Lukuteoriaa

Pentti Haukkanen

Sisällys

1 Kongruensseista

1.1 Eulerin-Fermat'n lause

Määritelmä Joukko $\{r_1, r_2, \ldots, r_m\}$ on *täydellinen jäännössysteemi modulo* m, jos $r_i \not\equiv r_j \pmod{m}$ aina, kun $i \neq j$.

Esimerkki 1.1.1 Joukot $\{0, 1, \ldots, m-1\}$ ja $\{1, 2, \ldots, m\}$ ovat täydellisiä jäännössysteemejä modulo m.

Lause 1.1.1 *Olkoon* $\{r_1, r_2, \ldots, r_m\}$ *täydellinen jäännössysteemi modulo* m*, olkoon* a *sellainen kokonaisluku, että* $(a, m) = 1$*, ja olkoon* b *mikä tahansa kokonaisluku. Silloin*

$$\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$$

on täydellinen jäännössysteemi modulo m*.*

Todistus Joukossa $\{ar_1 + b, ar_2 + b, \ldots, ar_m + b\}$ on m alkiota, joten riittää todistaa, että sen alkiot ovat pareittain epäkongruentteja modulo m. Tehdään vastaoletus, että on olemassa sellaiset i ja j $(i \neq j)$, että

$$ar_i + b \equiv ar_j + b \pmod{m}.$$

Silloin $ar_i \equiv ar_j \pmod{m}$. Koska $(a, m) = 1$, niin algebran monisteen lauseen 1.8.4 mukaan $r_i \equiv r_j \pmod{m}$. Tämä on ristiriidassa sen kanssa, että $\{r_1, r_2, \ldots, r_m\}$ on täydellinen jäännössysteemi modulo m. Siis vastaoletus on väärä. □

Määritelmä *Eulerin funktio* ϕ määritellään kaavalla

$$\phi(n) = |\{r : \ 1 \leq r \leq n, (r, n) = 1\}|, \ n \in \mathbf{Z}^+.$$

Huomautus Funktio ϕ toteuttaa muun muassa kaavan

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

Erityisesti $\phi(p^k) = p^k - p^{k-1}$, kun p on alkuluku ja $k \in \mathbf{Z}^+$.

Määritelmä Joukko $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ on *supistettu jäännössysteemi modulo* m, jos

1) $(r_i, m) = 1$, kun $i = 1, 2, \ldots, \phi(m)$,

2) $r_i \not\equiv r_j \pmod{m}$, kun $i \neq j$.

Esimerkki 1.1.2 Joukot $\{r:\ 0 \leq r \leq m-1, (r,m)=1\}$ ja $\{r:\ 1 \leq r \leq m, (r,m)=1\}$ ovat supistettuja jäännössysteemejä modulo m.

Huomautus Supistetun jäännössysteemin modulo m käsite on analoginen algebran käsitteen alkuluokkaryhmä modulo m kanssa.

Lause 1.1.2 *Olkoon $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ supistettu jäännössysteemi modulo m, ja olkoon a sellainen kokonaisluku, että $(a,m)=1$. Silloin*

$$\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$$

on supistettu jäännössysteemi modulo m.

Todistus Joukossa $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ on $\phi(m)$ alkiota, joten riittää todistaa, että supistetun jäännössysteemin määritelmän kohdat 1 ja 2 ovat voimassa.

Kohta 1. Tehdään vastaoletus, että on olemassa sellainen $i \in \{1, 2, \ldots, \phi(m)\}$, että $(ar_i, m) > 1$. Siis on olemassa sellainen alkuluku p, että $p|ar_i$ ja $p|m$. Siis $p|a$ ja $p|m$, tai $p|r_i$ ja $p|m$. Jos $p|a$ ja $p|m$, niin $(a,m) > 1$, mikä on ristiriidassa oletuksen $(a,m)=1$ kanssa. Jos taas $p|r_i$ ja $p|m$, niin $(r_i, m) > 1$. Siis $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ ei ole supistettu jäännössysteemi modulo m, mikä on ristiriidassa oletuksen kanssa. Näin ollen vastaoletus on väärä, joten $(ar_i, m) = 1$ aina, kun $i = 1, 2, \ldots, \phi(m)$.

Kohta 2. Tehdään vastaoletus, että on olemassa sellaiset i ja j $(i \neq j)$, että $ar_i \equiv ar_j \pmod{m}$. Koska $(a,m)=1$, niin algebran monisteen lauseen 1.8.4 mukaan $r_i \equiv r_j \pmod{m}$. Tämä on ristiriidassa sen kanssa, että $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ on supistettu jäännössysteemi modulo m. Siis vastaoletus on väärin eli $ar_i \not\equiv ar_j \pmod{m}$, kun $i \neq j$. □

Lause 1.1.3 (Eulerin-Fermat'n lause) *Jos $(a,m)=1$, niin*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Todistus Merkitään

$$R = \{r_1, r_2, \ldots, r_{\phi(m)}\} = \{r:\ 0 \leq r \leq m-1, (r,m)=1\}$$

ja

$$aR = \{ar_1, ar_2, \ldots, ar_{\phi(m)}\}.$$

Silloin joukot R ja aR ovat supistettuja jäännössysteemejä modulo m. Lisäksi jokaista lukua $ar_i \in aR$ kohti on olemassa sellainen yksikäsitteinen luku $r_j \in R$, että $r_j = (ar_i) \bmod m$. Siis jokaista lukua $ar_i \in aR$ kohti on olemassa sellainen yksikäsitteinen luku $r_j \in R$, että $r_j \equiv ar_i \pmod{m}$. Näin ollen

$$ar_1 ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$$

eli

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Koska $(r_1 r_2 \cdots r_{\phi(m)}, m) = 1$, niin supistamalla saamme, että $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Seuraus 1.1.1 (Fermat'n pieni lause) *Jos p on alkuluku ja $p \nmid a$, niin*

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

Todistus Seuraus saadaan lauseesta 1.1.3, koska $\phi(p) = p - 1$.

Seuraus 1.1.2 *Jos p on alkuluku, niin*

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

Todistus Jaetaan tarkastelu kahteen osaan: $p|a$, $p \nmid a$. Jos $p|a$, niin $a \equiv 0 \pmod{p}$ ja $a^p \equiv 0 \pmod{p}$, joten $a^p \equiv a \pmod{p}$. Jos $p \nmid a$, niin Fermat'n pienen lauseen mukaan $a^{p-1} \equiv 1 \pmod{p}$. Kertomalla kongruenssi puolittain luvulla a saadaan haluttu tulos. □

Huomautus Tarkastellaan kongruenssia $ax \equiv b \pmod{m}$, missä $(a, m) = 1$. Kertomalla kongruenssi puolittain luvulla $a^{\phi(m)-1}$ saadaan $a^{\phi(m)-1} ax \equiv a^{\phi(m)-1} b \pmod{m}$. Eulerin-Fermat'n lauseen perusteella saadaan ratkaisuksi

$$x \equiv a^{\phi(m)-1} b \pmod{m}.$$

Erityisesti jos p on alkuluku ja $p \nmid a$, niin kongruenssin $ax \equiv b \pmod{p}$ ratkaisu on

$$x \equiv a^{p-2} b \pmod{p}.$$

Esimerkki 1.1.3 Koska $\phi(10) = 4$ (totea!), niin kongruenssin $3x \equiv 7 \pmod{10}$ ratkaisu on

$$x \equiv 3^{\phi(10)-1} 7 \equiv 3^3 7 \equiv 9 \pmod{10}.$$

Esimerkki 1.1.4 Fermat'n pienen lauseen perusteella $3^{10} \equiv 1 \pmod{11}$. Näin ollen $3^{201} = (3^{10})^{20} 3 \equiv 3 \pmod{11}$. Siis $3^{201} \bmod 11 = 3$.

1.2 Wilsonin lause

Määritelmä Olkoon $(a, m) = 1$. Silloin kongruenssin $ax \equiv 1 \pmod{m}$ ratkaisua x sanotaan luvun *a käänteisluvuksi modulo m*. Merkitään $x = a^{-1}$.

Huomautus Kun $(a, m) = 1$, niin luvun a käänteisluku modulo m on olemassa ja on yksikäsitteinen modulo m. (Ks. algebran monisteen lause 1.11.1.)

Huomautus Käänteisluvun modulo m käsite on analoginen käänteisalkion käsitteen kanssa alkuluokkaryhmässä modulo m.

Huomautus Kun $(a, m) = 1$, niin kongruenssin $ax \equiv b \pmod{m}$ ratkaisu on $x \equiv a^{-1}b \pmod{m}$. (Totea!)

