TAMPEREEN YLIOPISTO
Pro gradu-tutkielma

Katja Auvinen

Tekijäfunktiosta ja sen ominaisuuksista

Matematiikan, tilastotieteen ja filosofian laitos
Matematiikka
Toukokuu 2005

Tampereen Yliopisto

Matematiikan, tilastotieteen ja filosofian laitos

AUVINEN, KATJA: Tekijäfunktiosta ja sen omaisuuksista

Pro gradu -tutkielma, 44s.

Matematiikka

Toukokuu 2005

Tiivistelmä

Työ käsittelee tekijäfunktiota ja sen ominaisuuksia. Aluksi määritellään käsitteitä, joita tarvitaan varsinaisen aiheen käsittelyyn. Ensimmäisessä luvussa määritellään muun muassa aritmeettinen funktio ja funktion multiplikatiivisuus.

Toisessa luvussa määritellään tekijäfunktio. Tekijäfunktiolla voidaan määrittää sekä luvun n tekijöiden lukumäärä, että luvun n tekijöiden summa. Tekijöiden lukumäärää merkitään symbolilla $d(n)$ ja tekijöiden summa symbolilla $\sigma(n)$. Toisessa luvussa esitellään myös täydellinen luku. Luvut voidaan jakaa täydellisiin, vajaisiin ja runsaisiin lukuihin tekijäfunktion avulla. Luku n on täydellinen, jos $\sigma(n) = 2n$. Jos $\sigma(n) < 2n$, niin luku n on vajaa, ja jos $\sigma(n) > 2n$, niin luku n on runsas. Luvussa esitellään myös monia muita ominaisuuksia, jotka saadaan käyttämällä tekijäfunktiota.

Kolmannessa luvussa käsitellään Mersennen ja Fermat'n lukuja. Mersennen alkuluvuksi sanotaan alkulukua, joka on muotoa $M_p = 2^p - 1$. Lucas-Lehmerin testillä voidaan helposti tutkia, onko jokin tietty Mersennen luku alkuluku. Fermat'n alkuluvuksi sanotaan alkulukua, joka on muotoa $2^{2^m} + 1$. Pepinin testillä taas voidaan tutkia, onko jokin Fermat'n luku alkuluku.

Neljännessä luvussa käsitellään tekijäfunktion sovelluksia. Luvussa todistetaan Dirichlet'n asymptoottinen kaava sekä funktiolle $d(n)$, että funktiolle $\sigma(n)$.

Sisältö

Johdanto

Tämä työ käsittelee tekijäfunktiota ja täydellisiä lukuja sekä niiden sovelluksia. Lukijan oletetaan tuntevan algebran peruskäsitteet sekä Tampereen Yliopiston lukuteorian kurssin. Sellaisia peruskäsitteitä on esitelty ensimmäisessä luvussa, jotka liittyvä läheisesti aiheeseen. Toisessa luvussa käsitellään tekijäfunktiota ja täydellisiä lukuja. Luvussa määritellään tekijäfunktio ja todistetaan, että se on multiplikatiivinen. Lisäksi luvussa esitellään tekijäfunktion ja täydellisen funktion ominaisuuksia, muun muassa miten luvut jaotellaan täydellisiin, vajaisiin ja runsaisiin lukuihin. Kolmas luku käsittää Mersennen ja Fermat'n luvut ja neljännessä luvussa esitellään joitakin tekijäfunktion sovelluksia. Aliluvussa 4.2 todistetaan Dirichlet'n asymptoottinen kaava tekijäfunktioiden $d(n)$ ja $\sigma_\alpha(n)$ osasummille.

Esimerkit ovat itse keksittyjä, ellei toisin mainita. Koska joitakin ominaisuuksia laskettaessa saadaa tulokseksi hyvin suuria lukuja ja lähdekirjallisuuksien esimerkeissä käytetään esimerkkeinä sellaisia laskuja, joista saadaan pieni numeroinen tulos, niin joitakin tämän työn esimerkkejä saataa esiintyä lähdekirjoissa. Todistukset ovat samoista lähteistä kuin lauseetkin, ellei toisin ole mainittu. Päälähdeteoksina on Tom M. Apostolin kirja Introduction to Analytic Number Theory, Kenneth H. Rosenin kirja Elementary Number Theory and Its Applications sekä MathWorld-internetsivustoa. Viitattaessa MathWorld-internetsivustoon viitteen perässä on hakusana, jolla ko. asia sivustolta löytyy.

1 Algebrallisia määritelmiä

1.1 Alkuluvut

1.1.1 Määritelmä

Määritelmä 1.1 ***Alkuluku*** *on positiivinen kokonaisluku ja* > 1*, joka on jaollinen ainoastaan ykkösellä ja itsellään.*

Esimerkki 1 *Luvut* $2, 3, 5, 7, 11, 13, 17, 19$ *ovat alkulukuja.*

Määritelmä 1.2 *Positiivista kokonaislukua, joka ei ole alkuluku, kutsutaan* ***yhdistetyksi luvuksi****.*

Lause 1.1 *Jokainen luku* n*,* $n > 1$*, on jaollinen alkuluvulla.* ([3], s.11)

Todistus. Tarkastellaan luvun n tekijöiden joukkoa. Joukon alkiot ovat suurempia kuin 1, mutta pienempiä kuin luku n itse. Joukko on joko tyhjä tai ei-tyhjä. Jos se on tyhjä, niin luku n on määritelmän mukaan alkuluku, sillä luvun n jakaa luku n itse. Jos joukko on ei-tyhjä, niin on olemassa pienin tekijä d. Jos luvulla d on tekijä, joka on suurempi kuin 1 ja pienempi kuin d, niin myös luvulla n on tämä tekijä. Tämä on mahdotonta, sillä d on pienin tekijä. Siis luku d on alkuluku ja luvulla n on alkulukutekijä, nimittäin luku d. □

Lause 1.2 *Jokainen luku* n*,* $n > 1$*, voidaan kirjoittaa alkulukujen tulona.* ([3], s.11)

Todistus. Edellisen lauseen mukaan tiedämme, että on olemassa sellainen alkuluku p_1, että $p_1|n$. Nyt siis $n = p_1 n_1$,missä $1 \leq n_1 < n$. Jos $n_1 = 1$, niin $n = p_1$ on kirjoitettu alkulukujen tulona. Jos $n_1 > 1$, niin edellisestä lauseesta saadaan, että on olemassa alkuluku, joka jakaa luvun n_1. Nyt $n_1 = p_2 n_2$, missä p_2 on alkuluku ja $1 \leq n_2 < n_1$. Jos $n_2 = 1$, niin $n = p_1 p_2$ on alkulukujen tulo. Mutta jos $n_2 > 1$, niin jälleen edellisen lauseen perusteella $n_2 = p_3 n_3$, missä p_3 on alkuluku ja $1 \leq n_3 < n_2$. Jos $n_3 = 1$, niin lause pätee, jos $n_3 > 1$, niin jatketaan kuten aiemmin. Ennen pitkään saadaan $n_i = 1$, jossa $n < n_1 < n_2 \ldots$ ja jokainen n_i on positiivinen luku, joten epäyhtälö ei voi jatkua loputtomiin. Jollakin luvulla k, on $n_k = 1$, missä tapauksessa $n = p_1 p_2 \cdots p_k$ ja luku n on kirjoitettu alkulukujen tulona. □

Esimerkki 2 *Luvut 6, 12, 110 ovat yhdistettyjä lukuja, sillä ne voidaan esittää alkulukujen tulona seuraavalla tavalla*

$$\begin{aligned} 2 \cdot 3 &= 6 \\ 4 \cdot 3 &= 2 \cdot 2 \cdot 3 = 12 \\ 55 \cdot 2 &= 2 \cdot 5 \cdot 11 = 110. \end{aligned}$$

1.1.2 Suurin yhteinen tekijä

Määritelmä 1.3 *Kahden luvun a ja b* ***suurin yhteinen tekijä*** *on suurin luku, joka jakaa sekä luvun a että luvun b. Suurinta yhteistä tekijää merkitään (a, b).*

Esimerkki 3 *Selvästi*

$$\begin{aligned} (12, 4) &= 4 \\ (36, 42) &= 6. \end{aligned}$$

Määritelmä 1.4 *Luvut a ja b ovat* ***suhteellisia alkulukuja****, jos lukujen a ja b suurin yhteinen tekijä on 1.* ([7], s.74)

Esimerkki 4 *Luvut* 99 *ja* 100 *ovat suhteellisia alkulukuja, sillä*

$$(99, 100) = 1.$$

1.1.3 Yksikkötekijä

Määritelmä 1.5 *Luku d on* ***yksikkötekijä*** *(engl. Unitary Divisor), jos luku d on luvun n tekijä ja luvun d ja luvun n/d suurin yhteinen tekijä on yksi. Toisin sanoen*

$$(d, n/d) = 1.$$

([9], Unitary Divisor)

Esimerkki 5 *Luvun* 20 *tekijät ovat* $\{1, 2, 4, 5, 10, 20\}$*. Nyt*

$$\begin{aligned} (1, 20) = (20, 1) &= 1 \\ (2, 10) = (10, 2) &= 2 \\ (4, 5) = (5, 4) &= 1, \end{aligned}$$

joten luvun 20 *yksikkötekijät ovat* $\{1, 4, 5, 20\}$*.*

Esimerkki 6 *Luvun* 110 *tekijät ovat* $\{1, 2, 5, 10, 11, 22, 55, 110\}$. *Koska*

$$(1, 110) = (110, 1) = 1,$$
$$(2, 55) = (55, 2) = 1,$$
$$(5, 22) = (22, 5) = 1,$$
$$(10, 11) = (11, 10) = 1,$$

niin kaikki luvun 110 *tekijät ovat myös sen yksikkötekijöitä.*

1.2 Aritmeettinen funktio

Määritelmä 1.6 ***Aritmeettinen funktio*** *on funktio, joka on reaali- tai kompleksiarvoinen ja jonka määrittelyjoukko on positiivisten kokonaislukujen joukko.*([1], s.24)

Esimerkki 7 *Olkoon* $\alpha \in \mathbb{R}$. *Symbolilla* N^α *merkitään sellaista aritmeettista funktiota, että* $N^\alpha(n) = n^\alpha$, *kun* $n \in \mathbb{Z}^+$. *Erityisesti merkitään* $N^1 = N$ *ja* $N^0 = \zeta$. *Siis* $N(n) = n$ *ja* $\zeta(n) = 1$, *kun* $n \in \mathbb{Z}^+$. ([5], s.27)

1.2.1 Dirichlet'n tulo

Määritelmä 1.7 *Jos funktiot* f *ja* g *ovat aritmeettisia funktioita, määritellään niiden* ***Dirichlet'n tulo (Dirichlet'n konvoluutio)*** *aritmeettisella funktiolla* h, *missä*

$$h(n) = \sum_{d|n} f(d)g(\frac{n}{d}).$$

Tulo voidaan kirjoittaa myös $h = f \star g$ *ja* $h(n) = (f \star g)(n)$. ([1], s.29)

Lause 1.3 *Dirichlet'n tulo on kommutatiivinen ja assosiatiivinen* ([1], s.29).

Todistus.
Todistetaan ensin kommutatiivisuus.
Funktio $f \star g$ voidaan kirjoittaa muodossa $(f \star g)(n) = \sum_{a \cdot b = n} f(a)g(b)$, missä a ja b käy läpi kaikki positiiviset kokonaisluvut, joiden tulo on n. Tästä seuraava kommutatiivisuus on itsestään selvää. Siis $f \star g = g \star f$ ja Dirichlet'n tulo on siis kommutatiivinen.

Todistetaan seuraavaksi assosiatiivisuus.
Olkoon $A = g \star k$. Nyt $f \star A = f \star (g \star k)$ ja voidaan kirjoittaa

$$\begin{aligned}(f \star A)(n) &= \sum_{a\cdot d=n} f(a)A(d) = \sum_{b\cdot c=n} f(a) \sum_{b\cdot c=d} g(b)k(c) \\ &= \sum_{a\cdot b\cdot c=n} f(a)g(b)k(c).\end{aligned}$$

Olkoon nyt $B = f \star g$. Nyt $B \star k = (f \star g) \star k$ ja voidaan kirjoittaa

$$\begin{aligned}(B \star k)(n) &= \sum_{d\cdot c=n} B(d)k(c) = \sum_{a\cdot b=d} f(a)g(b) \sum_{d\cdot c=n} k(c) \\ &= \sum_{a\cdot b\cdot c=n} f(a)g(b)k(c)\end{aligned}$$

Koska $f \star A = B \star k$, niin Dirichlet'n tulo on assosiatiivinen.

