*Todistus.* (Vrt. [2], s. 240) Todistetaan lause induktiolla.
Olkoon $s = 1$. Nyt siis $n = p_1^{a_1}$, joten $f(n) = f(p_1^{a_1})$. Lause on siis triviaalisti tosi.
Oletetaan nyt, että se on tosi kaikilla positiivisilla kokonaisluvuilla, jotka voidaan esittää $k$ erisuuren alkuluvun kanonisena esityksenä. Nyt
$f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k})$.
Olkoon $n$ nyt mikä tahansa positiivinen kokonaisluku, joka on $k+1$ erisuuren alkuluvun kanoninen esitys $n = p_1^{a_1} p_2^{a_2} \cdots p_{k+1}^{a_{k+1}}$. Koska $(p_1^{a_1} \cdots p_k^{a_k}, p_{k+1}^{a_{k+1}}) = 1$ ja $f$ on multiplikatiivinen, niin
$f(p_1^{a_1} \cdots p_k^{a_k} p_{k+1}^{a_{k+1}}) = f(p_1^{a_1} \cdots p_k^{a_k}) f(p_{k+1}^{a_{k+1}})$.
Nyt induktio-oletuksen mukaan
$f(p_1^{a_1} \cdots p_k^{a_k}) f(p_{k+1}^{a_{k+1}}) = f(p_1^{a_1}) \cdots f(p_k^{a_k}) f(p_{k+1}^{a_{k+1}})$.
Siis induktion perusteella lause on tosi kaikilla positiivisilla kokonaisluvuilla $n$. □

## 1.2 Eulerin phi-funktio

Aloitetaan luku määrittelemällä Eulerin $\phi$ -funktio ja sen jälkeen tarkastellaan Eulerin $\phi$ -funktion ominaisuuksia.

**Määritelmä 1.2** Olkoon $n$ positiivinen kokonaisluku. Eulerin phi-funktio $\phi(n)$ on niiden positiivisten kokonaislukujen lukumäärä, jotka eivät ylitä lukua $n$ ja ovat suhteellisia alkulukuja luvun $n$ kanssa.

**Lause 1.2** *Jos $p$ on alkuluku, niin $\phi(p) = p - 1$. Vastaavasti, jos $p$ on positiivinen kokonaisluku, jolle $\phi(p) = p - 1$, niin $p$ on alkuluku.*

*Todistus.* (Vrt. [2], s. 241) Jos $p$ on alkuluku, niin $p$ ja jokainen sitä pienempi positiivinen kokonaisluku ovat suhteellisia alkulukuja keskenään. Koska on olemassa $p - 1$ sellaista kokonaislukua, niin saadaan $\phi(p) = p - 1$. Vastaavasti, jos $p$ ei ole alkuluku, silloin $p = 1$ tai $p$ on yhdistetty luku. Jos $p = 1$, niin $\phi(p) \neq p - 1$, koska $\phi(1) = 1$. Jos $p$ on yhdistetty luku, niin silloin luku $d$, $1 < d < p$, on luvun $p$ jakaja ja tietysti $p$ ja $d$ eivät ole suhteellisia alkulukuja keskenään. Tiedetään, että vähintään yksi kokonaisluvuista 1, 2, ..., $p-1$, nimittäin $d$, ei ole suhteellinen alkuluku luvun $p$ kanssa, joten $\phi(p) \leq p-2$. Näin ollen, jos $\phi(p) = p-1$, luvun $p$ täytyy olla alkuluku. $\square$

**Esimerkki 1.2** Laske $\phi(5)$ ja $\phi(11)$.
Ratkaisu:
$\phi(5) = 5 - 1 = 4$ ja
$\phi(11) = 11 - 1 = 10$.

**Lause 1.3** *Olkoon $p$ alkuluku ja $a$ jokin positiivinen kokonaisluku. Silloin $\phi(p^a) = p^a - p^{a-1}$.*

*Todistus.* (Vrt. [2], s. 241) Lukua $p^a$ pienemmät positiiviset kokonaisluvut, jotka eivät ole suhteellisia alkulukuja luvun $p$ kanssa, ovat niitä kokonaislukuja, jotka eivät ylitä lukua $p^a$ ja ovat jaollisia luvulla $p$. Nämä ovat ne kokonaisluvut $kp$, missä $1 \leq k \leq p^{a-1}$. Koska on olemassa täsmälleen $p^{a-1}$ kappaletta tällaisia kokonaislukuja, on olemassa $p^a - p^{a-1}$ kappaletta lukua $p^a$ pienempiä kokonaislukuja, jotka ovat suhteellisia alkulukuja luvun $p^a$ kanssa. Näin ollen $\phi(p^a) = p^a - p^{a-1}$. $\square$

**Esimerkki 1.3** Laske $\phi(27)$, $\phi(16807)$ ja $\phi(29403)$.
Ratkaisu:
$\phi(27) = \phi(3^3) = 3^3 - 3^2 = 18$,
$\phi(16807) = \phi(7^5) = 7^5 - 7^4 = 14406$ ja
$\phi(29403) = \phi(3^5 \cdot 11^2) = \phi(3^5) \cdot \phi(11^2) = (3^5 - 3^4)(11^2 - 11) = 5940$.

Seuraava esimerkki sisältää tulevan lauseen todistuksen idean.