Esimerkki 1.2.1 Luku 9 on luvun 7 käänteisluku modulo 31, sillä $7 \cdot 9 \equiv 1 \pmod{31}$. Huomaa, että vastaavasti luku 7 on luvun 9 käänteisluku modulo 31.

Esimerkki 1.2.2 Kongruenssin $7x \equiv 22 \pmod{31}$ ratkaisu on

$$x \equiv 9 \cdot 22 \equiv 198 \equiv 12 \pmod{31}.$$

Huomautus Kun p on alkuluku ja $p \nmid a$, niin Fermat'n pienen lauseen perusteella luku a^{p-2} on luvun a käänteisluku modulo p. (Totea!)

Lause 1.2.1 *Olkoon p alkuluku. Silloin luku a on itsensä käänteisluku modulo p, jos ja vain jos* $a \equiv 1 \pmod{p}$ *tai* $a \equiv -1 \pmod{p}$.

Todistus Jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$, niin $a^2 \equiv 1 \pmod{p}$. Siis a on itsensä käänteisluku modulo p.

Jos a on itsensä käänteisluku modulo p, niin $a^2 \equiv 1 \pmod{p}$. Siis $p|(a^2 - 1)$. Koska $a^2 - 1 = (a-1)(a+1)$, niin $p|(a-1)$ tai $p|(a+1)$. Näin ollen $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$. □

Lause 1.2.2 (Wilsonin lause) *Jos p on alkuluku, niin* $(p-1)! \equiv -1 \pmod{p}$.

Todistus Lause on selvästi voimassa, kun $p = 2$ tai $p = 3$ (totea!). Oletetaan, että p on lukua 3 suurempi alkuluku. Olkoon $a \in \{2, 3, \ldots, p-2\}$. Koska $(a, p) = 1$, niin luvulla a on käänteisluku modulo p. Lauseen 1.2.1 mukaan luvun a käänteisluku modulo p on erisuuri kuin luku a itse. Siis luvut $2, 3, \ldots, p-2$ voidaan jakaa erillisiin pareihin niin, että jokaisen parin tulo on $\equiv 1 \pmod{p}$. Kertomalla nämä parit keskenään saadaan, että

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}.$$

Koska $(p-1) \equiv -1 \pmod{p}$, niin

$$2 \cdot 3 \cdots (p-2)(p-1) \equiv -1 \pmod{p}$$

eli $(p-1)! \equiv -1 \pmod{p}$. □

Huomautus Wilsonin lauseen tulos pitää paikkansa myös kääntäen (ks. lause 1.2.3). Siis sitä voi käyttää alkulukutestinä.

Lause 1.2.3 *Jos n on sellainen positiivinen kokonaisluku, että $(n-1)! \equiv -1 \pmod{n}$, niin n on alkuluku.*

Todistus Oletetaan, että $(n-1)! \equiv -1 \pmod{n}$, ja väitetään, että n on alkuluku. Tehdään vastaoletus, että n on yhdistetty luku. Siis $n = ab$, missä $1 < a, b < n$. Näin ollen $a|(n-1)!$. Koska $(n-1)! \equiv -1 \pmod{n}$, niin $n|((n-1)!+1)$. Nyt koska $a|n$, niin $a|((n-1)!+1)$. Siis $a|(n-1)!$ ja $a|((n-1)!+1)$, joten $a|((n-1)!+1-(n-1)!)$ eli $a|1$, mikä on mahdotonta, koska $a > 1$. Näin ollen vastaoletus on väärä. □

Esimerkki 1.2.3 *Koska $(6-1)! = 120 \equiv 0 \not\equiv -1 \pmod{6}$, niin 6 ei ole alkuluku.*

1.3 Kiinalainen jäännöslause

Lause 1.3.1 *Olkoot $m_1, m_2, \ldots, m_r$ (≥ 2) pareittain suhteellisia alkulukuja. Silloin kongruenssiryhmällä*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

on yksikäsitteinen ratkaisu modulo $M = m_1 m_2 \cdots m_r$.

Todistus Jaetaan todistus kahteen osaan: konstruoidaan ratkaisu ja todistetaan ratkaisun yksikäsitteisyys. Konstruoidaan ensin ratkaisu. Merkitään $M_k = M/m_k = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r$. Koska luvut $m_1, m_2, \ldots, m_r$ ovat pareittain suhteellisia alkulukuja, niin $(M_k, m_k) = 1$. Näin ollen luvulla M_k on käänteisluku modulo m_k. Merkitään käänteislukua symbolilla y_k, jolloin $M_k y_k \equiv 1 \pmod{m_k}$.

Todistetaan nyt, että kongruenssiryhmän ratkaisu on

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r.$$

Koska $m_k | M_j$, kun $j \neq k$, niin $M_j \equiv 0 \pmod{m_k}$, kun $j \neq k$. Näin ollen $x \equiv a_k M_k y_k \pmod{m_k}$. Koska $M_k y_k \equiv 1 \pmod{m_k}$, niin $x \equiv a_k \pmod{m_k}$. Siis x on kongruenssiryhmän ratkaisu.

Todistetaan, että ratkaisu on yksikäsitteinen modulo M. Olkoot x_0 ja x_1 kaksi kongruenssiryhmän ratkaisua. Silloin jokaista lukua $k = 1, 2, \ldots, r$ kohti $x_0 \equiv x_1 \equiv a_k \pmod{m_k}$, joten jokaista lukua $k = 1, 2, \ldots, r$ kohti $m_k | (x_0 - x_1)$. Näin ollen $M | (x_0 - x_1)$ eli $x_0 \equiv x_1 \pmod{M}$. □

Esimerkki 1.3.1 Ratkaistaan kongruenssiryhmä

$$\begin{aligned} x &\equiv 1 \pmod 3, \\ x &\equiv 2 \pmod 5, \\ x &\equiv 3 \pmod 7. \end{aligned}$$

Koska luvut $3, 5, 7$ ovat pareittain suhteellisia alkulukuja, niin kiinalaisen jäännöslauseen mukaan kongruenssiryhmällä on yksikäsitteinen ratkaisu modulo $3 \cdot 5 \cdot 7$ eli modulo 105. Sovelletaan kiinalaisen jäännöslauseen todistusta. Silloin $M = 3 \cdot 5 \cdot 7 = 105$, $M_1 = 105/3 = 35$, $M_2 = 105/5 = 21$, $M_3 = 105/7 = 15$. Lukujen M_k on käänteisluvut y_k modulo m_k toteuttavat ehdot $35y_1 \equiv 1 \pmod 3$, $21y_2 \equiv 1 \pmod 5$, $15y_3 \equiv 1 \pmod 7$. Näin ollen $y_1 \equiv 2 \pmod 3$, $y_2 \equiv 1 \pmod 5$, $y_3 \equiv 1 \pmod 7$. (Totea!) Siis

$$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \equiv 157 \equiv 52 \pmod{105}.$$

1.4 Polynomikongruensseista

Tarkastellaan polynomikongruenssin $f(x) \equiv 0 \pmod{m}$ ratkaisemista, missä $m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$. Kirjoitetaan se kongruenssiryhmänä

$$f(x) \equiv 0 \pmod{p_i^{a_i}},\ i = 1, 2, \ldots, n,$$

ja ratkaistaan ryhmän jokainen kongruenssi. Lopuksi sovelletaan kiinalaista jäännöslausetta.

Esimerkki 1.4.1 Kongruenssin

$$2x^3 + 7x - 4 \equiv 0 \pmod{200}$$

ratkaiseminen palautuu kongruenssiryhmän

$$\begin{aligned} 2x^3 + 7x - 4 &\equiv 0 \pmod{8}, \\ 2x^3 + 7x - 4 &\equiv 0 \pmod{25} \end{aligned}$$

ratkaisemiseksi, sillä $200 = 2^3 \cdot 5^2$. Lauseen 1.4.1 periaatteella voidaan todistaa, että tämä palautuu kongruenssiryhmän

$$\begin{aligned} x &\equiv 4 \pmod{8}, \\ x &\equiv 16 \pmod{25} \end{aligned}$$

ratkaisemiseksi. Kiinalaisen jäännöslauseen periaatteella saadaan ratkaisuksi $x \equiv 116 \pmod{200}$. (Totea!)

Kongruenssi

$$f(x) \equiv 0 \pmod{p^a}$$

ratkaistaan niin sanotulla nostoperiaatteella. Ensiksi kongruenssi $f(x) \equiv 0 \pmod{p}$ ratkaistaan kokeilemalla. Oletetaan sitten, että kongruenssin $f(x) \equiv 0 \pmod{p^k}$ ratkaisut tunnetaan. Silloin kongruenssin $f(x) \equiv 0 \pmod{p^{k+1}}$ ratkaisut saadaan seuraavan lauseen avulla.