1.2.2 Funktion multiplikatiivisuus

Määritelmä 1.8 *Aritmeettista funktiota sanotaan **multiplikatiiviseksi**, jos*

$$f(1) = 1 \text{ ja } f(mn) = f(m)f(n), \text{ kun } (m, n) = 1.$$

*Multiplikatiivista funktiota sanotaan **täydellisesti multiplikatiiviseksi**, jos*

$$f(mn) = f(m)f(n), \text{ kaikilla positiivisilla luvuilla m ja n.}$$

([7], s.207)

Lause 1.4 *Jos funktiot f ja g ovat multiplikatiivisia, niin myös $f \star g$ on multiplikatiivinen.* ([1], s.35)

Todistus. Olkoon $h = f \star g$ ja luvut m ja n suhteellisia alkulukuja. Tällöin

$$h(mn) = \sum_{c|mn} f(c)g(\frac{mn}{c}).$$

Nyt jokainen luvun mn tekijä c voidaan kirjoittaa muodossa $c = ab$, missä $a|m$ ja $b|n$. Koska $(a, b) = 1$ ja $(\frac{m}{a}, \frac{n}{b}) = 1$, niin

$$\begin{aligned}h(mn) &= \sum_{a|m,b|n} f(ab)g(\frac{mn}{ab}) = \sum_{a|m,b|n} f(a)f(b)g(\frac{m}{a})g(\frac{n}{b}) \\ &= \sum_{a|m} g(\frac{m}{a}) \sum_{b|n} f(b)g(\frac{n}{b}) = h(m)h(n).\end{aligned}$$

□

Lause 1.5 *Olkoon funktio f multiplikatiivinen. Funktio f on täydellisesti multiplikatiivinen, jos ja vain jos*

$$f^{-1}(n) = \mu(n)f(n),$$

kaikilla $n \geq 1$. ([1], s.36)

Todistus. Olkoon $g(n) = \mu(n)f(n)$. Jos funktio f on täydellisesti multiplikatiivinen, niin

$$(g \star f)(n) = \sum_{d|n} \mu(d)f(d)f\Big(\frac{n}{d}\Big) = f(n)\sum_{d|n} \mu(d) = f(n)I(n) = I(n),$$

kun $f(1) = 1$ ja $I(n) = 0$, kun $n > 1$. Siis $g = f^{-1}$.
Oletetaan nyt, että $f^{-1}(n) = \mu(n)f(n)$. Todistaaksemme, että funktio f on täydellisesti multiplikatiivinen, riittää osoittaa, että $f(p^a) = f(p)^a$ kaikille alkulukupotensseille. Yhtälöstä $f^{-1}(n) = \mu(n)f(n)$ saadaan

$$\sum_{d|n} \mu(d)f(d)f\Big(\frac{n}{d}\Big) = 0, \text{ kaikille } n > 1.$$

Nyt valitsemalla $n = p^a$ saadaan

$$\mu(1)f(1)f(p^a) + \mu(p)f(p)f(p^{a-1}) = 0.$$

Koska $f(p^a) = f(p)(p^{a-1})$, niin $f(p^a) = f(p)^a$. Siis funktio f on täydellisesti multiplikatiivinen. □

Lause 1.6 *Jos f on multiplikatiivinen funktio, niin aritmeettinen funktio $F(n) = \sum_{d|n} f(d)$ on myös multiplikatiivinen.* ([7], s.218)

Todistus. Näyttääksemme, että funktio F on multiplikatiivinen täytyy todistaa, että jos luvut m ja n ovat suhteellisia alkulukuja, niin $F(mn) = F(m)F(n)$.
Oletetaan siis, että $(m, n) = 1$.
Saadaan

$$F(mn) = \sum_{d|m\cdot n} f(d).$$

Koska $(m, n) = 1$, jokainen luvun $m \cdot n$ tekijä voidaan kirjoittaa yksikäsitteisesti luvun m suhteellisten alkulukutekijöiden d_1 ja luvun n suhteellisten alkulukutekijöiden d_2 tulona. Jokainen luvun m tekijän d_1 ja luvun n tekijän d_2 pari vastaa luvun $m \cdot n$ tekijää $d = d_1 d_2$.
Nyt saadaan

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

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

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

□

1.3 Funktioita

1.3.1 Möbiuksen funktio

Määritelmä 1.9 ***Möbiuksen funktio*** $\mu(n)$ *määritellään seuraavasti: Kun* $\mu(1) = 1$ *ja jos* $n > 1$, $n = p_1^{a_1} \cdots p_k^{a_k}$, *missä* p *on alkuluku, niin*

$$\mu(n) = \begin{cases} (-1)^k & \text{jos } a_1 = a_2 = \cdots = a_k = 1. \\ 0 & \text{jos ja vain jos } a > 1. \end{cases}$$

([1], s.24)

Lause 1.7 *Jos* $n \geq 1$, *niin*

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{jos } n = 1. \\ 0 & \text{jos } n > 1. \end{cases}$$

([1], s.25)
Todistus.
Jos $n = 1$, lause on selvästi tosi.

Oletetaan, että $n > 1$ ja olkoon $n = p_1^{a_1} \cdots p_k^{a_k}$. Summassa $\sum_{d|n} \mu(d)$ on ainoastaan nollasta eroavia termejä, joten $d = 1$ ja nämä luvun n tekijät ovat eri alkulukuja. Siis

$$\begin{aligned}\sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \ldots + \mu(p_k) + \mu(p_1p_2) + \ldots + \mu(p_{k-1}p_k) \\ &+ \ldots + \mu(p_1p_2 \cdots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \ldots + \binom{k}{k}(-1)^k = (1-1)^k = 0.\end{aligned}$$

□

1.3.2 Eulerin funktio

Määritelmä 1.10 *Olkoon $n \geq 1$. **Eulerin funktio** $\phi(n)$ määritellään siten, että se on niiden positiivisten lukujen lukumäärä, jotka ovat pienempiä kuin luku n ja jotka ovat suhteellisia alkulukuja luvun n kanssa.* ([7], s.201)
Toisin sanoen

$$\phi(n) = |\{r : 1 \leq r \leq n, (r, n) = 1\}|, n \in \mathbb{Z}^+ \text{ ([5], s.4).}$$

Lause 1.8 *Olkoon p alkuluku ja $a \in \mathbb{Z}^+$. Tällöin $\phi(p^a) = p^a - p^{a-1}$.*
([3], s.66)

Todistus. Ne positiiviset luvut, jotka ovat pienempiä tai yhtäsuuria kuin p^a ja jotka eivät ole suhteellisia alkulukuja luvun p kanssa, ovat jaollisia luvulla p. Nämä luvut ovat muotoa kp, missä $1 \leq k \leq p^{a-1}$. Kun tällaisia lukuja on täsmälleen p^{a-1} kappaletta, on sellaisia lukuja, jotka ovat pienempiä kuin p^a ja suhteellisia luvun p^a kanssa, $p^a - p^{a-1}$ kappaletta. Joten $\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$. □

Esimerkki 8 *Selvästi*

$$\phi(1331) = 11^3 - 11^2 = 11^2(11-1) = 1210$$

ja

$$\phi(83521) = 17^4 - 17^3 = 17^3(17-1) = 78608.$$

Määritelmä 1.11 *Jos m on positiivinen luku, sanotaan, että luku a on luvun m* ***neliöjäännös****, jos $(a, m) = 1$ ja kongruenssilla $x^2 \equiv a \pmod{m}$ on ratkaisu. Jos kongruenssilla $x^2 \equiv a \pmod{m}$ ei ole ratkaisua, sanotaan, että luku a on luvun m* ***neliöepäjäännös****.* ([7], s.331)

Lause 1.9 ***Fermat'n pieni lause*** *Jos p on alkuluku ja a on positiivinen kokonaisluku siten, että luku p ei jaa lukua a, niin*

$$a^{p-1} \equiv 1 \pmod{p}.$$

([7], s.187)

Todistus. Kts. ([7], s.187)

Määritelmä 1.12 *Olkoon luvut a ja m suhteellisia alkulukuja. Pienin sellainen positiivinen kokonaisluku x, että $a^x \equiv 1 \pmod{m}$, on* ***a:n kertaluku modulo m****. Merkitään $ord_m a$.* ([7], s.278)

Esimerkki 9 *Etsitään $ord_{13}3$. Selvästi*

$$3^1 \equiv 3 \pmod{13}, \quad 3^2 \equiv 9 \pmod{13}, \quad 3^3 \equiv 1 \pmod{13}.$$

Siispä $ord_{13}3 = 3$.

Määritelmä 1.13 *Jos luvut r ja n ovat suhteellisia alkulukuja ja $n > 0$. Jos $ord_n r = \phi(n)$, niin lukua r sanotaan* ***primitiiviseksi juureksi modulo n****.*([7], s.280)

Lause 1.10 ***Eulerin kriteeri.***
Olkoon p pariton alkuluku ja $(a, p) = 1$. Luku a on luvun p neliöjäännös, jos ja vain jos $a^{(p-1)/2} \equiv 1 \pmod{p}$. ([2], s.181)

Todistus. Oletetaan, että lukun a on luvun p neliöjäännös siten, että kongruenssi $x^2 \equiv a \pmod{p}$ antaa ratkaisun x_1. Koska $(a, p) = 1$, niin $(x_1, p) = 1$. Voidaan siis käyttää Fermat'n pientä lausetta, jolloin saadaan

$$a^{(p-1)/2} \equiv (x_1^2)^{(p-1)/2} \equiv x_1^{p-1} \equiv 1 \pmod{p}.$$

Oletetaan nyt kongruenssi $a^{(p-1)/2} \equiv 1 \pmod{p}$ ja olkoon luku r luvun p

primitiivinen juuri. Nyt $a \equiv r^k \pmod{p}$, jollekin luvulle k, missä $1 \leq k \leq p-1$. Joten

$$r^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Nyt luvun r kertaluvun $p-1$ täytyy jakaa eksponentti $k(p-1)/2$. Tästä seuraa, että k on parillinen luku ja $k = 2j$. Siis

$$(r^j)^2 = r^{2j} = r^k \equiv a \pmod{p},$$

jolloin saadaan luku r^j kongruenssin $x^2 \equiv a \pmod{p}$ ratkaisuksi. Tämä todistaa, että luku a on alkuluvun p neliöjäännös. □

Seuraus 1 *Olkoon p pariton alkuluku ja $(a,p) = 1$. Luku a on luvun p neliöjäännös tai neliöepäjäännös, eli*

$$a^{(p-1)/2} \equiv 1 \pmod{p} \quad \textit{tai} \quad a^{(p-1)/2} \equiv -1 \pmod{p}.$$

([2], s.182)

Esimerkki 10 *Olkoon $p = 11$, jolloin*

$$3^{(11-1)/2} = 3^5 = 243 \equiv 1 \pmod{11}.$$

Siis luku 3 on luvun 11 neliöjäännös.

1.3.3 Möbiuksen ja Eulerin funktion välinen yhteys

Lause 1.11 *Jos $n \geq 1$, niin*

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

([1], s.26)

Todistus. Eulerin funktio voidaan kirjoittaa muodossa

$$\phi(n) = \sum_{k=1}^{n} \left[\frac{1}{(n,k)}\right].$$

Kun k käy läpi kaikki luvut välillä $1 \leq k \leq n$.
Käyttämällä lausetta 1.7 ja korvaamalla luku n luvulla (n, k) saadaan

$$\phi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{d|n, d|k} \mu(d).$$

Luvun n jakajaa d varten täytyy laskea summa kaikista luvuista k välillä $1 \leq k \leq n$, jotka ovat luvun d kerrannaisia. Kirjoitetaan $k = qd$, missä $1 \leq k < n$ jos ja vain jos $1 \leq q \leq \frac{n}{d}$. Voidaan siis kirjoittaa

$$\phi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Tämä todistaa lauseen. □

Eulerin funktio $\phi(n)$ voidaan kirjoittaa myös tulona.

Lause 1.12 *Jos $n \geq 1$, niin*

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

([1], s.27)

Todistus. Kun $n = 0$ tulo on nolla, sillä ei ole olemassa alkulukua, joka jakaisi luvun 1.
Olkoon $n > 1$ ja olkoot luvut $p_1, \ldots, p_r$ luvun n eri alkulukutekijöitä. Tulo voidaan siis kirjoittaa

$$\begin{aligned} \prod_{p|n} \left(1 - \frac{1}{p}\right) &= \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \\ &= 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \ldots + \frac{(-1)^r}{p_1 p_2 \cdots p_r} \quad (1) \end{aligned}$$

Yhtälön oikealla puolella termi $\sum \frac{1}{p_i p_j p_k}$ tarkoittaa kaikkia mahdollisia tuloja $p_i p_j p_k$ kun kerrotaan luvun n kolme eri alkulukutekijää kerrallaan. Oikealla puolella jokainen termi on muotoa $\pm\frac{1}{d}$, missä luku d jakaa luvun n, joka on joko 1 tai eri alkulukujen tulo. Luku ± 1 on Möbiuksen funktio $\mu(d)$.

Nyt $\mu(d) = 0$ jos d on jonkin alkuluvun p_i neliön jakaja. Nyt nähdään, että summa (1) on täysin sama kuin

$$\sum_{d|n} \frac{\mu(d)}{d}.$$

Tämä todistaa lauseen. □

Esimerkki 11 *Osoitetaan, että* $\phi(5186) = \phi(5187) = \phi(5188)$.
Ratkaisu.
Ratkaistaan tehtävä käyttämällä lausetta 1.12.
Selvästi

$$\begin{aligned}
\phi(5186) &= \phi(2 \cdot 2593) = 5186 \cdot (1 - \frac{1}{2})(1 - \frac{1}{2593}) = 2592 \\
\phi(5187) &= \phi(3 \cdot 7 \cdot 13 \cdot 19) = 5187 \cdot (1 - \frac{1}{3})(1 - \frac{1}{7})(1 - \frac{1}{13})(1 - \frac{1}{19}) = 2592 \\
\phi(5188) &= \phi(2^2 \cdot 1297) = 5188(1 - \frac{1}{2})(1 - \frac{1}{1297}) = 2592.
\end{aligned}$$

Siis $\phi(5186) = \phi(5187) = \phi(5188) = 2592$.