**Esimerkki 1.4** Olkoon $m = 4$ ja $n = 5$. Nyt $(m, n) = 1$ ja $mn = 20$. Jotta voidaan selvittää $\phi(mn) = \phi(20)$, taulukoidaan kaikki positiiviset kokonaisluvut $\leq 20$ neljään riviin, joissa jokaisessa on 5 lukua. Sitten jätetään huomiotta kaikki sellaiset luvut, jotka eivät ole suhteellisia alkulukuja luvun 20 kanssa.

| | | | | |
|---|---|---|---|---|
| 1 | 5 | 9 | 13 | 17 |
| 2 | 6 | 10 | 14 | 18 |
| 3 | 7 | 11 | 15 | 19 |
| 4 | 8 | 12 | 16 | 20 |

Nyt huomataan, että ensimmäisen pystyrivin toinen ja neljäs luku eivät ole suhteellisia alkulukuja luvun $m$ kanssa, eikä siis luvun $mn$ kanssa. Itse asiassa sama koskee koko vaakariviä. Nyt siis ei yksikään toisen tai neljännen vaakarivin luvuista ole suhteellinen alkuluku luvun 20 kanssa. Siispä positiiviset kokonaisluvut $\leq 20$ ja suhteelliset alkuluvut luvun 20 kanssa löytyvät jäljelle jääneistä $2 = \phi(4)$ rivistä.

| | | | | |
|---|---|---|---|---|
| 1 | 5 | 9 | 13 | 17 |
| 3 | 7 | 11 | 15 | 19 |

Jokainen näistä luvuista on suhteellinen alkuluku luvun $m$ kanssa. Jokainen rivi sisältää $4 = \phi(5)$ lukua, jotka ovat suhteellisia alkulukuja luvun 5 kanssa. Nyt taulukko siis sisältää 8 lukua, jotka ovat suhteellisia alkulukuja luvun 20 kanssa. Täten $\phi(20) = 8 = 2 \cdot 4 = \phi(4)\phi(5)$.

**Lemma 1.1** *Olkoot $m$ ja $n$ keskenään jaottomia positiivisia kokonaislukuja ja $r$ mikä tahansa kokonaisluku. Silloin luvut*

$$r, m + r, 2m + r, ..., (n - 1)m + r$$

*ovat kongruentteja lukujen $0, 1, 2, ..., (n - 1)$ kanssa modulo $n$ jossakin järjestyksessä.*

*Todistus.* (Vrt. [1], s. 348) Riittää osoittaa, että mitkään jonon kaksi alkiota eivät ole kongruentteja modulo $n$. Oletetaan, että $km + r \equiv lm + r \pmod{n}$, missä $0 \leq k,\ l < n$. Silloin $km \equiv lm \pmod{n}$. Mutta $(m, n) = 1$, joten $k \equiv l \pmod{n}$. Koska $k$ ja $l$ ovat pienimmät jäännökset mod $n$, niin tästä seuraa, että $k = l$. Näin ollen, jos $k \neq l$, niin $km + r \not\equiv lm + r \pmod{n}$. Eli kaikilla joukon alkioilla on eri jäännös. Mutta se sisältää $n$ alkiota, joten niiden jäännökset modulo $n$ ovat uudelleen järjestettynä kokonaisluvut
$0, ..., n - 1$. □

**Lause 1.4** *Funktio $\phi$ on multiplikatiivinen.*

*Todistus.* (Vrt. [2], s. 241 ja [1], s. 348) Olkoot $m$ ja $n$ positiivisia kokonaislukuja siten, että $(m, n) = 1$. Osoitetaan, että $\phi(mn) = \phi(m)\phi(n)$. Järjestetään nyt kokonaisluvut luvusta 1 lukuun $mn$ siten, että saadaan taulukko, jossa on $m$ riviä ja niissä jokaisessa $n$ kappaletta lukuja.

| | | | | |
|---|---|---|---|---|
| $1$ | $m+1$ | $2m+1$ | ... | $(n-1)m+1$ |
| $2$ | $m+2$ | $2m+2$ | ... | $(n-1)m+2$ |
| $3$ | $m+3$ | $2m+3$ | ... | $(n-1)m+3$ |
| $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ |
| $r$ | $m+r$ | $2m+r$ | ... | $(n-1)m+r$ |
| $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ |
| $m$ | $2m$ | 3m | ... | $nm$ |

Olkoon $r$ positiivinen kokonaisluku $\leq m$ siten, että $(r, m) > 1$. Osoitamme, ettei mikään taulukon luvuista ole suhteellinen alkuluku luvun $mn$ kanssa. Olkoon $d = (r, m)$. Silloin $d|r$ ja $d|m$, joten $d|km + r$ millä tahansa kokonaisluvulla $k$. Nyt siis $d$ on jokaisen luvun jakaja rivillä $r$. Nyt mikään luku riviltä $r$ ei ole suhteellinen alkuluku luvun $m$ kanssa, eikä siten luvun $mn$ kanssa, jos $(r, m) > 1$. Toisin sanoen taulukon luvut, jotka ovat suhteellisia alkulukuja luvun $mn$ kanssa, tulevat riviltä $r$ vain jos $(r, m) = 1$. Määritelmän mukaan on olemassa $\phi(m)$ sellaisia kokonaislukuja $r$ ja siten $\phi(m)$ kappaletta sellaisia rivejä. Tarkastellaan nyt riviä $r$, jossa $(r, m) = 1$:

$$r, m + r, 2m + r, ..., (n - 1)m + r.$$

Lemma 1.1 mukaan rivin $r$ pienin jäännös modulo $n$ on permutaatio luvuista 0, 1, 2, ..., $(n - 1)$, jossa $\phi(n)$ on suhteellinen alkuluku luvun $n$ kanssa. Nyt löytyy $\phi(m)$ kappaletta rivejä sisältäen positiivisia kokonaislukuja, jotka ovat suhteellisia alkulukuja luvun $mn$ kanssa. Jokainen näistä riveistä sisältää $\phi(n)$ lukua, jotka ovat sen kanssa suhteellisia alkulukuja. Siis taulukko sisältää $\phi(m)\phi(n)$ positiivista kokonaislukua, jotka ovat $\leq mn$ ja suhteellisia alkulukuja luvun $mn$ kanssa. Täten $\phi(mn) = \phi(m)\phi(n)$. $\square$

Lauseita 1.3 ja 1.4 voidaan soveltaa tehokkaasti funktion $\phi(n)$ täsmällisen kaavan johtamisessa.