Lause 1.4.1 *Olkoon $f(x)$ kokonaislukukertoiminen polynomi, p alkuluku ja k (≥ 1) kokonaisluku. Silloin x_{k+1} on kongruenssin*

$$f(x) \equiv 0 \pmod{p^{k+1}} \tag{1.4.1}$$

ratkaisu, jos ja vain jos $x_{k+1} = x_k + tp^k$*, missä* x_k*,* $0 \leq x_k < p^k$*, on kongruenssin*

$$f(x) \equiv 0 \pmod{p^k} \tag{1.4.2}$$

ratkaisu ja t*,* $0 \leq t < p$*, on kongruenssin*

$$f'(x_k)t \equiv -\frac{f(x_k)}{p^k} \pmod{p} \tag{1.4.3}$$

ratkaisu.

Todistus Olkoon x_{k+1} kongruenssin (1.4.1) ratkaisu. Silloin x_{k+1} on myös kongruenssin (1.4.2) ratkaisu. Näin ollen on olemassa sellainen kongruenssin (1.4.2) ratkaisu x_k, että $x_{k+1} \equiv x_k \pmod{p^k}$, missä $0 \leq x_k < p^k$. Täten $x_{k+1} = x_k + tp^k$, missä $t \in \mathbf{Z}$. Koska

$$x_k + (t + lp)p^k \equiv x_k + tp^k \pmod{p^{k+1}}, \text{ kun } l \in \mathbf{Z},$$

niin riittää, että $0 \leq t < p$. Todistetaan vielä, että t toteuttaa kongruenssin (1.4.3). Binomikaavan avulla voidaan todistaa (harj.), että

$$f(x_{k+1}) = f(x_k + tp^k) = f(x_k) + tp^k f'(x_k) + \frac{1}{2}t^2 p^{2k} f''(x_k) + \cdots \tag{1.4.4}$$

Koska $2k \geq k + 1$, niin

$$f(x_{k+1}) \equiv f(x_k) + tp^k f'(x_k) \pmod{p^{k+1}}.$$

Koska $f(x_{k+1}) \equiv 0 \pmod{p^{k+1}}$, niin

$$tp^k f'(x_k) \equiv -f(x_k) \pmod{p^{k+1}}.$$

Edelleen koska $f(x_k) \equiv 0 \pmod{p^k}$, niin $p^k | f(x_k)$. Näin ollen t toteuttaa kongruenssin (1.4.3). Olemme siis todistaneet, että jos x_{k+1} on kongruenssin (1.4.1) ratkaisu, niin $x_{k+1} = x_k + tp^k$, missä x_k, $0 \leq x_k < p^k$, on kongruenssin (1.4.2) ratkaisu ja t, $0 \leq t < p$, on kongruenssin (1.4.3) ratkaisu. Käänteinen puoli voidaan todistaa yhtälön (1.4.4) avulla. □

Esimerkki 1.4.2 Ratkaistaan kongruenssi

$$x^3 + x^2 + 29 \equiv 0 \pmod{25}.$$

Merkitään $f(x) = x^3 + x^2 + 29$. Kokeilemalla havaitaan, että kongruenssin $f(x) \equiv 0 \pmod 5$ ainoa ratkaisu on $x_1 \equiv 3 \pmod 5$. Etsitään kongruenssin $f(x) \equiv 0 \pmod{25}$ ratkaisu muodossa $x_2 = 3 + 5t$, missä t, $0 \leq t < 5$, toteuttaa kongruenssin

$$f'(3)t \equiv -\frac{f(3)}{5} \pmod 5$$

eli kongruenssin

$$33t \equiv -13 \pmod 5.$$

Siis $t = 4$, joten kongruenssin $f(x) \equiv 0 \pmod{25}$ ratkaisu on $x_2 \equiv 23 \pmod{25}$.

Esimerkki 1.4.3 Ratkaistaan kongruenssi

$$x^2 + x + 7 \equiv 0 \pmod{27}.$$

Merkitään $f(x) = x^2 + x + 7$. Kokeilemalla havaitaan, että kongruenssin $f(x) \equiv 0 \pmod 3$ ainoa ratkaisu on $x_1 \equiv 1 \pmod 3$.

Etsitään kongruenssin $f(x) \equiv 0 \pmod 9$ ratkaisu muodossa $x_2 = 1 + 3t$, missä t, $0 \leq t < 3$, toteuttaa kongruenssin

$$f'(1)t \equiv -\frac{f(1)}{3} \pmod 3$$

eli kongruenssin

$$0t \equiv -3 \pmod 3.$$

Kaikki luvut t, $0 \leq t < 3$, toteuttavat kongruenssin, joten kongruenssin $f(x) \equiv 0 \pmod 9$ ratkaisut ovat $x_2 \equiv 1, 4, 7 \pmod 9$.

Etsitään kongruenssin $f(x) \equiv 0 \pmod{27}$ ratkaisu muodossa $x_3 = x_2 + 9t$, missä $x_2 = 1, 4, 7$ ja t, $0 \leq t < 3$, toteuttaa kongruenssin

$$f'(x_2)t \equiv -\frac{f(x_2)}{9} \pmod 3. \tag{1.4.5}$$

Olkoon $x_2 = 1$. Silloin kongruenssi (1.4.5) tulee muotoon $3t \equiv -1 \pmod 3$, jolla ei ole ratkaisua. Siis kongruenssin $f(x) \equiv 0 \pmod 9$ ratkaisu $x_2 \equiv 1 \pmod 9$ ei tuota yhtään kongruenssin $f(x) \equiv 0 \pmod{27}$ ratkaisua.

Olkoon $x_2 = 4$. Silloin kongruenssi (1.4.5) tulee muotoon $9t \equiv -3 \pmod 3$. Kaikki luvut t, $0 \leq t < 3$, toteuttavat tämän kongruenssin, joten saadaan kongruenssin $f(x) \equiv 0 \pmod{27}$ ratkaisut $x_3 \equiv 4, 13, 22 \pmod{27}$.

Olkoon $x_2 = 7$. Silloin kongruenssi (1.4.5) tulee muotoon $15t \equiv -7 \pmod 3$, jolla ei ole ratkaisua. Siis kongruenssin $f(x) \equiv 0 \pmod 9$ ratkaisu $x_2 \equiv 7 \pmod 9$ ei tuota yhtään kongruenssin $f(x) \equiv 0 \pmod{27}$ ratkaisua.

Siis kaiken kaikkiaan kongruenssin $f(x) \equiv 0 \pmod{27}$ ratkaisut ovat $x_3 \equiv 4, 13, 22 \pmod{27}$.

1.5 Julkisen avaimen kryptausjärjestelmä RSA

Julkisen avaimen järjestelmä

Henkilöllä A on julkinen kryptausfunktio E_A (salausfunktio) ja salainen dekryptausfunktio D_A (purkufunktio). Oletetaan, että henkilö B lähettää viestin henkilölle A. Merkitään lähetettävän viestin selvätekstimuotoa kirjaimella w ja kryptotekstimuotoa kirjaimella c. Henkilö B kryptaa viestin w funktiolla E_A, jolloin siis $c = E_A(w)$, ja lähettää viestin muodossa c. Henkilö A purkaa viestin funktiolla D_A, jolloin hän saa viestin w. Siis $D_A(c) = w$. Tässä funktiot E_A ja D_A ovat toistensa käänteisfunktioita eli

$$D_A(c) = D_A(E_A(w)) = w. \tag{1.5.1}$$

RSA-järjestelmä

Julkinen kryptausfunktio E_A ja salainen dekryptausfunktio D_A laaditaan RSA-järjestelmässä seuraavalla tavalla. Valitaan kaksi (suurta) alkulukua p ja q ($p \neq q$). Lasketaan $n = pq$ ja $m = \phi(n) = (p-1)(q-1)$. Valitaan sellainen luku e, että $(e, m) = 1$. Luku d olkoon luvun e käänteisluku modulo m, ts. $de \equiv 1 \pmod m$. (Siis on olemassa sellainen kokonaisluku k, että $de = km + 1$.)

Henkilön A julkinen kryptausfunktio E_A on

$$E_A(w) = w^e \,\mathbf{mod}\, n$$

ja salainen dekryptausfunktio D_A on

$$D_A(c) = c^d \,\mathbf{mod}\, n.$$

Tällöin kaava (1.5.1) toteutuu, sillä

$$D_A(c) \equiv c^d \equiv (w^e)^d = w^{de} = w^{km+1} = (w^m)^k w \equiv w \pmod n,$$

missä viimeinen päättely perustuu Eulerin-Fermat'n lauseeseen. (Todennäköisyys, että Eulerin-Fermat'n lauseessa vaadittava ehto $(w, n) = 1$ ei ole voimassa, on äärimmäisen pieni.)