2 Tekijäfunktio ja täydelliset luvut

2.1 Tekijäfunktio

Määritelmä 2.1 *Olkoon* $\alpha \in \mathbb{R}$ *ja* $n \geq 1$. ***Tekijäfunktio***

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha$$

määritellään luvun n *tekijöiden* α*:nen potenssien summana.* ([1], s.38)

Funktiot σ_α ovat multiplikatiivisia, koska $\sigma_\alpha = \xi \star N^\alpha$, eli kahden multiplikatiivisen funktion Dirichlet'n tulo. (kts. lause 1.4)
Kun $\alpha = 0$, niin $\sigma_0(n)$ on luvun n tekijöiden lukumäärä ja merkitään $d(n)$.
Kun $\alpha = 1$, niin $\sigma_1(n)$ on luvun n tekijöiden summa ja merkitään $\sigma(n)$.

Koska σ_α on multiplikatiivinen, niin $\sigma_\alpha(p_1^{a_1} \cdots p_k^{a_k}) = \sigma_\alpha(p_1^{a_1}) \cdots \sigma_\alpha(p_k^{a_k})$. Nyt alkulukutulon p^a tekijät ovat $1, p, p^2, \ldots, p^a$, joten

$$\begin{aligned} \sigma_\alpha(p^\alpha) = 1^\alpha + p^\alpha + p^{2\alpha} + \ldots + p^{a\alpha} &= \tfrac{p^{\alpha(a+1)}-1}{p^\alpha - 1}, \quad \text{jos } \alpha \neq 0. \\ &= a + 1, \quad \text{jos } \alpha = 0. \end{aligned}$$

([1], s.38)

Määritelmä 2.2 ***Rajoitettu tekijäfunktio*** *(engl. Restricted Divisor Function) on luvun n aitojen tekijöiden summa*

$$s(n) \equiv \sigma(n) - n,$$

missä $\sigma(n)$ on tekijäfunktio. ([9], Restricted Divisor Function)

Tekijöiden summa $\sigma(N)$ voidaan esittää seuraavalla tavalla. Olkoon $N = ab$, missä $a \neq b$ ja $(a, b) = 1$. Nyt mille tahansa luvun n tekijälle d pätee $d = a_i b_i$, missä a_i on luvun a tekijä ja b_i on luvun b tekijä. Luvun a tekijät ovat $1, a_1, a_2, \ldots$ ja luvun b tekijät ovat $1, b_1, b_2, \ldots$. Tekijöiden summat ovat

$$\sigma(a) = 1 + a_1 + a_2 + \ldots + a,$$

$$\sigma(b) = 1 + b_a + b_2 + \ldots + b.$$

Nyt jollain tietyllä luvulla a_i

$$a_i(1 + b_1 + b_2 + \ldots + b) = a_i\sigma(b).$$

Nyt kun lasketaan kaikki luvut a_i yhteen, niin

$$(1 + a_1 + a_2 + \ldots + a)\sigma(b) = \sigma(a)\sigma(b),$$

joten $\sigma(N) = \sigma(ab) = \sigma(a)\sigma(b)$. Ja jakamalla luvut a ja b alkulukutekijöihin saadaan

$$\sigma(N) = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2}) \cdots \sigma(p_r^{\alpha_r}).([9], \text{Divisor Function})$$

Lause 2.1 *Olkoon p alkuluku ja α positiivinen luku. Tällöin*

$$\sigma(p^\alpha) = (1 + p + p^2 + \cdots + p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1} \tag{2}$$

ja

$$d(p^\alpha) = \alpha + 1.$$

([7], s.219)
Todistus. Luvun p^α tekijät ovat $1, p, p^2, \ldots, p^{\alpha-1}, p^a$. Koska luvulla p^α on täsmälleen $\alpha + 1$ kappaletta tekijöitä, niin $d(p^\alpha) = \alpha + 1$. Nyt $\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^{\alpha-1} + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}$. □

Tekijöiden summa $\sigma(N)$ voidaan nyt esittää muodossa

$$\sigma(N) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_1 - 1}.$$

Jos luku N on alkuluku voidaan yhtälö (2) kirjoittaa muotoon

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

Ja samalla tavalla, jos luku N on kakkosen potenssi, yhtälö (2) voidaan kirjoittaa

$$\sigma(2^\alpha) = \frac{2^{\alpha+1} - 1}{2 - 1} = 2^{\alpha+1} - 1.$$

([9], Divisor Function)

Lause 2.2 *Kaikilla $n \geq 1$ on*

$$\sigma_\alpha^{-1}(n) = \sum_{d|n} d^\alpha \mu(d)\mu(\frac{n}{d}).$$

([1], s.39)

Todistus. Koska $\sigma_\alpha = N^\alpha \star \xi$, niin (kts. [1], s.31) voidaan kirjoittaa

$$\sigma_\alpha^{-1} = (N^\alpha \star \xi)^{-1} = (N^\alpha)^{-1} \star \xi^{-1}.$$

Nyt koska Möbiuksen funktio μ on funktion ξ käänteisfunktio Dirichlet'n konvoluution suhteen ja N^α on täydellisesti multiplikatiivinen, niin lauseen 1.5 mukaan voidaan kirjoittaa

$$\sigma_\alpha^{-1} = (N^\alpha \star \xi)^{-1} = (N^\alpha)^{-1} \star \xi^{-1} = \mu N^\alpha \star \mu.$$

□

Esimerkki 12 *Lasketaan* $d(231)$, $\sigma(231)$, $d(4851)$, $\sigma(4851)$.
Ratkaisu.
Selvästi

$$\begin{aligned}
d(231) &= d(3\cdot 7\cdot 11) = d(3)d(7)d(11) = \textstyle\sum_{d|3} 1 \cdot \sum_{d|7} 1 \cdot \sum_{d|11} 1 \\
&= (1+1)(1+1)(1+1) = 2\cdot 2\cdot 2 = 8, \\
\sigma(231) &= \sigma(3\cdot 7\cdot 11) = \sigma(3)\sigma(7)\sigma(11) = \textstyle\sum_{d|3} d \cdot \sum_{d|7} d \cdot \sum_{d|11} d \\
&= (1+3)(1+7)(1+11) = 4\cdot 8\cdot 12\cdot = 384, \\
d(4851) &= d(3^2\cdot 7^2\cdot 11) = d(3^2)d(7^2)d(11) = \textstyle\sum_{d|9} 1 \sum_{d|49} 1 \sum_{d|11} 1 \\
&= (1+1+1)(1+1+1)(1+1)) = 3\cdot 3\cdot 2 = 18, \\
\sigma(4851) &= \sigma(3^2\cdot 7^2\cdot 11) = \sigma(3^2)\sigma(7^2)\sigma(11) = \textstyle\sum_{d|9} d \sum_{d|49} d \sum_{d|11} d \\
&= (1+3+9)(1+7+49)(1+11) = 13\cdot 57\cdot 12 = 8892.
\end{aligned}$$

Esimerkki 13 *Etsitään* $\sigma_3(4), \sigma_3(6), \sigma_3(12)$.
Ratkaisu.
Selvästi

$$\begin{aligned}
\sigma_3(4) &= \textstyle\sum_{d|4} d^3 = 1^3 + 2^3 + 4^3 = 73, \\
\sigma_3(6) &= \textstyle\sum_{d|6} d^3 = 1^3 + 2^3 + 3^3 + 6^3 = 252, \\
\sigma_3(12) &= \textstyle\sum_{d|12} d^3 = 1^3 + 2^3 + 3^3 + 4^3 + 6^3 + 12^3 = 2044.
\end{aligned}$$

Määritelmä 2.3 *Luvun n parittomien tekijöiden k:nnen potenssien summaa sanotaan* ***parittomaksi tekijäfunktioksi****. Pariton tekijäfunktio $\sigma_k^{(o)}(n)$ on kuten tekijäfunktio, mutta huomioon otetaan vain parittomat tekijät. Kun $k = 1$, niin*

$$\sigma_1^{(o)}(n) = \sigma_1(n) - 2\sigma_1(n/2),$$

missä $\sigma_k(n/2) = 0$, jos n on pariton. ([9], Odd Divisor Function)

Määritelmä 2.4 *Luvun parillisten tekijöiden potenssien summaa sanotaan* ***parilliseksi tekijäfunktioksi****. Parillinen tekijäfunktio $\sigma_k^{(e)}(n)$ on kuten tekijäfunktio, mutta huomioon otetaan vain parilliset tekijät. Parillinen tekijäfunktio ilmaistaan tekijäfunktion termeillä seuraavasti*

$$\sigma_k^{(e)}(n) = \begin{cases} 0 & \text{kun } n \text{ on pariton} \\ 2^k\sigma_k(n/2) & \text{kun } n \text{ on parillinen.} \end{cases}$$ ([9], Even Divisor Function)

n	$\sigma^{(o)}(n)$	$\sigma^{(e)}(n)$
1	1	0
2	1	2
3	4	0
4	1	6
5	6	0
6	4	8
7	8	0
8	1	14
9	13	0
10	6	12
11	12	0
12	4	24
13	14	0
14	8	16
15	24	0
16	1	30
17	18	0
18	13	26
19	20	0
20	6	36

Taulukko 1: Pariton ja parillinen tekijäfunktio, kun $1 \leq n \leq 20$.

Määritelmä 2.5 ***Yksikkötekijäfunktio*** *(engl. Unitary Divisor Funktion)* $\sigma_k^\star(n)$ *on tekijäfunktion* $\sigma_k(n)$ *vastine yksikkötekijöille ja tarkoittaa yksikkötekijöiden* k*:nen potenssien summaa. Kuten tavallinenkin tekijäfunktio, yksikkötekijäfunktio* $\sigma_1^\star(n)$ *kirjoitetaan usein* $\sigma^\star(n)$*.* ([9], Unitary Divisor Function)

Yksikkötekijöiden lukumäärä $\sigma_0^\star(n)$ on sama kuin luvun n neliövapaiden tekijöiden lukumäärä. Esimerkiksi 2^q, missä q on sellaisten alkulukujen lukumäärä, jotka jakavat luvun n.
Jos n on neliövapaa, niin $\sigma(n) = \sigma^\star(n)$.
Yksikkötekijäfunktio voidaan laskea käyttämällä yhtälöä

$$\sigma_k^\star(p_1^{\alpha_1}p^{\alpha_2}\cdots) = (1+p_1^{k\alpha_1})(1+p_2^{k\alpha_2})\cdots$$

([9], Unitary Divisor Function)

Esimerkki 14 *Lasketaan* $\sigma^\star(35)$, $\sigma_3^\star(15)$ *ja* $\sigma_7^\star(16)$.
Selvästi

$$\begin{aligned}\sigma^\star(35) &= \sigma^\star(5\cdot 7) = (1+5)(7+1) = 48,\\ \sigma_3^\star(15) &= \sigma_3^\star(3\cdot 5) = (1+3^3)(1+5^3) = 3528,\\ \sigma_7^\star(12) &= \sigma_7^\star(2^2\cdot 3) = (1+2^{7\cdot 2})(1+3^7) = 35850380.\end{aligned}$$

2.2 Täydelliset luvut

Määritelmä 2.6 *Jos* $n > 0$ *ja* $\sigma(n) = 2n$, *niin luku* n *on* ***täydellinen luku***. ([7], s.223)

Lause 2.3 *Positiivinen luku* n *on parillinen täydellinen luku, jos ja vain jos*

$$n = 2^{m-1}(2^m - 1),$$

kun $m \geq 2$ *ja* $2^m - 1$ *on alkuluku.* ([7], s.223)

Todistus. Todistetaan ensin, että jos $n = 2^{m-1}(2^m-1)$, missä 2^m-1 on alkuluku, niin luku n on täydellinen. Koska $2^m - 1$ on pariton, saadaan $(2^{m-1}, 2^m - 1) = 1$. Koska σ on multiplikatiivinen funktio, saadaan

$$\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1).$$

Lauseen 2.1 mukaan $\sigma(2^{m-1}) = 2^m - 1$ ja $\sigma(2^m - 1) = 2^m$. Oletuksen mukaan $2^m - 1$ on alkuluku. Joten

$$\sigma(n) = (2^m - 1)2^m = 2n$$

osoittaa, että n on täydellinen luku.
Olkoon nyt n parillinen täydellinen luku. Kirjoitetaan $n = 2^s t$, missä s ja t ovat positiivisia lukuja ja t on pariton. Koska $(2^s, t) = 1$, lauseesta 2.1 saadaan

$$\sigma(n) = \sigma(2^s t) = \sigma(2^s)\sigma(t) = (2^{s+1} - 1)\sigma(t). \tag{3}$$

Koska n on täydellinen, saadaan

$$\sigma(n) = 2n = 2^{s+1}t. \tag{4}$$

Yhdistämällä yhtälöt (3) ja (4) saadaan

$$(s^{s+1} - 1)\sigma(t) = 2^{s+1}t. \tag{5}$$

Koska $(2^{s+1}, 2^{s+1} - 1) = 1$, niin $2^{s+1}|\sigma(t)$. Joten on olemassa sellainen luku q, että $\sigma(t) = 2^{s+1}q$. Asettamalla tämä yhtälöön (5) saadaan

$$(2^{s+1} - 1)2^{s+1}q = 2\ s + 1t,$$

ja siten

$$(2^{s+1} - 1)q = t. \tag{6}$$

Näin ollen $q|t$ ja $q \neq t$.
Kun korvataan luku t yhtälön (6) vasemmalla puolella, saadaan

$$t + q = (2^{s+1} - 1)q + q = 2^{s+1}q = \sigma(t). \tag{7}$$

Näytetään, että $q = 1$.
Jos $q \neq 1$, niin on olemassa ainakin kolme eri positiivista luvun t tekijää, nimittäin 1, q ja t. Tästä seuraa, että $\sigma(t) \geq t + q + 1$, mikä on ristiriidassa yhtälön 7 kanssa. Näin ollen $q = 1$ ja yhtälöstä (6) nähdään että $t = 2^{s+1} - 1$. Ja yhtälöstä (7) nähdään, että $\sigma(t) = t + 1$, joten luvun t on oltava alkuluku ja sen ainoat positiiviset tekijät ovat 1 ja t. Täten $n = 2^s(2^{s+1} - 1)$, missä $2^{s+1} - 1$ on alkuluku. □

Lauseesta 2.3 nähdään, että löytääksemme täydellisen luvun on ensin löydettävä alkuluvut, jotka on muotoa $2^m - 1$. Löytääksemme tätä muotoa olevat alkuluvut, osoitamme, että eksponenttin m on oltava alkuluku.