**Lause 1.5** *Olkoon $n$ positiivinen kokonaisluku ja sen kanoninen esitys $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$. Silloin*

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_s}).$$

*Todistus.* (Vrt. [1], s. 350) Koska $\phi$ on multiplikatiivinen, niin lauseen 1.1 mukaan se saadaan muotoon

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_s^{a_s}).$$

Lauseen 1.3 mukaan $\phi(p^a) = p^a - p^{a-1}$, joten

$$\begin{aligned}\phi(n) &= p_1^{a_1}(1 - \frac{1}{p_1})p_2^{a_2}(1 - \frac{1}{p_2}) \cdots p_s^{a_s}(1 - \frac{1}{p_s}) \\ &= p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_s}) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_s}).\end{aligned}$$

Lause on täten todistettu. $\square$

**Esimerkki 1.5** Laske $\phi(525)$ ja $\phi(31625)$.
Ratkaisu:
$525 = 3 \cdot 5^2 \cdot 7$, joten $\phi(525) = 525(1 - \frac{1}{3})(1 - \frac{1}{5})(1 - \frac{1}{7}) = 240$ ja
$31625 = 5^3 \cdot 11 \cdot 23$, joten $\phi(31625) = 31625(1 - \frac{1}{5})(1 - \frac{1}{11})(1 - \frac{1}{23}) = 22000$.

Tämän kappaleen 1.2 esimerkeistä huomataan, että funktio $\phi(n)$ on usein parillinen. Itse asiassa se on parillinen aina, kun $n > 2$. Tämä todistetaan seuraavassa lauseessa.

**Lause 1.6** *Jos $n$ on positiivinen kokonaisluku ja $n \geq 3$, niin $\phi(n)$ on parillinen.*

*Todistus.* (Vrt. [2], s. 243) Merkitään, että $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ on luvun $n$ kanoninen esitys. Koska $\phi$ on multiplikatiivinen, niin

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_s^{a_s}).$$

Lauseen 1.3 mukaan

$$\phi(p_j^{a_j}) = p_j^{a_j} - p_j^{a_j-1} = p_j^{a_j-1}(p_j - 1).$$

Tästä huomataan, että $\phi(p_j^{a_j})$ on parillinen, jos $p_j$ on pariton alkuluku, koska silloin $p_j - 1$ on parillinen. Vastaavasti, jos $p_j = 2$ ja $a_j > 1$, on $p_j^{a_j-1}$ parillinen. Koska $n \geq 3$, ainakin toinen näistä kahdesta ehdosta toteutuu, joten $\phi(p_j^{a_j})$ on parillinen ainakin yhdellä luvulla $j$, $1 \leq j \leq s$. Tästä seuraa, että $\phi(n)$ on parillinen. □

**Lause 1.7** *Olkoon $n$ positiivinen kokonaisluku. Silloin $\Sigma_{d|n}\phi(d) = n$.*

*Todistus.* (Vrt. [2], s. 244) Aluksi kokonaisluvut $1, 2, ..., n$ jaetaan ryhmiin. Laitetaan luku $m$ ryhmään $C_d$, jos lukujen $m$ ja $n$ suurin yhteinen tekijä on $d$. Nyt luku $m$ on ryhmässä $C_d$ eli ryhmässä $(m, n) = d$, jos ja vain jos $(m/d, n/d) = 1$. Täten ryhmän $C_d$ kokonaislukujen määrä on niiden positiivisten kokonaislukujen määrä, jotka eivät ylitä lukua $n/d$ ja ovat suhteellisia alkulukuja luvun $n/d$ kanssa. Nyt huomataan, että ryhmässä $C_d$ on $\phi(n/d)$ kokonaislukua. Koska kokonaisluvut $1, 2, ..., n$ on jaettu erillisiin ryhmiin ja jokainen luku on yhdessä ryhmässä, luku $n$ on eri ryhmien alkioiden lukumäärien summa. Täten huomataan, että $n = \Sigma_{d|n}\phi(n/d)$. Koska $d$ käy läpi kaikki positiiviset kokonaisluvut, jotka jakavat luvun $n$, niin myös $n/d$ käy läpi nämä samat luvut. Siis

$$n = \Sigma_{d|n}\phi(n/d) = \Sigma_{d|n}\phi(d).$$

Lause on täten todistettu. □

**Esimerkki 1.6** Osoita, että $\Sigma_{d|28}\phi(d) = 28$.
Ratkaisu:
Luvun 28 positiiviset tekijät ovat 1,2,4,7,14 ja 28.
Siis
$\Sigma_{d|28}\phi(d) = \phi(1)+\phi(2)+\phi(4)+\phi(7)+\phi(14)+\phi(28) = 1+1+2+6+6+12 = 28.$

# Luku 2

# Tekijäfunktiot

Edellisessä luvussa osoitettiin, että funktio $\phi$ on multiplikatiivinen. Tässä luvussa tarkastellaan kahta funktiota, $\tau$ ja $\sigma$. Tietysti myös osoitetaan, että ne ovat multiplikatiivisia.

## 2.1 $\tau$- ja $\sigma$-funktiot

Määritellään aluksi nämä funktiot.

**Määritelmä 2.1** Olkoon $n$ positiivinen kokonaisluku. Silloin $\tau(n)$ määritellään kaavalla

$$\tau(n) = \Sigma_{d|n} 1.$$

Funktio $\tau(n)$ on siis luvun $n$ positiivisten tekijöiden lukumäärä.