Henkilö voi vapaasti jakaa kryptausfunktionsa E_A, jonka pohjalta on äärimmäisen vaikea löytää dekryptausfunktio D_A. (Perustelu sivuutetaan.)

Esimerkki 1.5.1 Olkoon $p = 7$ ja $q = 11$. (Alkuluvut ovat pieniä yksinkertaisuuden vuoksi.) Silloin $n = pq = 77$ ja $m = \phi(n) = (p-1)(q-1) = 60$. Olkoon $e = 13$ (missä siis $(e, m) = 1$). Silloin henkilön A julkinen kryptausfunktio on

$$E_A(w) = w^{13} \,\mathbf{mod}\, 77.$$

Luku d toteuttaa kongruenssin $de \equiv 1 \pmod{m}$ eli kongruenssin $13d \equiv 1 \pmod{60}$. Tämän kongruenssin ratkaisu on $d \equiv 37 \pmod{60}$. (Totea!) Siis henkilön A salainen dekryptausfunktio D_A on

$$D_A(c) = c^{37} \,\mathbf{mod}\, 77.$$

Oletetaan, että viesti on $w = 3$. (Silloin $(w, n) = 1$.) Koska

$$w^{13} \equiv 3^{13} = 3^5(3^4)^2 = 243 \cdot 81^2 \equiv 12 \cdot 4^2 = 192 \equiv 38 \pmod{77},$$

niin viestin w kryptotekstimuoto on

$$c = E_A(w) = w^{13} \,\mathbf{mod}\, 77 = 38.$$

Puretaan c funktiolla $D_A(c) = c^{37} \,\mathbf{mod}\, 77$. Koska

$$\begin{aligned}
38^2 &= 1444 \equiv -19 \pmod{77}, \\
38^4 &\equiv (-19)^2 = 361 \equiv -24 \pmod{77}, \\
38^8 &\equiv (-24)^2 = 576 \equiv 37 \pmod{77}, \\
38^{16} &\equiv 37^2 = 1369 \equiv -17 \pmod{77}, \\
38^{32} &\equiv (-17)^2 = 289 \equiv -19 \pmod{77},
\end{aligned}$$

niin

$$\begin{aligned}
c^{37} &= 38^{37} = 38^{32} \cdot 38^4 \cdot 38 \equiv -19 \cdot (-24) \cdot 38 \\
&= 456 \cdot 38 \equiv -6 \cdot 38 = -228 \equiv 3 \pmod{77}.
\end{aligned}$$

Näin ollen

$$D_A(c) = c^{37} \,\mathbf{mod}\, 77 = 3 = w.$$

Allekirjoitus

Viestin allekirjoitus voidaan toteuttaa julkisen avaimen järjestelmässä. Oletetaan taas, että henkilö B lähettää viestin henkilölle A. Silloin B laskee muunnokset

$$D_B(w) = s,\ E_A(s) = c.$$

Viesti lähetetään muodossa c. Henkilö A purkaa sen laskemalla

$$D_A(c) = s,\ E_B(s) = w.$$

Siis A saa parin (s, w), jota voidaan pitää viestin allekirjoitettuna muotona. Nimittäin B ei voi kiistää lähettäneensä viestiä (s, w), sillä D_B on B:n salainen funktio ja täten vain B on voinut laskea luvun s luvusta w.

2 Primitiiviset juuret

2.1 Kokonaisluvun kertaluku

Olkoot a ja m (> 1) keskenään jaottomia kokonaislukuja. Silloin Eulerin-Fermat'n lauseen mukaan $a^{\phi(m)} \equiv 1 \pmod{m}$. Näin ollen on olemassa ainakin yksi sellainen positiivinen kokonaisluku x, että $a^x \equiv 1 \pmod{m}$.

Määritelmä Olkoot a ja m (> 1) keskenään jaottomia kokonaislukuja. Silloin luvun *a kertaluku modulo m* on on pienin sellainen positiivinen kokonaisluku x, että $a^x \equiv 1 \pmod{m}$. Merkitään $x = \mathrm{ord}_m a$.

Esimerkki 2.1.1 Etsitään $\mathrm{ord}_7 2$. Selvästi

$$2^1 \equiv 2 \pmod{7},\ 2^2 \equiv 4 \pmod{7},\ 2^3 \equiv 1 \pmod{7},$$

joten $\mathrm{ord}_7 2 = 3$. Vastaavasti voidaan perustella, että $\mathrm{ord}_7 3 = 6$. (Totea!)

Lause 2.1.1 *Olkoot a ja m* (> 0) *keskenään jaottomia. Silloin*

$$a^x \equiv 1 \pmod{m} \iff \mathrm{ord}_m a | x.$$

Todistus Jos $\mathrm{ord}_m a | x$, niin $x = (\mathrm{ord}_m a)k$, missä $k \in \mathbf{Z}^+$. Näin ollen

$$a^x = (a^{\mathrm{ord}_m a})^k \equiv 1^k = 1 \pmod{m}.$$

Oletetaan käänteisesti, että $a^x \equiv 1 \pmod{m}$. Jakoalgoritmin mukaan

$$x = (\mathrm{ord}_m a)q + r, \quad 0 \leq r < \mathrm{ord}_m a.$$

Näin ollen

$$a^x = a^{(\mathrm{ord}_m a)q + r} = a^{(\mathrm{ord}_m a)^q} a^r \equiv a^r \pmod{m}.$$

Koska $a^x \equiv 1 \pmod{m}$, niin $a^r \equiv 1 \pmod{m}$. Täten epäyhtälön $0 \leq r < \mathrm{ord}_m a$ ja luvun $\mathrm{ord}_m a$ määritelmän perusteella $r = 0$. Näin ollen $x = (\mathrm{ord}_m a)q + r = (\mathrm{ord}_m a)q$ eli $\mathrm{ord}_m a | x$. □

Esimerkki 2.1.2 Koska $\mathrm{ord}_7 2 = 3$ (ks. esim. 2.1.1), niin esimerkiksi $x = 9$ on kongruenssin $2^x \equiv 1 \pmod{7}$ ratkaisu mutta $x = 10$ ei ole kongruenssin $2^x \equiv 1 \pmod{7}$ ratkaisu.

Seuraus 2.1.1 *Jos a ja m (> 0) ovat keskenään jaottomia, niin* $\mathrm{ord}_m a | \phi(m)$.

Todistus Seuraus saadaan suoraan Eulerin-Fermat'n lauseesta ja lauseesta 2.1.1.

Esimerkki 2.1.3 Etsitään $\mathrm{ord}_9 7$. Koska $\phi(9) = 6$, niin lauseen 2.1.1 perusteella luvun $\mathrm{ord}_9 7$ mahdolliset arvot ovat $1, 2, 3$ ja 6. Selvästi

$$7^1 \equiv 7 \pmod{9}, \; 7^2 \equiv 4 \pmod{9}, \; 7^3 \equiv 1 \pmod{9},$$

joten $\mathrm{ord}_9 7 = 3$.

Lause 2.1.2 *Olkoot a ja m (> 0) keskenään jaottomia ja $i, j \geq 0$. Silloin*

$$a^i \equiv a^j \pmod{m} \iff i \equiv j \pmod{\mathrm{ord}_m a}.$$

Todistus Oletetaan, että $i \equiv j \pmod{\mathrm{ord}_m a}$. Menettämättä yleisyyttä voidaan olettaa, että $0 \leq j \leq i$. Silloin $i = j + k(\mathrm{ord}_m a)$, missä k on ei-negatiivinen kokonaisluku. Näin ollen

$$a^i = a^{j + k(\mathrm{ord}_m a)} = a^j (a^{\mathrm{ord}_m a})^k \equiv a^j \pmod{m}.$$

Oletetaan käänteisesti, että $a^i \equiv a^j \pmod{m}$, missä $0 \leq j \leq i$. Silloin

$$a^j a^{i-j} \equiv a^j \pmod{m}.$$

Koska $(a, m) = 1$, niin $(a^j, m) = 1$. Näin ollen supistussäännön perusteella $a^{i-j} \equiv 1 \pmod{m}$. Täten lauseen 2.1.1 mukaan $\mathrm{ord}_m a \mid (i - j)$ eli $i \equiv j \pmod{\mathrm{ord}_m a}$. □

Esimerkki 2.1.4 Esimerkin 2.1.3 mukaan $\mathrm{ord}_9 7 = 3$. Näin ollen lauseen 2.1.2 perusteella esimerkikisi

$$7^2 \equiv 7^5 \equiv 7^8 \pmod{9}, \; 7^2 \not\equiv 7^6 \pmod{9}.$$

Lause 2.1.3 *Jos* $\mathrm{ord}_m a = t$ *ja* u *on positiivinen kokonaisluku, niin*

$$\mathrm{ord}_m(a^u) = \frac{t}{(t, u)}.$$

Todistus Lause seuraa lauseesta 2.1.1 ja kaavasta $[t, u] = tu/(t, u)$.