Lause 2.4 *Jos m on positiivinen luku ja $2^m - 1$ on alkuluku, niin luvun m on oltava alkuluku.* ([7], s.224)

Todistus. Oletetaan, että m ei ole alkuluku, joten $m = ab$, missä $1 < a < m$ ja $1 < b < m$. Joten

$$2^m - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1).$$

Koska kummatkin tekijät yhtälön oikealla puolella ovat suurempia kuin yksi, nähdään, että $2^m - 1$ on yhdistetty luku, jos m ei ole alkuluku. Täten jos $2^m - 1$ on alkuluku, niin luvun m on myös oltava alkuluku. □

Esimerkki 15 *Osoitetaan, että* 8128 *on täydellinen luku.*
Ratkaisu.
Valitaan $m = 7$*, joka on alkuluku. Nyt* $2^m - 1 = 127$ *on myös alkuluku. Joten* $2^{(m-1)}2^m - 1 = 2^6 \cdot 127 = 8128$*. Siis* 8128 *on täydellinen luku.*

2.3 Tekijäfunktion ja täydellisen luvun sovelluksia

Määritelmä 2.7 *Luku* n *on positiivinen luku. Jos* $\sigma(n) < 2n$*, niin sanotaan että luku* n *on* ***vajaa*** *(engl. deficient). Jos* $\sigma(n) > 2n$*, niin luku* n *on* ***runsas*** *(engl. abundant). Jokainen luku on joko vajaa, täydellinen tai runsas.* ([7], s.230)

Esimerkki 16 *Etsitään kaksi vajaata ja kaksi runsasta lukua.*
Ratkaisu.
Selvästi

$$\begin{array}{rcll} \sigma(5) & = & \sum_{d|5} d = 1 + 5 = 6 \ < 2 \cdot 5 & \textit{vajaa} \\ \sigma(13) & = & \sum_{d|13} d = 1 + 13 = 14 \ < 2 \cdot 13 & \textit{vajaa} \\ \sigma(12) & = & \sum_{d|12} d = 1 + 2 + 3 + 4 + 6 + 12 = 28 \ > 2 \cdot 12 & \textit{runsas} \\ \sigma(20) & = & \sum_{d|20} d = 1 + 2 + 4 + 5 + 10 + 20 = 42 \ > 2 \cdot 20 & \textit{runsas} \end{array}$$

Määritelmä 2.8 *Kahta positiivista lukua* m *ja* n *sanotaan* ***sovinnolliseksi lukupariksi*** *(engl. Amicable Pair), jos* $\sigma(m) = \sigma(n) = m + n$*.* ([7], s.230)

Esimerkki 17 *Tutkitaan, ovatko luvut* 2620 *ja* 2924 *sovinnollinen lukupari.*
Ratkaisu.
Nyt

$$\begin{array}{rcl} \sigma(2620) = & \sum_{d|2620} d & \\ = & 1 + 2 + 4 + 5 + 10 + 20 + 131 + 262 + 524 + 655 + 1310 + 2620 & \\ = & 5544, & \\ \sigma(2924) = & \sum_{d|2924} d & \\ = & 1 + 2 + 4 + 17 + 34 + 43 + 68 + 86 + 172 + 731 + 1462 + 2924 & \\ = & 5544. & \end{array}$$

Luvut 2620 *ja* 2924 *ovat siis sovinnollinen lukupari.*

Esimerkki 18 *Luvut* 120 *ja* 190 *eivät ole sovinnollinen lukupari.*
Ratkaisu.
Nyt

$$\sigma(120) = \sigma(190) = 360,$$

mutta

$$120 + 190 = 310.$$

Summan olisi pitänyt olla 360*, jotta luvut olisivat olleet sovinnollinen lukupari.*

Määritelmä 2.9 *Kokonaislukua* n *sanotaan* ***k-täydelliseksi****, jos* $\sigma(n) = kn$*.* ([7], s.230)

Esimerkki 19 *Osoitetaan, että* $30240 = 2^5 \cdot 3^3 \cdot 5 \cdot 7$ *on* 4*-täydellinen.*
Selvästi

$$\sigma(30240) = \sigma(2^5)\sigma(3^3)\sigma(5)\sigma(7) = 63 \cdot 40 \cdot 6 \cdot 8 = 120960.$$

Koska $120960 = 4 \cdot 30240$*, luku* 30240 *on* 4*-täydellinen.*

Määritelmä 2.10 *Kokonaisluku* n *on* ***k-runsas****, jos* $\sigma(n) > kn$*.* ([7], s.231)

Esimerkki 20 *Etsitään* 3*-runsas kokonaisluku.*
Luku 240 *on* 3*-runsas, sillä*

$$\sigma(240) = 744 > 3 \cdot 240 = 720.$$

Määritelmä 2.11 *Olkoon*

$$\sum(n) \equiv \frac{\sigma(n)}{n},$$

missä $\sigma(n)$ *on tekijäfunktio. Lukupari* (k, m) *on* ***kaveripari*** *(engl. Friendly Pair) ja sanotaan, että luku* k *on luvun* m ***kaveri****, jos*

$$\sum(k) = \sum(m).$$

([9], Friendly Pair)

Esimerkki 21 *Tutkitaan, onko luku* 30 *luvun* 140 *kaveri.*
Ratkaisu.

$$\begin{aligned}
\sigma(30) &= \textstyle\sum_{d|30} d = 1 + 2 + 3 + 5 + 6 + 10 + 15 + 30 = 72, \\
\textstyle\sum(30) &= \frac{\sigma(30)}{30} = \frac{72}{30} = \frac{12}{5}, \\
\sigma(140) &= \textstyle\sum_{d|140} d \\
&= 1 + 2 + 4 + 5 + 7 + 10 + 14 + 20 + 28 + 35 + 70 + 140 = 336, \\
\textstyle\sum(140) &= \frac{\sigma(140)}{140} = \frac{336}{140} = \frac{12}{5}.
\end{aligned}$$

Nyt $\sum(30) = \sum(140)$*, joten luvut* 30 *ja* 140 *ovat kaveripari.* ([9], Friendly Pair)

Määritelmä 2.12 *Lukua, jolla ei ole kaveria, kutsutaan* ***yksinäiseksi*** *(engl. Solitary Number). Yksinäisiin lukuihin kuuluvat kaikki alkuluvut, alkulukujen potenssit ja luvut, joille* $(n, \sigma(n)) = 1$*, missä* (a, b) *on suurin yhteinen tekijä ja* $\sigma(n)$ *on tekijäfunktio.* ([9], Solitary Number)

Esimerkki 22 *Esimerkiksi luku* 23 *on yksinäinen, koska se on alkuluku. Myös luku* 25 *on yksinäinen, sillä*

$$\sigma(25) = 1 + 5 + 25 = 31 \text{ ja } (25, 31) = 1.$$

Määritelmä 2.13 *Positiivista lukua* n *kutsutaan* ***supertäydelliseksi****, jos* $\sigma(\sigma(n)) = 2n$*.* ([7], s.231)

Esimerkki 23 *Etsitään supertäydellinen luku.*
Ratkaisu.
Nyt

$$\begin{aligned} \sigma(2) &= 1 + 2 = 3, \\ \sigma(3) &= 1 + 3 = 4 = 2 \cdot 2. \end{aligned}$$

Koska $\sigma(\sigma(2)) = 2 \cdot 2$*, luku* 2 *on supertäydellinen.*

$$\begin{aligned} \sigma(4) &= 1 + 2 + 4 = 7, \\ \sigma(7) &= 1 + 7 = 8 = 2 \cdot 4. \end{aligned}$$

Koska $\sigma(\sigma(4)) = 2 \cdot 4$*, luku* 4 *on supertäydellinen.*

$$\begin{aligned} \sigma(13) &= 1 + 13 = 14, \\ \sigma(14) &= 1 + 2 + 7 + 14 = 24. \end{aligned}$$

Luku 13 *ei ole supertäydellinen.*

Määritelmä 2.14 *Lukua* n *sanotaan* ***k-hypertäydelliseksi*** *luvuksi, jos* $n = 1 + k\sum_i d_i = 1 + k[\sigma(n) - n - 1]$*, missä* $\sigma(n)$ *on tekijäfunktio ja tekijät ovat välillä* $1 < d_i < n$*. Kun järjestetään yhtälö uudelleen saadaan* $k\sigma(n) = (k + 1)n + k - 1$*.* ([9], k-hyperperfect Number)

Jos $k = 1$, saadaan tavallinen täydellinen luku. Jos $k > 1$ on pariton kokonaisluku, ja $p = \frac{(3k+1)}{2}$ ja $q = 3k + 4 = 2p + 3$ ovat alkulukuja, niin p^2q on k-hypertäydellinen. Samoin, jos p ja q ovat parittomia alkulukuja, niin että $k(p+q) = pq-1$ jollakin kokonaisluvulla k, niin $n = pq$ on k-hypertäydellinen. Lopuksi, jos $k > 0$ ja $p = k+1$ on alkuluku, niin jos $q = p^i - p+1$ on alkuluku jollakin $i > 1$, niin $n = p^{i-1}q$ on k-hypertäydellinen. ([9], k-hyperperfect Number)

Määritelmä 2.15 *Kokonaislukua n sanotaan* ***melkein täydelliseksi luvuksi*** *(engl. Almost Perfect Number), jos $\sigma(n) = 2n-1$.* ([9], Almost Perfect Number)

Ainoat tunnetut melkein täydelliset luvut ovat luvun 2 potenssit, nimittäin $1, 2, 4, 8, \ldots$. Ei kuitenkaan ole pystytty todistamaan, että luku on melkein täydellinen, jos ja vain jos luku on muotoa 2^m. ([9], Almost Perfect Number)

Määritelmä 2.16 ***Yksikkö sovinnollinen lukupari*** *(engl. Unitary Amicable Pair) on lukujen m ja n lukupari, jolle*

$$\sigma^\star(m) = \sigma^\star(n) = m + n,$$

missä $\sigma^\star(n)$ on yksikkötekijäfunktio. ([9], Unitary Amicable Pair)

Määritelmä 2.17 *Lukua n sanotaan* ***super yksikkö täydelliseksi luvuksi*** *(engl. Super Unitary Perfect Number), jos*

$$\sigma^\star(\sigma^\star(n)) = 2n,$$

missä $\sigma^\star$ on yksikkötekijäfunktio. ([9], Super Unitary Perfect Number)

Esimerkki 24 *Super yksikkö täydellisiä lukuja ovat muun muassa* $2, 9, 238, 4320, 10824, \ldots$ ([9], Super Unitary Perfect Number)

Ei tiedetä, onko olemassa muita parittomia super yksikkö täydellisiä lukuja kuin luku 9.