**Määritelmä 2.2** Olkoon $n$ positiivinen kokonaisluku. Silloin $\sigma(n)$ määritellään kaavalla

$$\sigma(n) = \Sigma_{d|n} d.$$

Funktio $\sigma(n)$ on siis luvun $n$ positiivisten tekijöiden summa.

**Esimerkki 2.1** Laske positiivisten tekijöiden lukumäärä ja summa seuraaville luvuille
a) 22 b) 36.

Ratkaisu:

a) Luvun 22 tekijät ovat $1, 2, 11$ ja $22$.
Nyt $\tau(22) = \Sigma_{d|22} 1 = 1 + 1 + 1 + 1 = 4$ ja
$\sigma(22) = \Sigma_{d|22} d = 1 + 2 + 11 + 22 = 36$.

b) Luvun 36 tekijät ovat $1, 2, 3, 4, 6, 9, 12, 18$ ja $36$.
Vastaavasti nyt $\tau(36) = \Sigma_{d|36} 1 = 9$ ja $\sigma(36) = \Sigma_{d|36} d = 91$.

Todistamme seuraavan lauseen helpottaaksemme funktioiden $\tau$ ja $\phi$ multiplikatiivisiksi todistamisia.

**Lause 2.1** *Jos $f$ on multiplikatiivinen, niin funktion $f$ summafunktio*

$$F(n) = \Sigma_{d|n} f(d)$$

*on myös multiplikatiivinen.*

Todistus. (Vrt. [2], s. 251) Jotta voidaan osoittaa, että $F$ on multiplikatiivinen funktio, on osoitettava, että $F(mn) = F(m)F(n)$, kun $m$ ja $n$ ovat suhteellisia alkulukuja keskenään. Siis oletetaan, että $(m, n) = 1$. Nyt

$$F(mn) = \Sigma_{d|mn} f(d).$$

Koska $(m, n) = 1$, jokainen positiivinen luvun $mn$ tekijä voidaan yksikäsitteisesti kirjoittaa muodossa $d_1 d_2$, missä $d_1 \mid m$, $d_2 \mid n$ ja $(d_1, d_2) = 1$. Voidaan siis kirjoittaa

$$F(mn) = \Sigma_{d_1|m, d_2|n} f(d_1 d_2).$$

Koska $f$ on multiplikatiivinen ja $(d_1, d_2) = 1$, niin

$$\begin{aligned} F(mn) &= \Sigma_{d_1|m, d_2|n} f(d_1) f(d_2) \\ &= \Sigma_{d_1|m} f(d_1) \Sigma_{d_2|n} f(d_2) \\ &= F(m)F(n). \end{aligned}$$

Siis $F$ on multiplikatiivinen. □

**Esimerkki 2.2** Olkoon funktio $f$ multiplikatiivinen ja $F(n) = \Sigma_{d|n} f(d)$. Osoita, että $F(15) = F(3)F(5)$.
Ratkaisu:
Luvun 15 positiiviset tekijät ovat $1, 3, 5$ ja 15. Nyt
$F(15) = \Sigma_{d|15} f(d) = f(1) + f(3) + f(5) + f(15)$.
Koska funktio $f$ on multiplikatiivinen, niin esimerkiksi $f(1) = f(1)f(1)$ ja $f(15) = f(3)f(5)$.
Siis

$$\begin{aligned} F(15) &= f(1)f(1) + f(1)f(3) + f(1)f(5) + f(3)f(5) \\ &= (f(1) + f(3))(f(1) + f(5)) \\ &= F(3)F(5). \end{aligned}$$

Nyt voidaan osoittaa, että funktiot $\sigma$ ja $\tau$ ovat multiplikatiivisia.

**Lause 2.2** *Tau- ja Sigma-funktio ovat multiplikatiivisia.*

Todistus. (Vrt. [2], s. 252) Olkoon $f(n) = n$ ja $g(n) = 1$. Molemmat funktiot $f$ ja $g$ ovat multiplikatiivisia. Lauseen 2.1 mukaan funktiot $\sigma(n) = \Sigma_{d|n} f(d)$ ja $\tau(n) = \Sigma_{d|n} g(d)$ ovat multiplikatiivisia. □

## 2.2 Tekijäfunktioiden ominaisuuksia

Edellisessä pykälässä osoitettiin, että funktiot $\sigma$ ja $\tau$ ovat multiplikatiivisia.

Jatketaan vielä näiden funktioiden tarkastelua. Otetaan ensin esimerkki, jossa tarkastellaan geometrisen sarjan osasummaa. Osasummaa tarvitaan seuraavan lemman todistuksessa.

**Esimerkki 2.3** (Vrt. [2], s. 18) Jotta voidaan laskea osasumma
$S = \Sigma_{j=0}^{n} ar^j$, eli geometrisen sarjan $n+1$ ensimmäisen termin
$a, ar, ..., ar^k, ..., ar^n$ summa, yhtälö kerrotaan puolittain luvulla $r$.

$$\begin{aligned} rS &= r\Sigma_{j=0}^{n} ar^j \\ &= \Sigma_{j=0}^{n} ar^{j+1} \\ &= \Sigma_{k=1}^{n+1} ar^k \quad \text{(suoritetaan muuttujan vaihto)} \\ &= \Sigma_{k=0}^{n} ar^k + (ar^{n+1} - a) \\ &= S + (ar^{n+1} - a). \end{aligned}$$