Esimerkki 2.1.5 Esimerkin 2.1.1 mukaan $\mathrm{ord}_7 2 = 3$. Näin ollen lauseen 2.1.3 perusteella $\mathrm{ord}_7 2^5 = 3/(3, 5) = 3$.

2.2 Primitiivinen juuri

Määritelmä Olkoot r ja m (> 1) keskenään jaottomia kokonaislukuja. Jos $\mathrm{ord}_m r = \phi(m)$, niin sanotaan, että r on *primitiivinen juuri modulo* m.

Esimerkki 2.2.1 Koska $\phi(9) = 6$ ja $2^2 \equiv 4$, $2^3 \equiv 8$ ja $2^6 \equiv 1 \pmod{9}$, niin 2 on primitiivinen juuri modulo 9.

Esimerkki 2.2.2 Koska $\phi(7) = 6$, niin esimerkin 2.1.1 perusteella 3 on primitiivinen juuri modulo 7, mutta 2 ei ole primitiivinen juuri modulo 7.

Huomautus Kaikilla kokonaisluvuilla ei ole primitiivisiä juuria. Esimerkikisi ei ole primitiivisiä juuria modulo 8. Voidaan nimittäin osoittaa, että $\mathrm{ord}_8 1 = 1$ ja $\mathrm{ord}_8 3 = \mathrm{ord}_8 5 = \mathrm{ord}_8 7 = 2$, missä 1, 3, 5 ja 7 ovat luvun 8 kanssa suhteelliset alkuluvut (< 8), mutta $\phi(8) = 4$. *Voidaan todistaa, että on olemassa primitiivinen juuri modulo* m*, jos ja vain jos* $m = 2, 4, p^t, 2p^t$*, missä* p *on pariton alkuluku ja* t *positiivinen kokonaisluku.*

Lause 2.2.1 *Olkoot r ja m (> 1) keskenään jaottomia, ja olkoon r primitiivinen juuri modulo m. Silloin*

$$\{r^1, r^2, \ldots, r^{\phi(m)}\}$$

on supistettu jäännössysteemi modulo m.

Todistus Oletuksen mukaan $(r, m) = 1$. Näin ollen $(r^k, m) = 1$ aina, kun $k = 1, 2, \ldots, \phi(m)$. Vielä pitää osoittaa, että luvut $r^1, r^2, \ldots, r^{\phi(m)}$ pareittain epäkongruentteja modulo m. Oletetaan, että $r^i \equiv r^j \pmod{m}$. Lauseen 2.1.2 mukaan $i \equiv j \pmod{\phi(m)}$. Koska $1 \leq i, j \leq \phi(m)$, niin $i = j$. Näin ollen luvut $r^1, r^2, \ldots, r^{\phi(m)}$ ovat pareittain epäkongruentteja modulo m. □

Esimerkki 2.2.3 Esimerkin 2.2.1 ja lauseen 2.2.1 perusteella joukko $\{2^1, 2^2, \ldots, 2^{\phi(9)}\}$ eli joukko $\{2, 4, 8, 7, 5, 1\}$ on supistettu jäännössysteemi modulo 9.

Lause 2.2.2 *Olkoon r primitiivinen juuri modulo m. Silloin r^u on primitiivinen juuri modulo m, jos ja vain jos $(u, \phi(m)) = 1$.*

Todistus Lauseen 2.1.3 perusteella

$$\mathrm{ord}_m(r^u) = \frac{\mathrm{ord}_m r}{(\mathrm{ord}_m r, u)} = \frac{\phi(m)}{(\phi(m), u)}.$$

Näin ollen $\mathrm{ord}_m(r^u) = \phi(m)$ (eli r^u on primitiivinen juuri modulo m), jos ja vain jos $(u, \phi(m)) = 1$. □

Esimerkki 2.2.4 Esimerkin 2.2.1 mukaan luku 2 on primitiivinen juuri modulo 9. Koska $\phi(9) = 6$, niin lauseen 2.2.2 perusteella luvut 2 ja 2^5 ovat primitiivisiä juuria modulo 9.

Lause 2.2.3 *Jos on olemassa primitiivinen juuri modulo m, niin primitiivisten juurten modulo m kokonaislukumäärä on $\phi(\phi(m))$.*

Todistus Olkoon r primitiivinen juuri modulo m. Silloin lauseen 2.2.1 perusteella ehdokkaat primitiivisiksi juuriksi modulo m ovat $r^1, r^2, \ldots, r^{\phi(m)}$. Lauseen 2.2.2 mukaan r^u on primitiivinen juuri modulo m, jos ja vain jos $(u, \phi(m)) = 1$. Täten Eulerin funktion määritelmän nojalla primitiivisten juurten modulo m kokonaislukumäärä on $\phi(\phi(m))$. □

Esimerkki 2.2.5 Lauseen 2.2.3 ja esimerkin 2.2.4 perusteella luvut 2 ja 2^5 ovat ainoat primitiiviset juuret modulo 9.

2.3 Diskreetti logaritmi

Olkoon r primitiivinen juuri modulo m. Silloin lauseen 2.2.1 mukaan $\{r^1, r^2, \ldots, r^{\phi(m)}\}$ on supistettu jäännössysteemi modulo m. Siis jos a on suhteellinen alkuluku luvun m kanssa, niin on olemassa sellainen yksikäsitteinen luku x, että $1 \leq x \leq \phi(m)$ ja

$$r^x \equiv a \pmod{m}.$$

Määritelmä Olkoon r primitiivinen juuri modulo m. Olkoon a suhteellinen alkuluku luvun m kanssa. Silloin lukua x, joka toteuttaa ehdot $1 \leq x \leq \phi(m)$ ja $r^x \equiv a \pmod{m}$, sanotaan luvun a *r-kantaiseksi diskreetiksi logaritmiksi (eli indeksiksi) modulo* m. Silloin merkitään $x = \mathrm{ind}_r a$.

Huomautus 1) Luku $\mathrm{ind}_r a$ riippuu modulista m.

2) $r^{\mathrm{ind}_r a} \equiv a \pmod{m}$.

3) Olkoon $(a, m) = (b, m) = 1$. Silloin $a \equiv b \pmod{m}$, jos ja vain jos $\mathrm{ind}_r a = \mathrm{ind}_r b$, jos ja vain jos $\mathrm{ind}_r a \equiv \mathrm{ind}_r b \pmod{\phi(m)}$

Esimerkki 2.3.1 Olkoon $m = 7$. Esimerkissä 2.2.2 on todettu, että luku 3 on primitiivinen juuri modulo 7. Voidaan laskea, että $3^1 \equiv 3 \pmod{7}$, $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$, $3^4 \equiv 4 \pmod{7}$, $3^5 \equiv 5 \pmod{7}$, $3^6 \equiv 1 \pmod{7}$. Näin ollen $\mathrm{ind}_3 1 = 6, \mathrm{ind}_3 2 = 2, \mathrm{ind}_3 3 = 1, \mathrm{ind}_3 4 = 4, \mathrm{ind}_3 5 = 5, \mathrm{ind}_3 6 = 3$.

Lause 2.3.1 *Olkoon r primitiivinen juuri modulo m. Olkoot a ja b suhteellisia alkulukuja luvun m kanssa. Silloin*

(i) $\mathrm{ind}_r 1 \equiv 0 \pmod{\phi(m)}$,

(ii) $\mathrm{ind}_r(ab) \equiv \mathrm{ind}_r a + \mathrm{ind}_r b \pmod{\phi(m)}$,

(iii) $\mathrm{ind}_r(a^k) \equiv k \cdot \mathrm{ind}_r a \pmod{\phi(m)}$.

Todistus (i) Eulerin-Fermat'n lauseen mukaan $r^{\phi(m)} \equiv 1 \pmod{m}$. Koska r on primitiivinen juuri modulo m, niin mikään luvun r alempi potenssi ei ole kongruentti luvun 1 kanssa modulo m. Näin ollen $\mathrm{ind}_r 1 = \phi(m) \equiv 0 \pmod{\phi(m)}$.