Määritelmä 2.18 *Olkoon*

$$s(n) \equiv \sigma(n) - n,$$

missä $\sigma(n)$ on tekijäfunktio ja $s(n)$ on rajoitettu tekijäfunktio. Lukujonoa

$$s^0(n) \equiv n, s^1(n) = s(n), s^2(n) = s(s(n)), \ldots$$

sanotaan ***alikvuotiksi lukujonoksi*** *(engl. Aliquot Sequence).*([9], Aliquot Sequence)

Jos lukujono on rajoitettu, se joko päättyy kun $s(1) = 0$ tai tulee jaksolliseksi.
Alikvuotilla lukujonolla on seuraavanlaisia ominaisuuksia:
1. Jos lukujono saavuttaa vakion, tämä vakio on täydellinen luku.
2. Jos lukujono saavuttaa vuorottelevan parin, tämä pari on ystävällinen lukupari.
3. Jos, k:n iteraatiokierroksen jälkeen, lukujono tuottaa syklin, jonka minimi pituus on t ja on muotoa $s^{k+1}(n), s^{k+1}, \ldots, s^{k+t}(n)$, nämä luvut muodostavat kertaluvun t **seurallisten lukujen** (engl. Sociable Number) ryhmän. ([9], Aliquot Sequence)

On löydetty seurallisten lukujen yleistys määrittelemällä se yleistämällä aito lukujono

$$a(n) = \frac{\sigma(a(n-1))}{m}.$$

Multitäydelliset luvut ovat kiinteissä pisteissä tässä kuvauksessa, sillä $a(n) = a(n-1)$, joten

$$ma(n) = \sigma(a(n)),$$

joka taas on m-multitäydellisen luvun määritelmä. Jos lukujono a(n) muuttuu sykliseksi termin $k > 1$ jälkeen, niin lukua sanotaan **k:nen kertaluvun 1/m-seuralliseksi luvuksi**

Jos luvut M_m ja M_n ovat erillisiä Mersennen alkulukuja, niin

$$\frac{1}{2}\sigma(2^{m-1}M_n) = \frac{1}{2}(2^m - 1)2^n = 2^{n-1}M_m$$

ja

$$\frac{1}{2}\sigma(2(n-1)M_m) = 2^{m-1}M_n,$$

joten $2^{m-1}M_n$ ja $2^{n-1}M_m$ ovat toisen kertaluvun 1/2-seurallisia lukuja. ([9], Sociable Number)

Mersennen alkulukuja käsitellään tarkemmin seuraavassa kappaleessa.

n	$\sigma(n)$	$d(n)$		
1	1	1	vajaa	
2	3	2	vajaa	supertäydellinen
3	4	2	vajaa	
4	7	3	vajaa	supertäydellinen
5	6	2	vajaa	
6	12	4	täydellinen	
7	8	2	vajaa	
8	15	4	vajaa	
9	13	3	vajaa	
10	18	4	vajaa	
11	12	2	vajaa	
12	28	6	runsas	
13	14	2	vajaa	
14	24	4	vajaa	
15	24	4	vajaa	
16	31	5	vajaa	supertäydellinen
17	18	2	vajaa	
18	39	6	runsas	
19	20	2	vajaa	
20	42	6	runsas	

Taulukko 2: Tekijöiden summat ja lukumäärät, kun $1 \leq n \leq 20$. Lisäksi luvut on luokiteltu täydellisiin, vajaisiin, runsaisiin ja supertäydellisiin.

3 Mersennen ja Fermat'n luvut

Edellisissä lauseissa on käsitelty vain parillisia täydellisiä lukuja. Kukaan ei tiedä eikä ole pystynyt todistamaan, että lauseet pätisivät myös parittomiin täydellisiin lukuihin. Tiedetään kuitenkin, että jos pariton täydellinen luku on olemassa, se on suuri luku, suurempi kuin 10^{38}. Esimerkiksi, jos $p_1, p_2, \ldots, p_k$ ovat parittoman täydellisen luvun alkulukutekijöitä, niin $1/p_1 + 1/p_2 + \cdots + 1/p_k > (150/151) \ln 2$.

3.1 Mersennen alkuluku

Määritelmä 3.1 *Jos m on positiivinen luku, niin luku $M_m = 2^m - 1$ on **m:s Mersennen luku**. Jos p on alkuluku, niin alkulukuja, jotka ovat muotoa $M_p = 2^p - 1$ sanotaan **Mersennen alkuluvuiksi**.* ([7], s.225)

Esimerkki 25 *Etsitään kaksi Mersennen alkulukua ja kaksi Mersennen lukua.*
Ratkaisu.

$$\begin{array}{lcll} M_3 = 2^3 - 1 = 7 & \Rightarrow & M_3 = 7 & \textit{Mersennen alkuluku} \\ M_5 = 2^5 - 1 = 31 & \Rightarrow & M_5 = 31 & \textit{Mersennen alkuluku} \\ M_4 = 2^4 - 1 = 15 & \Rightarrow & M_4 = 3 \cdot 5 = 15 & \textit{4:s Mersennen luku} \\ M_6 = 2^6 - 1 = 63 & \Rightarrow & M_6 = 3 \cdot 21 = 63 & \textit{6:s Mersennen luku} \end{array}$$

On olemassa monia lauseita, jolla voidaan todeta onko jokin Mersennen luku alkuluku. Seuraavaksi esitetään yksi.

Lause 3.1 *Jos p on pariton alkuluku, niin mikä tahansa Mersennen luvun $m_p = 2^p + 1$ tekijä on muodossa $2kp + 1$, missä k on positiivinen luku.* ([7], s.225)

Todistus. Olkoon q alkuluku, joka on luvun $m_p = 2^p - 1$ tekijä. Fermat'n pienen lauseen mukaan tiedetään että $q|(2^{q-1} - 1)$. Lisäksi tiedetään, että

$$(2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)} - 1. \tag{8}$$

Koska luku q on lukujen $2^p - 1$ ja $2^{q-1} - 1$ yhteinen tekijä, niin $(2^p - 1, 2^{q-1} - 1) > 1$. Joten $(p, q-1) = p$, sillä toinen mahdollisuus, $(p, q-1) = 1$, antaisi yhtälöstä (8) tuloksen $(2^p - 1, 2^{q-1} - 1) = 1$. Niinpä $p|(q-1)$ ja täten $q - 1 = mp$, missä m on positiivinen luku. Koska q on pariton, niin luvun m on oltava parillinen , jotta $m = 2k$, missä k on positiivinen luku. Siispä $q = mp + 1 = 2kp + 1$. □

Esimerkki 26 *Tutkitaan, onko $M_{11} = 2^{11} - 1 = 2047$ alkuluku.*
Ratkaisu.
Tarvitsee käydä läpi ainoastaan sellaiset alkulukutekijät, jotka ovat pienempiä kuin $\sqrt{2047} = 45,243\ldots$ Lauseen 3.1 mukaan alkulukutekijä on muotoa $22k+1$. Siis ainoa mahdollinen on 23. Koska $23 \cdot 89 = 2047$, M_{11} on yhdistetty luku.

Esimerkki 27 *Tutkitaan, onko* $M_{19} = 2^{19} - 1 = 524287$ *alkuluku.*
Ratkaisu.
Tarvitsee siis käydä läpi sellaiset alkulukutekijät,jotka ovat pienempiä kuin $\sqrt{524287} = 724,0766\ldots$ *Lauseen 3.1 mukaan alkulukutekijä on muotoa* $38k+1$*. Siis mahdolliset tekijät ovat* $191, 229, 419, 457, 571$ *ja* 647*. Mikään näistä alkuluvuista ei kuitenkaan jaa lukua* 524287*, joten* M_{19} *on alkuluku.*

Lause 3.2 ***Lucas-Lehmerin testi.*** *Olkoon* p *alkuluku ja* $M_p = 2^p - 1$ *Mersennen p:s luku. Asetetaan* $r_1 = 4$ *ja* $k \geq 2$*, jolloin*

$$r_k \equiv r_{k-1}^2 - 2 \pmod{M_p},\ 0 \leq r_k < M_p.$$

M_p *on alkuluku jos ja vain jos* $r_{p-1} \equiv 0 \pmod{M_p}$*.* ([7], s.226-227)

Todistus. Sivuutetaan.

Esimerkki 28 *Tutkitaan, onko* $M_7 = 2^7 - 1 = 127$ *alkuluku.*
Ratkaisu.
Nyt lauseen 3.2 mukaan $r_1 = 4$*,* $k \geq 2$ *ja* $0 \leq r_k < M_p$*.*

$$\begin{aligned}
r_2 &\equiv 4^2 - 2 = 14 \pmod{127},\\
r_3 &\equiv 14^2 - 2 \equiv 67 \pmod{127},\\
r_4 &\equiv 67^2 - 2 \equiv 42 \pmod{127},\\
r_5 &\equiv 42^2 - 2 \equiv 111 \pmod{127},\\
r_6 &\equiv 111^2 - 2 \equiv 0 \pmod{127}.
\end{aligned}$$

Siis $M_7 = 127$ *on alkuluku.*

Määritelmä 3.2 ***Mersennen kaksoisluku****(engl. Double Mersenne Number) on luku, joka on muotoa*

$$M_{M_n} = 2^{2^n - 1} - 1,$$

missä M_n *on Mersennen luku. Mersennen kaksoisluku, joka on alkuluku, on* ***Mersennen kaksoisalkuluku****.* ([9], Double Mersenne Number)

Koska Mersennen alkuluku M_n voi olla alkuluku vain, jos n on alkuluku, niin Mersennen kaksoisalkuluku voi olla alkuluku vain, jos M_n on alkuluku, toisin sanoen, jos M_n on Mersennen alkuluku.

3.1.1 Rationaalinen sovinnollinen lukupari

Määritelmä 3.3 ***Rationaalinen sovinnollinen lukupari*** *(engl. Rational Amicable Pair) sisältää kaksi kokonaislukua a ja b, joiden tekijäfunktiot ovat yhtäsuuret ja on muotoa*

$$\sigma(a) = \sigma(b) = \frac{P(a,b)}{Q(a,b)} = R(a,b), \tag{9}$$

missä $P(a,b)$ ja $Q(a,b)$ ovat kahden muuttujan polynomeja ja joille pätee seuraavat ominaisuudet.

1. Kaikkien termien asteet oikeanpuoleisen osamäärän osoittajassa ovat samat.
2. Kaikkien termien asteet oikeanpuoleisen osamäärän nimittäjässä ovat samat.
3. Polynomin P aste on yhden suurempi kuin polynomin Q. ([9], Rational Amicable Pair)

Jos $a = b$ ja polynomi $P(a,b)$ on muotoa ma^r, niin yhtälö (9) tuottaa erikoistapauksen

$$\sigma(a) = \frac{m}{n}a,$$

joten jos $\frac{m}{n}$ on kokonaisluku, niin luku a on multitäydellinen luku.

Olkoon polynomi muodossa

$$R_n(a,b) = \frac{(a+b)^n}{a^{n-1}+b^{n-1}}. \tag{10}$$

Kun $n = 1$, yhtälö (10) tuottaa

$$\sigma(a) = \sigma(b) = 1/2(a+b),$$

josta ei tiedetä olevan esimerkkejä.
Kun $n = 2$, yhtälö (10) tuottaa

$$\sigma(a) = \sigma(b) = \frac{(a+b)^2}{(a+b)} = a+b,$$

joten (a,b) on sovinnollinen lukupari.
Kun $n = 3$, yhtälö (10) tuottaa

$$\sigma(a) = \sigma(b) = \frac{(a+b)^3}{a^2+b^2}.$$

Tästä on löydetty kolmea erityyppistä ratkaisujoukkoa.
Ensimmäinen ratkaisujoukko on muotoa

$$2^{m-1}M_m \cdot 3 \cdot 5^2 \cdot 13 \cdot 31 \cdot 139 \cdot 277 \cdot 3877 \left[\begin{array}{c} 11 \cdot 19 \\ 239 \end{array} \right],$$

missä M_m on Mersennen alkuluku, ja $m \neq 2 \neq 5$.
Toinen ratkaisujoukko on muotoa

$$2^{m-1}M_m \cdot 3 \cdot 7 \cdot 11^2 \cdot 17^2 \cdot 19^2 \cdot 23 \cdot 127 \cdot 307 \cdot 359 \cdot 3739 \cdot 22433 \cdot 68209 \left[\begin{array}{c} 83 \cdot 1931 \\ 162287 \end{array} \right],$$

missä $m \neq 2 \neq 3 \neq 7$.
Kolmas tyyppi on yksikäsitteinen ratkaisu

$$2^{11} \cdot 3^7 \cdot 13 \cdot 17 \cdot 19^2 \cdot 23 \cdot 41 \cdot 127 \cdot 227 \cdot 271 \cdot 541 \cdot 2269 \cdot 124429 \left[\begin{array}{c} 29 \cdot 569 \\ 17099 \end{array} \right].$$

Ajattellaan polynomit yleisemmässä muodossa

$$R_{k,n}(a,b) = \frac{(a+b)^n}{k(a^{n-1}+b^{n-1})}.$$

Kun $(k,n) = (2,4)$, on löydetty ratkaisu

$$2^{m-1}M_m \cdot 3 \cdot 5 \cdot 7 \cdot 23^2 \cdot 59 \cdot 79 \cdot 137 \cdot 547 \cdot 2477 \cdot 158527 \cdot$$

$$173428537 \cdot 8671426849 \left[\begin{array}{c} 83 \cdot 1931 \\ 162287 \end{array} \right],$$

missä m on Mersennen alkuluvun indeksi lukuunottamatta kun $m = 2$ ja $m = 3$.
Ajatellaan polynomit nyt muodossa

$$R_{r/s}(a,b) = \frac{r}{s}\frac{(a+b)^3}{a^2+ab+b^2}.$$

Kun $r/s = 3/2$, niin on löydetty ratkaisu

$$2^8 \cdot 3^2 \cdot 13 \cdot 17 \cdot 41 \cdot 53 \cdot 73^2 \cdot 1801 \cdot 11971 \left[\begin{array}{c} 5 \cdot 11 \\ 71 \end{array} \right].$$

Polynomit voidaan ajatella myös muodossa

$$R_k(a,b) = \frac{kab}{a+b}$$

tai vastaavasti muodossa

$$\frac{1}{\sigma(a)} = \frac{1}{\sigma(b)} = \frac{1}{a} + \frac{1}{b}. \text{ ([9], Rational Amicable Pair)}$$

3.2 Fermat'n luku

Määritelmä 3.4 *Jos n on positiivinen kokonaisluku, niin **Fermat'n luvuksi** sanotaan lukua F_n, joka on muotoa*

$$2^{2^n} + 1.$$

([2], s.226)

Määritelmä 3.5 *Fermat'n lukua $F_n = 2^{2^n} + 1$, joka on alkuluku, sanotaan **Fermat'n alkuluvuksi**.* ([2], s.226)

Esimerkki 29 *Fermat'n lukuja ovat esimerkiksi*

$$\begin{aligned} F_0 &= 2^{2^0} + 1 = 3, \\ F_1 &= 2^{2^1} + 1 = 5, \\ F_2 &= 2^{2^2} + 1 = 17, \\ F_3 &= 2^{2^3} + 1 = 257, \\ F_4 &= 2^{2^4} + 1 = 65537, \\ F_5 &= 2^{2^5} + 1 = 4294967297. \end{aligned}$$

Lause 3.3 *Numeroiden lukumäärä Fermat'n luvussa voidaan laskea kaavalla*

$$\begin{aligned} D(n) &= \lfloor [\log(2^{2^n} + 1)] + 1 \rfloor \\ &\approx \lfloor \log(2^{2^n} + 1) \rfloor \\ &= \lfloor 2^n \log 2 + 1 \rfloor. \text{([9], Fermat Number)} \end{aligned}$$

Todistus. Sivuutetaan.