Tästä seuraa, että

$$rS - S = (ar^{n+1} - a).$$

Kun $r \neq 1$, ratkaisu on

$$S = \frac{ar^{n+1} - a}{r - 1}.$$

Vastaavasti, kun $r = 1$

$$\Sigma_{j=0}^{n} ar^j = \Sigma_{j=0}^{n} a = (n+1)a.$$

**Lemma 2.1** *Olkoon $p$ alkuluku ja $a$ positiivinen kokonaisluku. Silloin*

$$\sigma(p^a) = 1 + p + p^2 + ... + p^a = \frac{p^{a+1} - 1}{p - 1} \tag{2.2.1}$$

*ja*

$$\tau(p^a) = a + 1. \tag{2.2.2}$$

*Todistus.* (Vrt. [2], s. 252) Luvun $p^a$ tekijät ovat 1, $p$, $p^2$, ..., $p^{a-1}$ ja $p^a$.
Koska luvulla $p^a$ on täsmälleen $a + 1$ tekijää, niin $\tau(p^a) = a + 1$.
Edellisen esimerkin osasumman kaavassa korvataan luvut $n$, $a$ ja $r$ luvuilla $a$, 1 ja $p$. Nyt

$$\sigma(p^a) = \Sigma_{j=0}^{a} p^j = 1 + p + p^2 + ... + p^{a-1} + p^a = \frac{p^{a+1} - 1}{p - 1}.$$

□

**Esimerkki 2.4** Laske positiivisten tekijöiden lukumäärä ja summa seuraaville luvuille
a) 625 b) 6561.
Ratkaisu:

a) Luku 625 voidaan esittää alkulukupotenssina $5^4$.
Nyt $\tau(625) = \tau(5^4) = 4 + 1 = 5$ ja
$\sigma(625) = \sigma(5^4) = 1 + 5 + 5^2 + 5^3 + 5^4 = \frac{5^{4+1}-1}{5-1} = 781.$

b) Luku 6561 voidaan esittää alkulukupotenssina $3^8$.
Vastaavasti nyt $\tau(6561) = \tau(3^8) = 9$ ja
$\sigma(6561) = \sigma(3^8) = 1 + 3 + 3^2 + ... + 3^8 = \frac{3^{8+1}-1}{3-1} = 9841.$

**Lause 2.3** *Olkoon positiivinen kokonaisluku $n$ jaettu alkulukutekijöihin seuraavasti $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$. Nyt*

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \ \cdots \ \cdot \frac{p_s^{a_s+1} - 1}{p_s - 1} = \Pi_{j=1}^{s} \frac{p_j^{a_j+1} - 1}{p_j - 1}$$

*ja*

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_s + 1) = \Pi_{j=1}^{s} (a_j + 1).$$

*Todistus.* (Vrt. [2], s.252) Koska $\sigma$ ja $\tau$ ovat molemmat multiplikatiivisia funktioita, huomataan, että

$$\sigma(n) = \sigma(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}) = \sigma(p_1^{a_1}) \sigma(p_2^{a_2}) \cdots \sigma(p_s^{a_s})$$

ja

$$\tau(n) = \tau(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}) = \tau(p_1^{a_1}) \tau(p_2^{a_2}) \cdots \tau(p_s^{a_s}).$$

Käyttämällä edellisen lemman 2.1 lausekkeita (2.2.1) ja (2.2.2) saadaan halutut arvot funktioille $\sigma(p_i^{a_i})$ ja $\tau(p_i^{a_i})$. □

**Esimerkki 2.5** Laske positiivisten tekijöiden lukumäärä ja summa seuraaville luvuille
a) 288 b) 43659.
Ratkaisu:

a) Luku 288 voidaan esittää muodossa $2^5 \cdot 3^2$.
Nyt $\tau(288) = \tau(2^5 \cdot 3^2) = (5+1)(2+1) = 18$ ja
$\sigma(288) = \sigma(2^5 \cdot 3^2) = \frac{2^{5+1}-1}{2-1} \cdot \frac{3^{2+1}-1}{3-1} = 63 \cdot 13 = 819$.

b) Luku 43659 voidaan esittää muodossa $3^4 \cdot 7^2 \cdot 11$.
Vastaavasti nyt $\tau(43659) = \tau(3^4 \cdot 7^2 \cdot 11) = (4+1)(2+1)(1+1) = 30$ ja
$\sigma(43659) = \sigma(3^4 \cdot 7^2 \cdot 11) = \frac{3^{4+1}-1}{3-1} \cdot \frac{7^{2+1}-1}{7-1} \cdot \frac{11^{1+1}-1}{11-1} = 121 \cdot 57 \cdot 12 = 82764$.

Tutkitaan seuraavassa esimerkissä funktiota $\sigma_k$ ja osoitetaan, että se on multiplikatiivinen.

**Esimerkki 2.6** Olkoon $\sigma_k(n)$ luvun $n$ tekijöiden $k$. potenssien summa eli $\sigma_k(n) = \Sigma_{d|n} d^k$. Huomioidaan myös, että $\sigma_1(n) = \sigma(n)$. Osoitetaan, että funktio $\sigma_k$ on multiplikatiivinen.

*Todistus.* (Vrt. [2], s.652) Oletetaan, että $a$ ja $b$ ovat keskenään jaottomia positiivisia kokonaislukuja. Haluamme nyt todistaa, että $\sigma_k(n)$ on multiplikatiivinen eli $\sigma_k(ab) = \sigma_k(a)\sigma_k(b)$. Nyt

$$\sigma_k(ab) = \Sigma_{d|ab} d^k = \Sigma_{d_1|a, d_2|b}(d_1 d_2)^k = \Sigma_{d_1|a} d_1^k \cdot \Sigma_{d_2|b} d_2^k = \sigma_k(a)\sigma_k(b).$$

Siis funktio $\sigma_k(n)$ on multiplikatiivinen. $\square$

# Luku 3

# Möbiuksen funktio $\mu$

Tässä luvussa määritellään Möbiuksen funktio $\mu$ ja osoitetaan, että se on multiplikatiivinen. Tarkastellaan myös Möbiuksen funktion summafunktiota ja kuuluisaa Möbiuksen käänteiskaavaa.