(ii) Diskreetin logaritmin määritelmän perusteella

$$r^{\mathrm{ind}_r(ab)} \equiv ab \pmod{m}$$

ja

$$r^{\mathrm{ind}_r a} r^{\mathrm{ind}_r b} \equiv ab \pmod{m}.$$

Koska

$$r^{\mathrm{ind}_r a} r^{\mathrm{ind}_r b} = r^{\mathrm{ind}_r a + \mathrm{ind}_r b},$$

niin

$$r^{\mathrm{ind}_r(ab)} \equiv r^{\mathrm{ind}_r a + \mathrm{ind}_r b} \pmod{m}$$

Nyt lauseen 2.1.2 perusteella kohta (ii) on voimassa.

(iii) Kohta (iii) seuraa induktiolla kohdasta (ii). □

Esimerkki 2.3.2 Olkoon $m = 7$. Esimerkissä 2.3.1 on todettu, että $\mathrm{ind}_3 2 = 2$, $\mathrm{ind}_3 3 = 1$, $\mathrm{ind}_3 6 = 3$. Tämä sopii yhteen lauseen 2.3.1 kanssa, sillä $\mathrm{ind}_3 6 = \mathrm{ind}_3(2 \cdot 3) \equiv \mathrm{ind}_3 2 + \mathrm{ind}_3 3 = 2 + 1 = 3 \pmod{\phi(7)}$.

Esimerkki 2.3.3 Ratkaistaan diskreettien logaritmien avulla kongruenssi $6x^{12} \equiv 11 \pmod{17}$. Voidaan todistaa, että 3 on primitiivinen juuri modulo 17. (Totea!) Taulukossa 1 on esitetty 3-kantaiset diskreetit logaritmit modulo 17.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Taulukko 1: 3-kantaiset diskreetit logaritmit modulo 17.

Otetaan kongruenssin kummastakin puolesta 3-kantainen diskreetti logaritmi modulo 17, jolloin saadaan, että

$$\mathrm{ind}_3(6x^{12}) \equiv \mathrm{ind}_3 11 = 7 \pmod{16}.$$

(Huomaa, että yo. kongruenssissa moduli on nyt $\phi(17)$ eli 16 mutta 3-kantaisessa diskreetissä logaritmissa ind_3 moduli on 17.) Lauseen 2.3.1 kohtien (ii) ja (iii) perusteella

$$\text{ind}_3(6x^{12}) \equiv \text{ind}_3 6 + \text{ind}_3(x^{12}) \equiv 15 + 12 \cdot \text{ind}_3 x \pmod{16}.$$

Siis

$$15 + 12 \cdot \text{ind}_3 x \equiv 7 \pmod{16}$$

eli

$$12 \cdot \text{ind}_3 x \equiv 8 \pmod{16}.$$

Tämän lineaarisen kongruenssin ratkaisu on

$$\text{ind}_3 x \equiv 2 \pmod{4}.$$

(Totea!) Näin ollen

$$\text{ind}_3 x \equiv 2, 6, 10, 14 \pmod{16}.$$

Diskreetin logaritmin määritelmän nojalla

$$x \equiv 3^2, 3^6, 3^{10}, 3^{14} \pmod{17}$$

eli

$$x \equiv 9, 15, 8, 2 \pmod{17}.$$

Koska yo. laskennan jokainen vaihe on voimassa myös käänteisesti, niin on saatu kongruenssin $6x^{12} \equiv 11 \pmod{17}$ ratkaisu.

Esimerkki 2.3.4 Ratkaistaan diskreettien logaritmien avulla kongruenssi $7^x \equiv 6 \pmod{17}$. (Moduli on sama kuin esimerkissä 2.3.3.) Otetaan kongruenssin kummastakin puolesta 3-kantainen diskreetti logaritmi modulo 17, jolloin saadaan, että

$$\text{ind}_3(7^x) \equiv \text{ind}_3 6 = 15 \pmod{16}.$$

Lauseen 2.3.1 kohdan (iii) perusteella

$$\text{ind}_3(7^x) \equiv x \cdot \text{ind}_3 7 \equiv 11x \pmod{16}.$$

Siis

$$11x \equiv 15 \pmod{16}$$

Tämän lineaarisen kongruenssin ratkaisu on

$$x \equiv 13 \pmod{16}.$$

(Totea!) Tämä on kongruenssin $7^x \equiv 6 \pmod{17}$ ratkaisu, sillä yo. laskennan jokainen vaihe on voimassa myös käänteisesti.

2.4 Potenssin jäännös

Diskreettien logaritmien avulla voidaan tutkia kongruenssia $x^k \equiv a \pmod{m}$, missä m on positiivinen kokonaisluku, jolla on primitiivinen juuri, ja missä $(a, m) = 1$.

Määritelmä Olkoot m ja k positiivisia kokonaislukuja ja olkoon a suhteellinen alkuluku luvun m kanssa. Silloin sanotaan, että a on k. *potenssin jäännös modulo* m, jos kongruenssi

$$x^k \equiv a \pmod{m} \tag{2.4.1}$$

on ratkeava.

Lause 2.4.1 *Olkoon m positiivinen kokonaisluku, jolla on primitiivinen juuri, ja olkoon a suhteellinen alkuluku luvun m kanssa. Silloin kongruessi* (2.4.1) *on ratkeava, jos ja vain jos*

$$a^{\frac{\phi(m)}{(k,\phi(m))}} \equiv 1 \pmod{m}.$$

Jos kongruessi on ratkeava, niin ratkaisuja modulo m on täsmälleen $(k, \phi(m))$ kappaletta.

Todistus Olkoon r primitiivinen juuri modulo m. Kongruenssi (2.4.1) on voimassa, jos ja vain jos

$$k \cdot \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{\phi(m)}. \tag{2.4.2}$$

Merkitään $y = \operatorname{ind}_r x$. Jos $(k, \phi(m)) \nmid \operatorname{ind}_r a$, niin lineaarisella kongruenssilla

$$ky \equiv \operatorname{ind}_r a \pmod{\phi(m)} \tag{2.4.3}$$

ei ole ratkaisua y. Siis ei ole sellaista lukua x, että kongruenssi (2.4.2) toteutuisi. Jos $(k, \phi(m)) \mid \operatorname{ind}_r a$, niin lineaarisella kongruenssilla (2.4.3) on täsmälleen $(k, \phi(m))$

ratkaisua y modulo $\phi(m)$. Koska $x \equiv r^y \pmod{m}$, niin lauseen 2.1.2 nojalla kongruenssin (2.4.2) toteuttaa täsmälleen $(k, \phi(m))$ lukua x modulo m.

Olemme siis todistaneet, että kongruenssi (2.4.1) on ratkeava, jos ja vain jos $(k, \phi(m)) \mid \text{ind}_r a$. Tämä jaollisuus on voimassa, jos ja vain jos

$$\frac{\phi(m)}{(k, \phi(m))} \text{ind}_r a \equiv 0 \pmod{\phi(m)}$$

eli jos ja vain jos

$$a^{\frac{\phi(m)}{(k,\phi(m))}} \equiv 1 \pmod{m}.$$

□

Esimerkki 2.4.1 Tutkittava, onko kongruenssi $x^6 \equiv 5 \pmod{17}$ ratkeava eli onko luku 5 kuudennen potenssin jäännös modulo 17. Selvästi $5^{16/(6,16)} = 5^8 \equiv -1 \pmod{17}$, joten 5 ei ole kuudennen potenssin jäännös modulo 17.

3 Neliönjäännökset

3.1 Määritelmä

Määritelmä Olkoon m positiivinen kokonaisluku (≥ 2) ja a sellainen kokonaisluku, että $(a, m) = 1$. Silloin a on *neliönjäännös modulo* m, jos kongruenssi $x^2 \equiv a \pmod{m}$ on ratkeava, ja a on *neliönepäjäännös modulo* m, jos kongruenssi $x^2 \equiv a \pmod{m}$ ei ole ratkeava.

Esimerkki 3.1.1 Etsitään neliönjäännökset modulo 9. Asetetaan x käymään läpi supistettu jäännössysteemi modulo 9. Esimerkiksi x käy läpi luvut $\pm 1, \pm 2, \pm 4$. Tällöin x^2 on vastaavasti kongruentti lukujen $1, 4, 7$ kanssa modulo 9. Siis luvut $1, 4, 7$ ovat neliönjäännöksiä modulo 9 ja luvut $2, 5, 8$ ovat neliönepäjäännöksiä modulo 9.

Jatkossa rajoitutaan tapaukseen, jossa m on pariton alkuluku p.

Esimerkki 3.1.2 Etsitään neliönjäännökset modulo 11. Asetetaan x käymään läpi supistettu jäännössysteemi modulo 11. Esimerkiksi x käy läpi luvut $\pm 1, \pm 2, \pm 3, \pm 4, \pm 5$. Tällöin x^2 on vastaavasti kongruentti lukujen $1, 4, 9, 5, 3$ kanssa modulo 11. Siis luvut $1, 3, 4, 5, 9$ ovat neliönjäännöksiä modulo 11 ja luvut $2, 6, 7, 8, 10$ ovat neliönepäjäännöksiä modulo 11.