Esimerkki 30 *Edellisessä esimerkissä lasketun kuuden ensimmäisen Fermat'n luvun numeroiden lukumäärä on*

$$\begin{aligned} D(0) &= \lfloor 2^0 \log 2 + 1 \rfloor = 1, \\ D(1) &= \lfloor 2^1 \log 2 + 1 \rfloor = 1, \\ D(2) &= \lfloor 2^2 \log 2 + 1 \rfloor = 2, \\ D(3) &= \lfloor 2^3 \log 2 + 1 \rfloor = 3, \\ D(4) &= \lfloor 2^4 \log 2 + 1 \rfloor = 5, \\ D(5) &= \lfloor 2^5 \log 2 + 1 \rfloor = 10. \end{aligned}$$

Seuraavien viiden Fermat'n luvun numeroiden lukumäärä on

$$\begin{aligned} D(6) &= \lfloor 2^6 \log 2 + 1 \rfloor = 20, \\ D(7) &= \lfloor 2^7 \log 2 + 1 \rfloor = 39, \\ D(8) &= \lfloor 2^8 \log 2 + 1 \rfloor = 78, \\ D(9) &= \lfloor 2^9 \log 2 + 1 \rfloor = 155, \\ D(10) &= \lfloor 2^{10} \log 2 + 1 \rfloor = 309. \end{aligned}$$

Lause 3.4 *Jos k, a ja b ovat positiivisia kokonaislukuja, siten että $k = ab$, missä luku a on pariton, niin $2^b + 1 | 2^k + 1$. Erityisesti, jos $2^k + 1$ on alkuluku, niin luku k on 0 tai luvun 2 potenssi.* ([8], s.98)

Todistus. Osoitetaan $2^k + 1 \equiv 0 \pmod{2^b + 1}$ eli $2^k \equiv -1 \pmod{2^b + 1}$. Nyt $2^b \equiv -1 \pmod{2^b + 1}$, joten

$$2^k = 2^{ab} = (2^b)^a \equiv (-1)^a \equiv -1 \pmod{2^b + 1},$$

missä ensimmäinen kongruenssi seuraa lauseesta 1.21 (kts.[8], s. 39). Toinen kongruenssi seuraa siitä, että luku a on pariton. Jos $k > 0$ ei ole luvun 2 potenssi, niin valitaan $a > 1$. Joten

$$1 < 2^b + 1 < 2^k + 1,$$

ja täten luvulla $2^k + 1$ on jokin muu positiivinen tekijä kuin luku 1 tai luku itse. □

Määritelmä 3.6 *Olkoon luku p pariton alkuluku ja $(a,p)=1$.* ***Legendren symboli*** *määritellään seuraavasti.*

$$(a/p) = \begin{cases} 1 & \textit{jos } a \textit{ on luvun } p \textit{ neliöjäännös} \\ -1 & \textit{jos } a \textit{ on luvun } p \textit{ neliöepäjäännös.} \end{cases}$$

([2], s.185)

Lause 3.5 ***Pepinin testi***
Jos $n > 0$, niin Fermat'n luku $F_n = 2^{2^n}+1$ on alkuluku jos ja vain jos

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}. \tag{11}$$

([2], s.228)

Todistus. Oletetaan ensin, että $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Jos luku p on mikä tahansa alkuluku, joka jakaa luvun F_n, niin saadaan

$$3^{(F_n+1)/2} \equiv -1 \pmod{p},$$

koska jos $a \equiv b \pmod{m}$ ja $d|m$, niin $a \equiv b \pmod{d}$. Neliöimällä nyt yhtälö saadaan

$$3^{F_n+1} \equiv 1 \pmod{p}.$$

Olkoon k luvun 3 *modulo* p kertaluku. Nyt luku k jakaa luvun $F_n - 1 = 2^{2^n}$. Joten $k = 2^t$, jollakin luvulla $t \leq 2^n$. Oletetaan, että $t < 2^n$. Nyt kongruenssin $3^k \equiv 1 \pmod{p}$ molemmat puolet voidaan korottaa potenssiin $2^{2^n-t-1} \geq 1$ ja saadaan

$$1 \equiv (3^k)^{2^{2^n-t-1}} = 3^{2^t(2^{2^n}-t-1)} = 3^{2^{2^n}-1} = 3^{2^{2^n}/2} = 3^{(F_n-1)/2} \equiv -1 \pmod{p}.$$

Mutta tämä tarkoittaa että $p = 2$, mikä on mahdotonta.
Täytyy siis olla $t = 2^n$ ja $k = 2^{2^n} = F_n - 1$. Nyt Fermat'n pienen lauseen mukaan $k \leq p-1$. Siis $p \geq k+1 = F_n$. Koska luku p on luvun F_n tekijä, niin on oltava $p = F_n$. Joten luku F_n on alkuluku.

Oletetaan, että F_n on alkuluku. Nyt $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, jos ja vain jos luku 3 ei ole neliö *modulo* F_n. Käyttämällä resiprookkilakia (engl. Quadratic Reciprocity) (kts.[2], s.196) voidaan osoittaa, että luku 3 ei ole minkään luvun neliö *modulo* F_n. Olkoon $(a/b)_2$ neliön symboli. Kun $n \geq 1$, niin

$$\begin{aligned} (3/F_n)_2 &= (F_n/3)_2 \quad (\text{silloin kun } F_n = 1 \pmod 4, n \geq 1) \\ &= (((-1)^{2^n}+1)/3)_2 = (2/3)_2 = -1. \end{aligned}$$

Siis luku 3 ei ole neliö *modulo* F_n, sillä käyttämällä Eulerin kriteeriä saadaan

$$3^{(F_n-1)/2} \equiv -1(mod\ F_n).$$

Näin ollen kongruenssi pitää paikkansa. □

Esimerkki 31 *Osoitetaan Pepinin testillä, että* $F_4 = 65537$ *on alkuluku. Nyt*

$$\begin{aligned} 3^{(F_4-1)/2} &= 3^{32768} = 3^{(2^{15})} \\ &\vdots \\ &\equiv 79524^{(2^6)} \pmod{65537} \\ &\vdots \\ &\equiv 64^{(2^3)} \pmod{65537} \\ &\vdots \\ &\equiv 65536 \pmod{65537} \\ &\equiv -1 \pmod{65537}. \end{aligned}$$

Siis $F_4 = 65537$ *on alkuluku.*

Lause 3.6 *Mikä tahansa Fermat'n luvun* $F_n = 2^{2^n} + 1$ *alkulukutekijä* p *on muotoa* $p = k \cdot 2^{n+2} + 1$*, missä* $n \geq 2$*.* ([2], s.230)

Todistus. Luvun F_n alkulukutekijälle p pätee

$$2^{2^n} \equiv -1 \pmod{p},$$

josta saadaan

$$2^{2^{n+1}} \equiv 1 \pmod{p}.$$

Jos luku h on luvun 2 kertaluku *modulo* p kongruenssista saadaan

$$h|2^{n+1}.$$

Nyt $h = 2^r$, missä $1 \leq r \leq n$ ja tästä saadaan

$$2^{2^n} \equiv 1 \pmod{p}.$$

Ja kääntäen tämä johtaa siihen että $p = 2$, mikä on ristiriita. Voidaan siis olettaa, että $h = 2^{n+1}$. Koska luvun 2 kertaluku *modulo* p jakaa luvun $\phi(p) =$

$p-1$, voidaan päätellä, että $2^{n+1}|p-1$. Ja näin saadaan $p \equiv 1 \pmod 8$, kun $n \geq 2$ ja käyttämällä Legendren symbolia, saadaan $(2/p) = 1$. Käyttämällä Eulerin kriteeriä saadaan

$$2^{(p-1)/2} \equiv (2/p) = 1 \pmod p.$$

Lauseen 8.1 (kts. [2], s.158) mukaan $h|(p-1)/2$ tai $2^{n+1}|(p-1)/2$. Tästä saadaan $2^{n+1}|p-1$ ja näin ollen $p = k \cdot 2^{n+2} + 1$ jollakin luvulla k. Tämä päättää todistuksen. □

4 Aritmeettisten funktioiden keskiarvo

Tässä kappaleessa tarkastellaan aritmeettisten funktioiden käyttäytymistä suurilla luvun n arvoilla. Esimerkiksi funktio $d(n)$ saa erittäin suuren arvon, kun luvulla n on paljon tekijöitä. Usein on kuitenkin vaikea päätellä miten aritmeettiset funktiot käyttäytyvät suurilla luvun n arvoilla. Tässä kappaleessa todistetaan tekijäfunktiolle tulos, jonka Dirichlet näytti vuonna 1849, nimittäin

$$\sum_{k \leq x} d(k) = x \log x + (2C-1)x + O(\sqrt{x}) \tag{12}$$

kaikille $x \geq 1$. Tässä C on Eulerin vakio, joka määritellään

$$C = \lim_{n \to \infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n \right). \tag{13}$$

4.1 Määritelmiä ja aputuloksia

4.1.1 Iso O-notaatio ja funktioiden asymptoottinen yhtäsuuruus

Määritelmä 4.1 *Jos $g(x) > 0$ kaikilla $x \geq a$, voidaan kirjoittaa*

$$f(x) = O(g(x))$$

tarkoittamaan, että osamäärä $f(x)/g(x)$ on rajoitettu kun $x \geq a$. Toisin sanoen on olemassa sellainen $M > 0$, että

$$|f(x)| \leq Mg(x) \text{ kaikilla } x \geq a.$$

([1], s.53)

Yhtälö, joka on muotoa

$$f(x) = h(x) + O(g(x)),$$

tarkoittaa, että $f(x) - h(x) = O(g(x))$. Huomattaan, että $f(t) = O(g(t))$, kun $t \geq a$, josta saadaan $\int_a^x f(t)dt = O(\int_a^x g(t)dt)$, kun $x \geq a$. ([1], s.53)

Määritelmä 4.2 *Jos*

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1,$$

sanotaan, että funktiot $f(x)$ ja $g(x)$ ovat asymptoottisesti yhtäsuuret, kun $x \to \infty$ ja tällöin kirjoittetaan

$$f(x) \sim g(x) \text{ kun } x \to \infty.$$

([1], s.53)

Esimerkiksi, yhtälöstä (12) saadaan

$$\sum_{k\leq x} d(k) \sim x \log x, \text{ kun } x \to \infty.$$

Yhtälön (12) termiä $x \log x$ sanotaan **summan asymptoottiseksi arvoksi**; kaksi muuta termiä kertoo virheen, joka tehdään kun arvioidaan summaa sen asymptoottisella arvolla. Kun merkitään virhettä symbolilla $E(x)$, niin yhtälöstä (12) saadaan

$$E(x) = (2C - 1)x + O(\sqrt{x}). \tag{14}$$

Tämä voidaan myös kirjoittaa muodossa $E(x) = O(x)$. Tämä merkintä ei kuitenkaan anna tarkempaa tietoa yhtälöstä (14). Yhtälöstä (14) nimittäin nähdään, että sen aymptoottinen arvo on $(2C - 1)x$.([1], s.54)

4.1.2 Eulerin summakaava

Joskus osittaissumman asymptoottinen arvo voidaan löytää vertaamalla sitä integraaliin. **Eulerin summakaava** antaa tarkan lausekkeen virheelle, joka tehdään aproksimaatiossa. Tässä kaavassa $[t]$ tarkoittaa suurinta kokonaislukua, joka on $\leq t$.