## 3.1 Määritelmä ja multiplikatiivisuus

**Määritelmä 3.1** Olkoon $n$ positiivinen kokonaisluku. Silloin

$$\mu(n) = \begin{cases} 1, & \text{jos } n = 1, \\ 0, & \text{jos } p^2 | n \text{ jollain alkuluvulla } p \text{ ja} \\ (-1)^k, & \text{jos } n = p_1 p_2 \cdots p_k, \text{ missä luvut } p_i \text{ ovat erisuuria alkulukuja.} \end{cases}$$

Määritelmän mukaan $\mu(n) = 0$ aina, kun luku $n$ on jaollinen alkuluvun neliöllä. Ainoat luvun $n$ arvot, joilla $\mu(n) \neq 0$, ovat ne luvut $n$, jotka ovat neliövapaita.

**Esimerkki 3.1** Laske a) $\mu(825)$ b) $\mu(3094)$.
Ratkaisu:

a) Luku 825 voidaan esittää muodossa $3 \cdot 5^2 \cdot 11$. Koska luvun tekijöissä on yksi alkuluvun neliö eli $5^2$, niin luku 825 ei ole neliövapaa ja $\mu(825) = \mu(3 \cdot 5^2 \cdot 11) = 0$.

b) Luku 3094 voidaan esittää muodossa $2 \cdot 7 \cdot 13 \cdot 17$ eli se on neliövapaa luku.
Nyt $\mu(3094) = \mu(2 \cdot 7 \cdot 13 \cdot 17) = (-1)^4 = 1$.

Todistetaan seuraavaksi, että Möbiuksen funktio on multiplikatiivinen.

**Lause 3.1** *Funktio $\mu$ on multiplikatiivinen.*

*Todistus.* (Vrt. [1], s. 383) Jotta voidaan osoittaa, että $\mu(n)$ on multiplikatiivinen, on osoitettava, että $\mu(mn) = \mu(m)\mu(n)$.
Olkoot $m$ ja $n$ positiivisia kokonaislukuja ja keskenään suhteellisia alkulukuja. Jos $m = 1$ tai $n = 1$, niin silloin ainakin toinen luvuista $\mu(m)$ ja $\mu(n)$ on 1 ja siis $\mu(mn) = \mu(m)\mu(n)$.
Oletetaan nyt, että $m$ tai $n$ on jaollinen alkuluvun neliöllä $p^2$.
Silloin $\mu(m)\mu(n) = 0$. Jos $p^2|m$ tai $p^2|n$, niin silloin myös $p^2|mn$ ja $\mu(mn) = 0$.
Siis $\mu(mn) = \mu(m)\mu(n)$.
Lopuksi oletetaan, että $m$ ja $n$ ovat neliövapaita. Olkoon $m = p_1p_2 \cdots p_r$ ja $n = q_1q_2 \cdots q_s$, missä $p_i$:t ja $q_j$:t ovat eri alkulukuja. Nyt $(m, n) = 1$. Siis $\mu(m) = (-1)^r$ ja $\mu(n) = (-1)^s$. Nyt $mn = p_1p_2 \cdots p_rq_1q_2 \cdots q_s$. Siis

$$\mu(mn) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \mu(m)\mu(n).$$

Koska jokaisessa tapauksessa $\mu(mn) = \mu(m)\mu(n)$, funktio $\mu$ on multiplikatiivinen. □

## 3.2 Möbiuksen funktion summafunktio ja käänteiskaava

Seuraavaksi tarkastellaan lauseketta $\Sigma_{d|n}\mu(d)$. Kun $n = 1$, on $\Sigma_{d|1}\mu(d) = \mu(1) = 1$. Jos $n > 1$, summa voidaan laskea käyttämällä luvun $n$ kanonista muotoa ja lausetta 2.1 olettaen, että tiedätään summa, kun luku $n$ on alkulukupotenssi $p^a$. Tätä varten tarvitaan uusi funktio, kuten seuraava lemma osoittaa.

**Lemma 3.1** *Olkoon $F(n) = \Sigma_{d|n}\mu(d)$. Silloin $F(p^a) = 0$, missä $a > 1$.*

*Todistus.* (Vrt. [1], s. 383) Valitaan $n = p^a$. Nyt oletuksen mukaan

$$F(p^a) = \Sigma_{d|p^a}\mu(d).$$

Luvun $p^a$ tekijät ovat 1, $p$, $p^2$, ..., $p^a$, joten

$$\begin{aligned} F(p^a) &= \Sigma_{i=0}^a \mu(p^i) \\ &= \mu(1) + \mu(p) + \mu(p^2) + ... + \mu(p^a) \\ &= 1 + (-1) + 0 + ... + 0 \\ &= 0. \end{aligned}$$

□

**Lause 3.2** *Olkoon $n$ positiivinen kokonaisluku. Silloin Möbiuksen funktion summafunktio saadaan muotoon*

$$\Sigma_{d|n}\mu(d) = \begin{cases} 1, & \textit{jos } n = 1 \textit{ ja} \\ 0, & \textit{jos } n > 1. \end{cases}$$

*Todistus.* (Vrt. [1], s. 384) Jos $n = 1$, niin $\Sigma_{d|1}\mu(d) = \mu(1) = 1$. Olkoon nyt $n > 1$ ja $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ luvun $n$ kanoninen esitys. Olkoon lisäksi $F(n) = \Sigma_{d|n}\mu(d)$. Koska $\mu$ on multiplikatiivinen, niin lauseen 2.1 mukaan myös sen summafunktio $F$ on multiplikatiivinen. Nyt siis

$$F(n) = \Pi_{i=1}^s F(p^{a_i}) = F(p_1^{a_1})F(p_2^{a_2}) \cdots F(p_s^{a_s}).$$