Lause 3.1.1 *Olkoon p pariton alkuluku ja r primitiivinen juuri modulo p. Olkoon a sellainen kokonaisluku, että $p \nmid a$. Silloin a on neliönjäännös modulo p, jos ja vain jos* $\mathrm{ind}_r a$ *on parillinen, ja a on neliönepäjäännös modulo p, jos ja vain jos* $\mathrm{ind}_r a$ *on pariton.*

Todistus Riittää todistaa neliönjäännöksiä koskeva väite. Olkoon a on neliönjäännös modulo p, ts. olkoon kongruenssi $x^2 \equiv a \pmod{p}$ ratkeava. Silloin $2 \cdot \mathrm{ind}_r x \equiv \mathrm{ind}_r a \pmod{p-1}$. Koska $p-1$ on parillinen, niin edellinen kongruenssi on voimassa modulo 2. Näin ollen $\mathrm{ind}_r a$ on parillinen.

Oletetaan käänteisesti, että $\mathrm{ind}_r a$ on parillinen. Merkitään $x = r^{\frac{\mathrm{ind}_r a}{2}}$. Silloin x toteuttaa kongruenssin $x^2 \equiv a \pmod{p}$, joten a on neliönjäännös modulo p. □

Seuraus Neliönjäännöksiä ja neliönepäjäännöksiä modulo p on kumpiakin $(p-1)/2$ kappaletta modulo p.

Lause 3.1.2 (Eulerin kriteeri) *Olkoon p pariton alkuluku, ja olkoon a sellainen kokonaisluku, että $p \nmid a$. Silloin a on neliönjäännös modulo p, jos ja vain jos*

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

ja a on neliönepäjäännös modulo p, jos ja vain jos

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

Todistus Todistetaan aluksi lauseen ensimmäinen osa. Oletetaan, että a on neliönjäännös modulo p. Silloin kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisu, sanokaamme x_1. Koska $(a, p) = 1$, niin $(x_1, p) = 1$. Näin ollen Fermat'n pienen lauseen perusteella

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

Oletetaan käänteisesti, että $a^{(p-1)/2} \equiv 1 \pmod{p}$. Olkoon r on primitiivinen juuri modulo p. Koska $(a, p) = 1$, niin $a \equiv r^k \pmod{p}$ jollakin luvun k arvolla, missä $1 \leq k \leq p-1$. Siis

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

Täten lauseen 2.1.1 mukaan $(\mathrm{ord}_p r) | k(p-1)/2$ eli $(p-1) | k(p-1)/2$. Siis k on parillinen, sanokaamme $k = 2j$. Nyt

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

joten r^j on kongruenssin $x^2 \equiv a \pmod{p}$ ratkaisu. Näin ollen a on neliönjäännös modulo p.

Todistetaan nyt lauseen toinen osa. Fermat'n pienen lauseen perusteella

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Siis

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

Nyt lauseen ensimmäisen osan perusteella saadaan lauseen toinen osa. □

Esimerkki 3.1.3 Olkoon $p = 11$. Silloin

$$2^{(11-1)/2} = 2^5 = 32 \equiv -1 \pmod{11}$$

ja

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

Siis 2 on neliönepäjäännös modulo 11 ja 3 on neliönjäännös modulo 11.

3.2 Legendren symboli

Määritelmä Olkoon $p\ (> 2)$ alkuluku ja a sellainen kokonaisluku, että $p \nmid a$. *Legendren symboli* $\left(\frac{a}{p}\right)$ määritellään kaavalla

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{jos } a \text{ on neliönjäännös modulo } p, \\ -1, & \text{jos } a \text{ on neliönepäjäännös modulo } p. \end{cases}$$

Esimerkki 3.2.1 Esimerkin 3.1.2 mukaan

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1,$$
$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1.$$

Lause 3.2.1 *Olkoon p pariton alkuluku, ja olkoot a ja b sellaisia kokonaislukuja, että $p \nmid a$ ja $p \nmid b$. Silloin*

(i) *jos $a \equiv b \pmod{p}$, niin $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,*

(ii) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$,

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Todistus (i) Jos $a \equiv b \pmod{p}$, niin kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisu, jos ja vain jos kongruenssilla $x^2 \equiv b \pmod{p}$ on ratkaisu. Näin ollen $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) Kohta (ii) seuraa lauseesta 3.1.2.

(iii) Kohdan (ii) perusteella

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Legendren symboli saa arvot ± 1. Siis jos $\left(\frac{ab}{p}\right) \neq \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, niin $1 \equiv -1 \pmod{p}$ eli $p|2$, mikä on mahdotonta, koska $p > 2$. Täten $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Esimerkki 3.2.2 Tutkitaan, onko kongruenssi $x^2 \equiv -5 \pmod{17}$ ratkeava. Lasketaan $\left(\frac{-5}{17}\right)$. Koska $-5 \equiv 12 \pmod{17}$, niin lauseen 3.2.1 kohdan i) perusteella $\left(\frac{-5}{17}\right) = \left(\frac{12}{17}\right)$. Lauseen 3.2.1 kohdan iii) perusteella

$$\left(\frac{12}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{4}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{2}{17}\right)^2 = \left(\frac{3}{17}\right)(\pm 1)^2 = \left(\frac{3}{17}\right).$$

Lauseen 3.2.1 kohdan ii) perusteella

$$\left(\frac{3}{17}\right) \equiv 3^{(17-1)/2} \equiv 3^8 \equiv (81)^2 \equiv (-4)^2 \equiv -1 \pmod{17}.$$

Näin ollen $\left(\frac{-5}{17}\right) = -1$ eli kongruenssi $x^2 \equiv -5 \pmod{17}$ ei ole ratkeava.

3.3 Neliönjäännösten resiprookkilaki

Lause 3.3.1 (Gaussin lemma) *Olkoon p pariton alkuluku, ja olkoon a sellainen kokonaisluku, että $p \nmid a$. Olkoon s joukon $\{a, 2a, \ldots, ((p-1)/2)a\}$ sellaisten alkioiden lukumäärä, joiden jakojäännös modulo p on suurempi kuin $p/2$. Silloin $\left(\frac{a}{p}\right) = (-1)^s$.*

Esimerkki 3.3.1 Lasketaan $\left(\frac{5}{11}\right)$ Gaussin lemman avulla. Lukujen $5, 2\cdot 5, 3\cdot 5, 4\cdot 5, 5\cdot 5$ jakojäännökset modulo 11 ovat $5, 10, 4, 9, 3$, joista kaksi on suurempaa kuin $11/2$. Näin ollen $\left(\frac{5}{11}\right) = (-1)^2 = 1$. (Toisin sanoen kongruenssi $x^2 \equiv 5 \pmod{11}$ on ratkeava.)

Lause 3.3.2 (Resiprookkilaki) *Olkoot p ja q erisuuria parittomia alkulukuja. Silloin*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Esimerkki 3.3.2 Lasketaan $\left(\frac{13}{17}\right)$. Resiprookkilain nojalla

$$\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right).$$

Lauseen 3.2.1 perusteella

$$\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)^2 = (\pm 1)^2 = 1.$$

Siis $\left(\frac{13}{17}\right) = 1$. Vastaus nähdään helposti myös lauseen 3.1.1 ja taulukon 1 avulla.

4 Aritmeettisia funktioita

4.1 Määritelmä

Määritelmä Reaaliarvoista (tai kompleksiarvoista) funktiota, jonka määrittelyjoukko on positiivisten kokonaislukujen joukko, sanotaan *aritmeettiseksi funktioksi*.

Esimerkki 4.1.1 Olkoon $\alpha \in \mathbf{R}$. Symbolilla N^α merkitään sellaista aritmeettista funktiota, että $N^\alpha(n) = n^\alpha$, kun $n \in \mathbf{Z}^+$. Erityisesti merkitään $N^1 = N$ ja $N^0 = \zeta$. Siis $N(n) = n$ ja $\zeta(n) = 1$, kun $n \in \mathbf{Z}^+$.

Esimerkki 4.1.2 Kirjaimella γ merkitään sellaista aritmeettista funktiota, että $\gamma(n) = \prod_{p|n} p$, kun $n > 1$. Lisäksi sovitaan, että $\gamma(1) = 1$.

Esimerkki 4.1.3 Kirjaimella ω merkitään sellaista aritmeettista funktiota, että $\omega(n) = \sum_{p|n} 1$, kun $n > 1$. Lisäksi sovitaan, että $\omega(1) = 0$.