Lause 4.1 ***Eulerin summakaava.*** *Jos funktio f on jatkuva ja derivoituva välillä $[y,x]$, missä $0<y<x$, niin*

$$\sum_{y<n\leq x} f(x) = \int_y^x f(t)dt + \int_y^x (t-[t])f'(t)dt + f(x)([x]-x) - f(y)([y]-y). \quad (15)$$

([1], s.54)

Todistus. Olkoon $m=[y]$ ja $k=[x]$. Luvuille n ja $n-1$ välillä $[y,x]$ pätee

$$\begin{aligned} \int_{n-1}^{n}[t]f'(t)dt &= \int_{n-1}^{n}(n-1)f'(t)dt = (n-1)f(x) - f(n-1) \\ &= nf(n) - (n-1)f(n-1) - f(x). \end{aligned}$$

Kun merkitään $n=m+1$ ja $n=k$ saadaan

$$\begin{aligned} \int_m^k [t]f'(t)dt &= \int_{n=m+1}^{k} nf(x) - (n-1)f(n-1) - \sum_{y<n\leq x} f(x) \\ &= kf(k) - mf(m) - \sum_{y<n\leq x} f(n), \end{aligned}$$

joten

$$\begin{aligned} \sum_{y<n\leq x} f(x) &= -\int_m^k [t]f'(t)dt + kf(k) - mf(m) \\ &= -\int_y^x [t]f'(t)dt + kf(x) - mf(y). \end{aligned} \quad (16)$$

Integrointi osittain antaa yhtälön

$$\int_y^x f(t)dt = xf(x) - yf(y) - \int_y^x tf'(t)dt.$$

Kun tämä yhdistetään yhtälöön (16), saadaan yhtälö (15). □

4.1.3 Alkeellisia asymptoottisia kaavoja

Seuraavan kaavan (a)-kohdassa vakio C on Eulerin vakio, joka määriteltiin yhtälössä (14). Kohdassa (b) $\xi(s)$ tarkoittaa Riemannin zeta-funkiota ,joka määritellään yhtälöllä

$$\xi(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \text{ jos } s>1,$$

ja yhtälöllä

$$\xi(s) = \lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right) \text{ jos } 0 < s < 1.$$

Lause 4.2 *Jos $x \ge 1$, saadaan*

$$\begin{array}{llll}
(a) & \sum_{n\le x}\frac{1}{n} & = & \log x + C + O\left(\frac{1}{x}\right), \\
(b) & \sum_{n\le x}\frac{1}{n^s} & = & \frac{x^{1-s}}{1-s} + \xi(s) + O(x^{-s}) \quad \textit{jos } s > 0, s \ne 1, \\
(c) & \sum_{n>x}\frac{1}{n^s} & = & O(x^{1-s}) \quad \textit{jos } s > 1, \\
(d) & \sum_{n\le x} n^\alpha & = & \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha) \quad \textit{jos } \alpha \ge 0.
\end{array}$$

([1], s.55)

Todistus. Kohdassa (a) asetetaan $f(t) = 1/t$ Eulerin summakaavaan ja saadaan

$$\begin{array}{rcl}
\sum_{n\le x}\frac{1}{n} & = & \int_1^x \frac{dt}{t} - \int_t^x \frac{t-[t]}{t^2}dt + 1 - \frac{x-[x]}{x} \\
& = & \log x - \int_1^x \frac{t-[t]}{t^2}dt + 1 + O\left(\frac{1}{x}\right) \\
& = & \log x + 1 - \int_1^\infty \frac{t-[t]}{t^2}dt + \int_x^\infty \frac{t-[t]}{t^2}dt + O\left(\frac{1}{x}\right).
\end{array}$$

Epäoleellinen integraali $\int_1^\infty (t-[t])t^{-2}dt$ on olemassa, koska sitä rajoitetaan integraalilla $\int_1^\infty t^{-2}dt$. Siis,

$$0 \le \int_x^\infty \frac{t-[t]}{t^2}dt \le \int_x^\infty \frac{1}{t^2}dt = \frac{1}{x},$$

joten viimeinen yhtälö saadaan muotoon

$$\sum_{n\le x}\frac{1}{n} = \log x + 1 - \int_1^\infty \frac{t-[t]}{t^2}dt + O\left(\frac{1}{x}\right).$$

Tämä todistaa kohdan (a), kun

$$C = 1 - \int_1^\infty \frac{t-[t]}{t^2}dt.$$

Kun $x \to \infty$ kohdassa (a), saadaan

$$\lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n} - \log x\right) = 1 - \int_1^\infty \frac{t-[t]}{t^2}dt,$$

joten C on Eulerin vakio.

Osoitettaessa kohtaa (b) käytetään saman tyyppistä perustelua mutta funktiolle $f(x) = x^{-s}$, missä $s > 0,\ s \neq 1$. Eulerin summakaavasta saadaan

$$\begin{aligned} \textstyle\sum_{n\leq x} \frac{1}{n^s} &= \int_1^x \frac{dt}{t^s} - s\int_1^x \frac{t-[t]}{t^{s+1}}dt + 1 - \frac{x-[x]}{x^s} \\ &= \frac{x^{1-s}}{1-s} - \frac{1}{1-s} + 1 - s\int_1^\infty \frac{t-[t]}{t^{s+1}}dt + O(x^{-s}). \end{aligned}$$

Täten

$$\sum_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + C(s) + O(x^{-s}), \tag{17}$$

missä

$$C(s) = 1 - \frac{1}{1-s} - s\int_1^\infty \frac{t-[t]}{t^{s+1}}dt.$$

Jos $s > 1$, niin vasen jäsen yhtälöstä (17) lähestyy vakiota $\xi(s)$, kun $x \to \infty$ ja kumpikin termeistä x^{1-s} ja x^{-s} lähestyvät nollaa. Joten $C(s) = \xi(s)$ jos $s > 1$. Jos $0 < s < 1$, niin $x^{-s} \to 0$ ja yhtälö (17) osoittaa, että

$$\lim_{x\to\infty}\left(\sum_{n\leq x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right) = C(s).$$

Täten $C(s)$ on yhtäsuuri vakion $\xi(s)$ kanssa, jos $0 < s < 1$. Tämä todistaa kohdan (b).

Kohtaa (c) todistettaessa käytetään kohtaa (b) kun $s > 1$ ja saadaan

$$\sum_{n>x}\frac{1}{n^s} = \xi(s) - \sum_{n\leq x}\frac{1}{n^s} = \frac{x^{1-s}}{s-1} + O(x^{-s}) = O(x^{1-s}),$$

kun $x^{-s} \leq x^{1-s}$.

Lopuksi kohta (d) todistetaan käyttämällä Eulerin summakaavaa kun $f(t) = t^\alpha$ ja näin ollen saadaan

$$\begin{aligned} \textstyle\sum_{n\leq x} n^\alpha &= \int_1^x t^\alpha dt + \alpha\int_1^x t^{\alpha-1}(t-[t])dt + 1 - (x-[x])x^\alpha \\ &= \frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + O(\alpha\int_1^x t^{\alpha-1}dt) + O(x^\alpha) \\ &= \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha). \end{aligned}$$

□

4.2 Tekijäfunktion kertaluku

4.2.1 Tekijäfunktion $d(n)$ keskiarvo

Tässä luvussa johdetaan Dirichlet'n aymptoottinen kaava tekijäfunktion $d(n)$ osasummalle.

Lause 4.3 *Kaikilla $x \geq 1$ on voimassa*

$$\sum_{n \leq x} d(n) = x \log x + (2C - 1)x + O(\sqrt{x}), \tag{18}$$

missä C on Eulerin vakio. ([1], s.57)

Todistus. Kun $d(n) = \sum_{a|n} 1$, saadaan

$$\sum_{n \leq x} d(n) = \sum_{n \leq x} \sum_{a|n} 1.$$

Tämä on kaksoissumma yli lukujen n ja a. Koska $a|n$, voidaan kirjoittaa $n = qa$ ja käydä summa läpi kaikilla positiivisilla kokonaislukupareilla q, a, missä $qa \leq x$. Siis

$$\sum_{n \leq x} d(n) = \sum_{q,a,qa \leq x} 1. \tag{19}$$

Tämä voidaan tulkita summata yli tiettyjen hilapisteiden qa-tasolla (hilapiste on piste kokonaislukukoordinaatistosta). Hilapisteet $qa = n$ on hyperbolilla, joten summa (17) laskee hilapisteiden lukumäärän hyperbolilla, jotka vastaavat arvoja $n = 1, 2, \ldots, [x]$. Jokaiselle $a \leq x$ voidaan laskea ensimmäinen hilapiste vaakasuoralla suorasegmentillä $1 \leq q \leq x/a$ ja tämän jälkeen voidaan laskea summa yli kaikkien $a \leq x$. Joten yhtälö (19) saadaan muotoon

$$\sum_{n \leq x} d(n) = \sum_{a \leq x} \sum_{q \leq x/a} 1. \tag{20}$$

Nyt käytetään kohtaa (d) lauseesta 4.2, kun $\alpha = 0$ ja saadaan

$$\sum_{q \leq x/a} 1 = \frac{x}{a} + O(1).$$

Käyttämällä tätä yhdessä lauseen 4.2 kohdan (a) kanssa, saadaan

$$\begin{aligned} \textstyle\sum_{n \leq x} d(n) &= \textstyle\sum_{a \leq x} \{\frac{x}{a} + O(1)\} = x \sum_{a \leq x} \frac{1}{a} + O(x) \\ &= x\{\log x + C + O\left(\tfrac{1}{x}\right)\} + O(x) = x \log x + O(x). \end{aligned}$$

Tämä on heikko versio yhtälöstä (18), joka merkitsee, että

$$\sum_{n\leq x} d(n) \sim x\log x \text{ kun } x\to\infty$$

ja että tekijäfunktion $d(n)$ keskimääräinen kertaluku on $\log n$.

Todistaaksemme tarkemman kaavan (18) täytyy palata summaan (19), joka laskee hyperbolisella alueella olevien hilapisteiden lukumäärän ja ottaa huomioon suoralla $q = a$ olevan alueen symmetrian. Alueen hilapisteiden kokonaismäärä on

$$\sum_{n\leq x} d(n) = 2\sum_{a\leq\sqrt{x}} \{\left[\frac{x}{a}\right] - a\} + [\sqrt{x}].$$

Käytetään nyt relaatiota $[y] = y+O(1)$ ja lauseen 4.2 kohtia (a) ja (d), joista saadaan

$$\begin{aligned}
\textstyle\sum_{n\leq x} d(n) &= 2\textstyle\sum_{a\leq\sqrt{x}}\{\frac{x}{a} - d + O(1)\} + O(\sqrt{x}) \\
&= 2x\textstyle\sum_{a\leq\sqrt{x}}\frac{1}{a} - s\sum_{a\leq\sqrt{x}} a + O(\sqrt{x}) \\
&= 2x\{\log\sqrt{x} + C + O\left(\tfrac{1}{\sqrt{x}}\right)\} - 2\{\tfrac{x}{2} + O(\sqrt{x})\} + O(\sqrt{x}) \\
&= x\log x + (2C-1)x + O(\sqrt{x}).
\end{aligned}$$

Tämä päättää Dirichlet'n kaavan todistuksen. □

4.2.2 Tekijäfunktion $\sigma_\alpha(n)$ keskiarvo

Tapaus $\alpha = 0$ käsiteltiin lauseessa 4.3. Seuraavaksi tarkastellaan reaalista $\alpha > 0$ ja käsitellään tapaus $\alpha = 1$ erikseen.