Koska lemman 3.1 mukaan oikeanpuoleiset termit ovat $= 0$, niin myös $F(n) = 0$. □

**Esimerkki 3.2** Laske $\Sigma_{d|n}\mu(d)$, kun luku n on a) 25 b) 58 c) 343.
Ratkaisu:

a) Luvun 15 tekijät ovat 1, 5 ja $25 = 5^2$.
Nyt

$$\begin{aligned} \Sigma_{d|25}\mu(d) &= \mu(1) + \mu(5) + \mu(5^2) \\ &= 1 + (-1) + 0 = 0. \end{aligned}$$

b) Luvun 58 tekijät ovat 1, 2, 29 ja $58 = 2 \cdot 29$.
Nyt

$$\begin{aligned} \Sigma_{d|58}\mu(d) &= \mu(1) + \mu(2) + \mu(29) + \mu(2 \cdot 29) \\ &= 1 + (-1) + (-1) + (-1)^2 = 0. \end{aligned}$$

c) Luvun 343 tekijät ovat 1, 7, $49 = 7^2$ ja $343 = 7^3$.
Nyt

$$\begin{aligned}\Sigma_{d|343}\mu(d) &= \mu(1) + \mu(7) + \mu(7^2) + \mu(7^3) \\ &= 1 + (-1) + 0 + 0 = 0.\end{aligned}$$

Seuraava lause (engl. Möbius Inversion Formula) käsittelee Möbiuksen käänteiskaavaa. Se tarjoaa mahdollisuuden esittää funktion $f$ arvot sen summafunktion $F$ arvoina.

**Lause 3.3** *(Möbiuksen käänteiskaava) Olkoon $f$ aritmeettinen funktio ja olkoon sen summafunktio $F(n) = \Sigma_{d|n} f(d)$. Silloin kaikilla positiivisilla kokonaisluvuilla $n$ on*

$$f(n) = \Sigma_{d|n}\mu(d)F(n/d).$$

*Todistus.* (Vrt. [2], s. 272) Tämä todistus edellyttää kaksoissummien käyttöä. Aloitetaan tutkiminen kaavan oikeanpuoleisesta summasta, jossa korvataan lauseke $F(n/d)$ lausekkeella $\Sigma_{a|(n/d)} f(a)$. Lauseke $\Sigma_{a|(n/d)} f(a)$ saadaan suoraan funktion $f$ summafunktion $F$ määritelmästä. Nyt

$$\begin{aligned}\Sigma_{d|n}\mu(d)F(n/d) &= \Sigma_{d|n}(\mu(d)\Sigma_{a|(n/d)} f(a)) \\ &= \Sigma_{d|n}(\Sigma_{a|(n/d)}\mu(d)f(a)).\end{aligned}$$

Kokonaislukuparien $(d, a)$ joukko, jossa $d|n$ ja $a|(n/d)$, on sama kuin kokonaislukuparien $(d, a)$ joukko, jossa $a|n$ ja $d|(n/a)$. Tästä seuraa, että

$$\begin{aligned}\Sigma_{d|n}(\Sigma_{a|(n/d)}\mu(d)f(a)) &= \Sigma_{a|n}(\Sigma_{d|(n/a)} f(a)\mu(d)) \\ &= \Sigma_{a|n}(f(a)\Sigma_{d|(n/a)}\mu(d)).\end{aligned}$$

Nyt edellisen lauseen 3.2 mukaan $\Sigma_{d|(n/a)}\mu(d) = 0$, ellei $n/a = 1$. Silloin, kun $n/a = 1$ eli kun $n = a$, on $\Sigma_{d|(n/a)}\mu(d) = 1$. Siis

$$\Sigma_{a|n}(f(a)\Sigma_{d|(n/a)}\mu(d)) = f(n) \cdot 1 = f(n).$$

Lause on täten todistettu. □

Möbiuksen käänteiskaava voidaan myös kirjoittaa muodossa

$$f(n) = \Sigma_{d|n}\mu(n/d)F(d).$$

Huomaa, että määritelmä $F(n) = \Sigma_{d|n} f(d)$ esittää summafunktion $F$ funktion $f$ termein. Kun taas käänteiskaava esittää funktion $f$ summafunktion $F$ termein. Valaistaan seuraavaksi hieman käänteiskaavaa. Muistutetaan ensin mieleen, että

$$\tau(n) = \Sigma_{d|n} = 1 \text{ ja } \sigma(n) = \Sigma_{d|n} = d.$$

Sekä vakiofunktio $f(n) = 1$ että identiteettifunktio $g(n) = n$ ovat multiplikatiivisia, joten edellisestä lauseesta 3.3 seuraa, että

$$1 = \Sigma_{d|n} \mu(d)\tau(n/d) = \Sigma_{d|n} \mu(n/d)\tau(d) \tag{3.2.1}$$

ja

$$n = \Sigma_{d|n} \mu(d)\sigma(n/d) = \Sigma_{d|n} \mu(n/d)\sigma(d). \tag{3.2.2}$$

**Esimerkki 3.3** Osoita edelliset yhtälöt (3.2.1) ja (3.2.2) tosiksi luvun $n$ arvolla 27.
Ratkaisu:

(1) Luvun 27 tekijät ovat 1, 3, 9 ja 27.
Nyt

$$\begin{aligned}\Sigma_{d|27} \mu(d)\tau(27/d) &= \mu(1)\tau(27) + \mu(3)\tau(9) + \mu(9)\tau(3) + \mu(27)\tau(1)\\ &= 1 \cdot \tau(27) + (-1) \cdot \tau(9) + 0 \cdot \tau(3) + 0 \cdot \tau(1)\\ &= 4 - 3 = 1.\end{aligned}$$