Lause 4.4 *Kaikilla $x \geq 1$ on voimassa*

$$\sum_{n\leq x}\sigma_\alpha(n) = \frac{1}{2}\xi(2)x^2 + O(x\log x). \tag{21}$$

([1], s.60)

Todistus. Menetelmä on samanlainen kun jota käytettiin derivoitaessa lauseen (4.3) heikkoa versiota. Käyttämällä lauseen (4.2) kohtia (a) ja (b) saadaan

$$\begin{aligned}
\textstyle\sum_{n\leq x}\sigma_1(n) &= \textstyle\sum_{n\leq x}\sum_{q|n} q = \sum_{q,a,qa\leq x} q = \sum_{a\leq x}\sum_{q\leq x/a} q \\
&= \textstyle\sum_{a\leq x}\{\frac{1}{2}\left(\frac{x}{a}\right)^2 + O\left(\frac{x}{a}\right)\} = \frac{x^2}{2}\sum_{a\leq x}\frac{1}{a^2} + O\left(x\sum_{a\leq x}\frac{1}{a}\right) \\
&= \tfrac{x^2}{2}\{-\tfrac{1}{x} + \xi(2) + O\left(\tfrac{1}{x^2}\right)\} + O(x\log x) = \tfrac{1}{2}\xi(2)x^2 + O(x\log x).
\end{aligned}$$

□

Huomautus. Voidaan osoittaa, että $\xi(2) = \pi^2/6$. Siksi yhtälö (21) osoittaa, että tekijäfunktion $\sigma_1(n)$ keskimääräinen kertaluku on $\pi^2 n/12$. ([1], s.60)

Lause 4.5 *Jos $x \geq 1$ ja $\alpha > 0$, $\alpha \neq 1$, niin*

$$\sum_{n \leq x} \sigma_\alpha(n) = \frac{\xi(\alpha+1)}{\alpha+1} x^{\alpha+1} + O(x^\beta),$$

missä $\beta = \max\{1, \alpha\}$. ([1], s.60)

Todistus Tällä kertaa käytetään lauseen 4.2 kohtia (b) ja (d), joista saadaan

$$\begin{aligned}
\textstyle\sum_{n\leq x} \sigma_\alpha(n) &= \textstyle\sum_{n\leq x} \sum_{q|n} q^\alpha = \sum_{a\leq x} \sum_{q\leq x/a} q^\alpha \\
&= \textstyle\sum_{a\leq x} \left\{ \frac{1}{\alpha+1} \left(\frac{x}{a}\right)^{\alpha+1} + O\left(\frac{x^\alpha}{a^\alpha}\right) \right\} \\
&= \textstyle\frac{x^{\alpha+1}}{\alpha+1} \sum_{a\leq x} \frac{1}{a^{\alpha+1}} + O\left(x^\alpha \sum_{a\leq x} \frac{1}{a^\alpha}\right) \\
&= \textstyle\frac{x^{\alpha+1}}{\alpha+1} \left\{ \frac{x^{-\alpha}}{-\alpha} + \xi(\alpha+1) + O(x^{-\alpha-1}) \right\} \\
&\quad \textstyle + O\left(x^\alpha \left\{ \frac{x^{1-\alpha}}{1-\alpha} + \xi(\alpha) + O(x^{-\alpha}) \right\} \right) \\
&= \textstyle\frac{\xi(\alpha+1)}{\alpha+1} x^{\alpha+1} + O(x) + O(1) + O(x^\alpha) = \frac{\xi(\alpha+1)}{\alpha+1} x^{\alpha+1} + O(x^\beta),
\end{aligned}$$

missä $\beta = \max\{1, \alpha\}$.

Jotta löydetään tekijäfunktion $\sigma_\alpha(n)$ keskiarvo negatiiviselle arvolle α, merkitään $\alpha = -\beta$, missä $\beta > 0$. ([1], s.60)

Lause 4.6 *Jos $\beta > 0$, niin olkoon $\delta = \max\{0, 1-\beta\}$. Sitten jos $x > 1$, saadaan*

$$\begin{aligned}
\textstyle\sum_{n\leq x} \sigma_{-\beta}(n) &= \xi(\beta+1)x + O(x^\delta), \quad \textit{jos } \beta \neq 1, \\
&= \xi(2)x + O(\log x), \qquad \textit{jos } \beta = 1.
\end{aligned}$$

[1], s.61)

Todistus. Nyt on

$$\begin{aligned}
\textstyle\sum_{n\leq x} \sigma_{-\beta}(n) &= \textstyle\sum_{n\leq x} \sum_{a|n} \frac{1}{a^\beta} = \sum_{a\leq n} \frac{1}{a^\beta} \sum_{q\leq x/a} 1 \\
&= \textstyle\sum_{a\leq x} \frac{1}{a^\beta} \left\{ \frac{x}{a} + O(1) \right\} = x \sum_{a\leq x} \frac{1}{a^{\beta+1}} + O\left(\sum_{a\leq x} \frac{1}{a^\beta}\right).
\end{aligned}$$

Viimeinen termi on $O(\log x)$, jos $\beta = 1$ ja $O(x^{-\beta})$, jos $\beta \neq 1$. Joten

$$x \sum_{d \leq x} \frac{1}{d^{\beta+1}} = \frac{x^{1-\beta}}{-\beta} + \xi(\beta+1)x + O(x^{-\beta}) = \xi(\beta+1)x + O(x^{1-\beta}).$$

Tämä päättää todistuksen. □

4.2.3 Tekijäfunktion sovellus

Alkulukuteoriaa voidaan joskus käyttää arvioimaan multiplikatiivisten aritmeettisten funktioiden suuruusluokkaa. Tässä kappaleessa sitä käytetetään johtamaan tekijäfunktion $d(n)$ epäyhtälöitä. Aikaisemmin todistettiin, että tekijäfunktion $d(n)$ keskiarvo on $\log n$. Kun n on alkuluku, niin $d(n) = 2$, joten funktion $d(n)$ kasvu korostuu eniten kun luvulla n on monta tekijää. Oletetaan, että n on kaikkien lukua x pienempien alkulukujen tulo, siis

$$n = 2 \cdot 3 \cdot 5 \cdot \cdots p_{\pi(x)}, \tag{22}$$

missä $\pi(x)$ on sellaisten alkulukujen lukumäärä, jotka ovat pienempiä kun luku x (kts.[1], s.74).

Koska $d(n)$ on multiplikatiivinen, niin

$$d(n) = d(2)d(3)\cdots d(p_{\pi(x)}) = 2^{\pi(x)}, ([1], \text{s.264})$$

Suurilla luvun x arvoilla, $\pi(x)$ on arviolta $x/\log x$ ja yhtälöstä (22) saadaan

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

missä ϑ on Chebysevin funktio (kts. [1], s.79).
Edellisten yhtälöiden perusteella $2^{\pi(x)}$ on arviolta $2^{\log n/\log\log n}$. Nyt

$$2^{a \log n} = e^{a \log n \log 2} = n^{a \log 2},$$

joten $2^{\log n/\log\log n} = n^{\log 2/\log\log n}$. Toisinsanoen, kun n on yhtälön (22) muodossa, niin $d(n)$ on arviolta $2^{\log n/\log\log n} = n^{\log 2/\log\log n}$.

Kehittämällä tätä hiukan enemmän saadaan seuraavat tekijäfunktion $d(n)$ epäyhtälöt. ([1], s.294)

Lause 4.7 *Olkoon $\epsilon > 0$ annettu, jolloin saadaan*

(*a*) *On olemassa kokonaisluku $N(\epsilon)$ siten, että kun $n \geq N(\epsilon)$, niin*

$$d(n) < 2^{(1+\epsilon)\log n/\log\log n} = n^{(1+\epsilon)\log 2/\log\log n}.$$

(*b*) *Äärettömän monella luvulla n on*

$$d(n) > 2^{(1-\epsilon)\log n/\log\log n} = n^{(1-\epsilon)\log 2/\log\log n}.$$

Huomautus. Epäyhtälöt ovat yhtäpitäviä yhtälön

$$\limsup_{n\to\infty} \frac{\log d(n)\log\log n}{\log n} = \log 2$$

kanssa. ([1], s.294)

Todistus. Kirjoitetaan $n = p_1^{a_1}\cdots p_k^{a_k}$, joten $d(n) = \prod_{i=1}^{k}(a_i+1)$. Jaetaan tulo kahteen osaan ja erotetaan alkutekijät, jotka ovat $< f(n)$, alkutekijöistä, jotka ovat $\geq f(n)$. Funktio $f(n)$ määritellään myöhemmin. Näin ollen $d(n) = P_1(n)P_2(n)$, missä

$$P_1(n) = \prod_{p_1<f(n)} (a_i+1) \text{ ja } P_2(n) = \prod_{p_i\geq f(n)} (a_i+1).$$

Tulossa $P_2(n)$ käytetään epäyhtälöä $(a+1) \leq 2^a$, jotta saadaan $P_2(n) \leq 2^{S(n)}$, missä

$$S(n) = \sum_{i=1, p_i\geq f(n)}^{k} a_i.$$

Nyt

$$n = \prod_{i=1}^{k} p_i^{a_i} \geq \prod_{p_i\geq f(n)} p_i^{a_i} \geq \prod_{p_i\geq f(n)} f(n)^{a_i} = f(n)^{S(n)},$$

joten

$$\log n \geq S(n)\log f(n) \quad \text{eli} \quad S(n) \leq \frac{\log n}{\log f(n)}.$$

Tästä saadaan

$$P_2(n) \leq 2^{\log n/\log f(n)}. \tag{23}$$

Arvioitaessa tuloa $P_1(n)$ saadaan

$$P_1(n) = \exp\Big\{ \sum_{p_i<f(n)} \log(a_i+1)\Big\}$$

ja osoitetaan, että $\log(a_i + 1) < 2 \log\log n$, jos n on riittävän suuri. Itse asiassa saadaan

$$n \geq p_i^{a_i} \geq 2^{a_i},$$

joten

$$\log n \geq a_i \log 2 \quad \text{eli} \quad a_i \leq \log n / \log 2.$$

Siksi

$$1 + a_i \leq 1 + \frac{\log n}{\log 2} < (\log n)^2, \quad \text{jos } n \geq n_1,$$

jollakin luvulla n_1. Täten siitä, että $n \geq n_1$, seuraa $\log(1+a_i) < \log(\log n)^2 = 2 \log\log n$. Tästä saadaan

$$P_1(n) < \exp\left\{2 \log\log n \sum_{p_i < f(n)} 1\right\} \leq \exp\{2 \log\log n \pi(f(n))\}.$$

Käyttämällä epäyhtälöä $\pi(x) < 6x/\log x$ (kts. [1], lause 4.6, s.82) saadaan

$$P_1(n) < \exp\left\{\frac{12 f(n) \log\log n}{\log f(n)}\right\} = 2^{cf(n) \log\log n / \log f(n)}, \tag{24}$$

missä $c = 12/\log 2$. Yhdistämällä yhtälöt (22) ja (24) saadaan $d(n) = P_1(n)P_2(n) < 2^{g(n)}$, missä

$$g(n) = \frac{\log n + cf(n) \log\log n}{\log f(n)} = \frac{\log n}{\log\log n} \frac{1 + c\frac{f(n) \log\log n}{\log n}}{\frac{\log f(n)}{\log\log n}}.$$

Nyt valitaan $f(n)$ niin, että $f(n) \log\log n / \log n \to 0$ ja myös $\log f(n) / \log\log n \to 1$, kun $n \to \infty$. Tähän riittää se, että valitaan

$$f(n) = \frac{\log n}{(\log\log n)^2}.$$

Silloin

$$g(n) = \frac{\log n}{\log\log n} \frac{1 + o(1)}{1 + o(1)} = \frac{\log n}{\log\log n}(1 + o(1)) < (1 + \epsilon)\frac{\log n}{\log\log n},$$

jos $n \geq N(\epsilon)$ jollakin $N(\epsilon)$. Tämä todistaa kohdan (a).

Todistaaksemme kohdan (b) valitaan sellainen kokonaislukujen joukko n, jossa on paljon alkulukutekijöitä . Olkoon n kaikkien lukua x pienempien

alkulukujen tulo. Nyt $n \to \infty$, jos ja vain jos $x \to \infty$. Alkulukulauseen (kts. [1] s.74) mukaan tällä luvulla n on

$$d(n) = 2^{\pi(x)} = 2^{(1+o(1))x/\log x}.$$

Myös tällaiselle luvulla n on olemassa

$$\log n = \sum_{p \le x} \log p = \vartheta(x) = x(1 + (81)).$$

Siis

$$x = \frac{\log n}{1 + o(1)} = (1 + o(1)) \log n,$$

joten

$$\begin{aligned} \log x &= \log\log n + \log(1 + o(1)) = \log\log n \left(1 + \tfrac{\log(1+o(1))}{\log\log n}\right) \\ &= (1 + o(1)) \log\log n. \end{aligned}$$

Täten $x/\log x = (1 + o(1)) \log n/\log\log n$ ja

$$d(n) = 2^{(1+o(1))\log n/\log\log n}$$

tällä luvulla n. Mutta $1 + o(1) > 1 - \epsilon$, jos $n \ge N(\epsilon)$ jollakin $N(\epsilon)$. Tämä todistaa kohdan (b).

□

Huomautus. Lauseen (4.7) seuraukseksi saadaan yhtälö

$$d(n) = o(n^{\delta}),$$

kaikilla $\delta > 0$. Tämä tulos voidaan johtaa myös ilman alkulukulauseen käyttöä. (Todistus sivuutetaan.) ([1], s.296)

Viitteet

[1] Apostol, Tom M. : *Introduction to Analytic Number Theory*, neljäs painos. Springer, 1995.

[2] Burton, David M. : *Elementary Number Theory*, viides painos. McGraw-Hill Companies, 2000.

[3] Dudley, Underwood: *Elementary Number Theory*, toinen painos. W. H. Freeman and Company, 1978.

[4] Halmetoja, Markku: *Matematiikkalehti Solmu: Täydellisistä luvuista*, 2/2005.

[5] Haukkanen, Pentti: *Lukuteoriaa*, Tampereen Yliopiston opetusmoniste.

[6] Nathanson, Melvyn B. : *Elementary Methods in Number Theory*, ensimmäinen painos. Springer, 2000.

[7] Rosen, Kenneth H. : *Number Theory and Its Application*, kolmas painos. Addison-Wesley Publishing Company, 1993.

[8] Vanden Eynden, Charles: *Elementary Number Theory*, toinen painos. McGraw-Hill Companies, 2001.

[9] Weisstein, Eric W. : *MathWorld*, A Wolfram Web Resource, http://mathworld.wolfram.com/, tammikuu 2005.