(2) Vastaavasti

$$\begin{aligned}\Sigma_{d|27} \mu(d)\sigma(n/d) &= \mu(1)\sigma(27) + \mu(3)\sigma(9) + \mu(9)\sigma(3) + \mu(27)\sigma(1)\\ &= 1 \cdot 40 + (-1) \cdot 13 + 0 \cdot 4 + 0 \cdot 1 = 27.\end{aligned}$$

$\square$

Lauseen 2.1 mukaan funktion $f$ ollessa multiplikatiivinen myös sen summafunktio $F(n) = \Sigma_{(d|n)} f(d)$ on multiplikatiivinen. Toinen hyödyllinen seuraus Möbiuksen käänteiskaavasta on, että edellinen voidaan kääntää myös toisinpäin. Eli, jos aritmeettisen funktion $f$ summafunktio $F$ on multiplikatiivinen, niin myös funktio $f$ on multiplikatiivinen.

**Lause 3.4** *Olkoon $f$ aritmeettinen funktio, jonka summafunktio on $F = \Sigma_{d|n} f(d)$. Silloin, jos $F$ on multiplikatiivinen, myös $f$ on multiplikatiivinen.*

*Todistus.* (Vrt. [2], s. 273) Oletetaan, että $m$ ja $n$ ovat keskenään jaottomia positiivisia kokonaislukuja. Halutaan osoittaa, että $f(mn) = f(m)f(n)$. Muistutetaan mieleen, että jos $d$ on luvun $mn$ jakaja, niin $d = d_1 d_2$, missä $d_1|m$, $d_2|n$ ja $(d_1, d_2) = 1$. Käyttämällä Möbiuksen käänteiskaavaa ja tietoa, että $\mu$ ja $F$ ovat multiplikatiivisia, saadaan

$$
\begin{aligned}
f(mn) &= \Sigma_{d|mn} \mu(d) F(\frac{mn}{d}) \\
&= \Sigma_{d_1|m, d_2|n} \mu(d_1 d_2) F(\frac{mn}{d_1 d_2}) \\
&= \Sigma_{d_1|m, d_2|n} \mu(d_1)\mu(d_2) F(\frac{m}{d_1}) F(\frac{n}{d_2}) \\
&= \Sigma_{d_1|m} \mu(d_1) F(\frac{m}{d_1}) \cdot \Sigma_{d_2|n} \mu(d_2) F(\frac{n}{d_2}) \\
&= f(m)f(n).
\end{aligned}
$$

Lause on siis todistettu. □

Käyttämällä Möbiuksen käänteiskaavaa, saadaan seuraavassa lauseessa aritmeettinen lauseke funktiolle $\phi(n)$.

**Lause 3.5** *Olkoon $n$ positiivinen kokonaisluku. Silloin $\phi(n) = n\Sigma_{d|n} \frac{\mu(d)}{d}$.*

*Todistus.* (Vrt. [1], s. 677) Lauseen 1.7 mukaan $n = \Sigma_{d|n} \phi(d)$. Siis Möbiuksen käänteiskaavan mukaan

$$\phi(n) = \Sigma_{d|n} \mu(d)(n/d) = n\Sigma_{d|n} \frac{\mu(d)}{d}.$$

□

**Esimerkki 3.4** Laske $n\Sigma_{d|n}\frac{\mu(d)}{d}$ luvun $n$ arvolla 16.
Ratkaisu:
Luvun 16 tekijät ovat 1, 2, 4, 8 ja 16.
Nyt

$$\begin{aligned}16\Sigma_{d|16}\frac{\mu(d)}{d} &= 16\mu(1)+8\mu(2)+4\mu(4)+2\mu(8)+\mu(16)\\ &= 16\cdot 1+8\cdot(-1)+4\cdot 0+2\cdot 0+0\\ &= 8=\phi(16).\end{aligned}$$

**Lause 3.6** *Olkoot $F$ ja $f$ aritmeettisia funktioita siten, että*

$$f(n)=\Sigma_{d|n}\mu(d)F(n/d).$$

*Silloin $F(n)=\Sigma_{d|n}f(d)$.*

*Todistus.* (Vrt. [1], s. 388) Funktion $f$ määritelmän mukaan

$$f(d)=\Sigma_{d'|d}\mu(d')F(d/d').$$

Nyt

$$\Sigma_{d|n}f(d)=\Sigma_{d|n}\Sigma_{d'|d}\mu(d')F(d/d').$$

Merkitään $d/d'=k$ ja $n/d=l$. Silloin $d=kd'$ ja $n=ld=kld'$, joten yhtälö saadaan nyt muotoon

$$\begin{aligned}\Sigma_{d|n}f(d) &= \Sigma_{d|n}\Sigma_{kd'=d}\mu(d')F(k)\\ &= \Sigma_{kd'|n}\mu(d')F(k)\\ &= \Sigma_{k|n}F(k)[\Sigma_{d'|(n/k)}\mu(d')].\end{aligned}$$

Lauseen 3.2 mukaan $\Sigma_{d'|(n/k)}\mu(d')=1$, jos $n=k$, ja nolla muutoin. Siis yhtälö saadaan muotoon

$$\Sigma_{d|n}f(d)=F(n)\cdot(1)=F(n).$$

Näin ollen $F(n)=\Sigma_{d|n}f(d)$. $\square$

# Kirjallisuutta


[1] Koshy, Thomas, Elementary Number Theory with Applications, Harcourt/Academic Press, 2002.

[2] Rosen, Kenneth H., Elementary Number Theory and Its Applications, 5th edition, AT & T Laboratories and Kenneth H. Rosen, 2005.