Esimerkki 4.1.4 Kirjaimella Ω merkitään sellaista aritmeettista funktiota, että $\Omega(n) = \sum_{p|n} n(p)$, kun $n > 1$, missä $n = \prod_{p|n} p^{n(p)}$ on luvun n kanoninen esitys. Lisäksi sovitaan, että $\Omega(1) = 0$.

Esimerkki 4.1.5 *Liouvillen funktio* λ on sellainen aritmeettinen funktio, että $\lambda(n) = (-1)^{\Omega(n)}$, kun $n \in \mathbf{Z}^+$.

4.2 Binäärioperaatioita

Määritelmä Aritmeettisten funktioitten f ja g (tavallinen) summa $f+g$ on sellainen aritmeettinen funktio, että $(f+g)(n) = f(n)+g(n)$, kun $n \in \mathbf{Z}^+$.

Määritelmä Aritmeettisten funktioitten f ja g (tavallinen) tulo fg on sellainen aritmeettinen funktio, että $(fg)(n) = f(n)g(n)$, kun $n \in \mathbf{Z}^+$.

Määritelmä Aritmeettisten funktioitten f ja g *Dirichlet'n tulo* (eli Dirichlet'n konvoluutio) $f * g$ on sellainen aritmeettinen funktio, että

$$(f*g)(n) = \sum_{d|n} f(d)g(n/d),\ n \in \mathbf{Z}^+.$$

Lause 4.2.1 *Dirichlet'n tulo on assosiatiivinen.*

Todistus Dirichlet'n tulon määritelmän perusteella

$$\begin{aligned}((f*g)*h)(n) &= \sum_{dc=n}(f*g)(d)h(c) = \sum_{dc=n}\sum_{ab=d} f(a)g(b)h(c)\\ &= \sum_{abc=n} f(a)g(b)h(c) = \sum_{aD=n} f(a)\sum_{bc=D} g(b)h(c)\\ &= \sum_{aD=n} f(a)(g*h)(D) = (f*(g*h))(n)\ \forall n \in \mathbf{Z}^+.\end{aligned}$$

Näin ollen $(f*g)*h = f*(g*h)$ aina, kun f, g, h ovat aritmeettisia funktioita. Olemme siis todistaneet lauseen 4.2.1. □

Lause 4.2.2 *Dirichlet'n tulo on kommutatiivinen.*

Todistus Kun d käy läpi luvun n tekijät, niin myös n/d käy läpi luvun n tekijät. Tästä voimme päätellä lauseen 4.2.2. □

Määritelmä Kirjaimella δ merkitään sellaista aritmeettista funktiota, että $\delta(1) = 1$ ja $\delta(n) = 0$ muulloin.

Lause 4.2.3 *Aritmeettinen funktio δ on ykkösfunktio Dirichlet'n tulon suhteen.*

Todistus Koska $\delta(n/d) = 0$, kun $d \neq n$, ja koska $\delta(n/d) = 1$, kun $d = n$, niin

$$(f*\delta)(n) = \sum_{d|n} f(d)\delta(n/d) = f(n)\ \forall n \in \mathbf{Z}^+.$$

Kommutatiivisuuden nojalla $(\delta * f)(n) = f(n)\ \forall n \in \mathbf{Z}^+$. Näin ollen $f*\delta = \delta*f = f$ aina, kun f on aritmeettinen funktio. Olemme siis todistaneet lauseen 4.2.3. □

Lause 4.2.4 *Dirichlet'n tulo on distributiivinen yli tavallisen summan.*

Todistus Harjoitustehtävä.

Merkintä Kirjaimella $\mathcal{A}$ merkitään kaikkien aritmeettisten funktioitten joukkoa.

Lause 4.2.5 *Pari* $(\mathcal{A}, *)$ *on kommutatiivinen monoidi.*

Lause 4.2.6 *Kolmikko* $(\mathcal{A}, +, *)$ *on kommutatiivinen ykkösrengas.*

Lauseet 4.2.5 ja 4.2.6 seuraavat lauseista 4.2.1, 4.2.2, 4.2.3 ja 4.2.4.

Lause 4.2.7 *Aritmeettisella funktiolla* f *on käänteisfunktio* f^{-1} *Dirichlet'n tulon suhteen, jos ja vain jos* $f(1) \neq 0$*. Käänteisfunktio* f^{-1} *saadaan rekursiivisesta kaavasta*

$$f^{-1}(1) = \frac{1}{f(1)}, \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d>1}} f(d) f^{-1}(n/d), \ n > 1. \tag{4.2.1}$$

Todistus Oletetaan, että aritmeettisella funktiolla f on käänteisfunktio. Silloin $(f * f^{-1})(n) = \delta(n)$ aina, kun $n \in \mathbf{Z}^+$. Siis erityisesti $(f * f^{-1})(1) = \delta(1)$ eli $f(1)f^{-1}(1) = 1$. Näin ollen $f(1) \neq 0$.

Oletetaan käänteisesti, että $f(1) \neq 0$. Olkoon g sellainen aritmeettinen funktio, että $g(1) = 1/f(1)$ ja

$$g(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d>1}} f(d) g(n/d),$$

kun $n > 1$. Silloin selvästi $(f * g)(n) = \delta(n)$ aina, kun $n \in \mathbf{Z}^+$. Kommutatiivisuuden nojalla funktio g on funktion f käänteisfunktio Dirichlet'n tulon suhteen. □

Merkintä Symbolilla $\mathcal{A}_0$ merkitään kaikkien sellaisten aritmeettisten funktioitten f joukkoa, jotka toteuttavat ehdon $f(1) \neq 0$.

Lause 4.2.8 *Pari* $(\mathcal{A}_0, *)$ *on Abelin ryhmä.*

4.3 Multiplikatiiviset funktiot

Määritelmä Aritmeettista funktiota f sanotaan *multiplikatiiviseksi*, jos $f(1) = 1$ ja $f(mn) = f(m)f(n)$ aina, kun $(m, n) = 1$.

Esimerkki 4.3.1 Aritmeettiset funktiot $N^\alpha, \gamma, \lambda$ ja δ ovat multiplikatiivisia.

Lause 4.3.1 *Olkoon f sellainen aritmeettinen funktio, että $f(1) = 1$. Silloin f on multiplikatiivinen, jos ja vain jos*

$$f(n) = \prod_p f(p^{n(p)}) \ \forall n \in \mathbf{Z}^+,$$

missä $n = \prod_p p^{n(p)}$ on luvun n kanoninen esitys.

Todistus Harjoitustehtävä.

Lause 4.3.2 *Jos f ja g ovat multiplikatiivisia, niin $f * g$ on multiplikatiivinen.*

Todistus Selvästi $(f * g)(1) = 1$. Oletetaan, että $(m, n) = 1$. Jos nyt $d|mn$, niin d voidaan esittää muodossa $d = ab$, missä $a|m$ ja $b|n$. Silloin $(a, b) = (m/a, n/b) = 1$. Näin ollen

$$\begin{aligned}
(f * g)(mn) &= \sum_{d|mn} f(d)g(mn/d) = \sum_{\substack{a|m \\ b|n}} f(ab)g((m/a)(n/b)) \\
&= \sum_{\substack{a|m \\ b|n}} f(a)f(b)g(m/a)g(n/b) = \sum_{a|m} f(a)g(m/a) \sum_{b|n} f(b)g(n/b) \\
&= (f * g)(m)(f * g)(n).
\end{aligned}$$

Näin olemme todistaneet lauseen 4.3.2. □

Lause 4.3.3 *Jos f on multiplikatiivinen, niin f^{-1} on multiplikatiivinen.*

Todistus Selvästi $f^{-1}(1) = 1$. Oletetaan, että $(m, n) = 1$. Jos $mn = 1$, niin $f^{-1}(mn) = 1 = f^{-1}(m)f^{-1}(n)$. Oletetaan, että $mn \neq 1$ ja että $f^{-1}(m'n') = f^{-1}(m')f^{-1}(n')$

aina, kun $(m', n') = 1$ ja $m'n' < mn$. Jos $m = 1$ tai $n = 1$, niin $f^{-1}(mn) = f^{-1}(m)f^{-1}(n)$. Oletetaan, että $m, n \neq 1$. Kaavan (4.2.1) nojalla saadaan

$$\begin{aligned}
f^{-1}(mn) &= -\sum_{\substack{d \mid mn \\ d>1}} f(d)f^{-1}(mn/d) = -\sum_{\substack{a \mid m \\ b \mid n \\ ab>1}} f(ab)f^{-1}((m/a)(n/b)) \\
&= -\sum_{\substack{a \mid m \\ b \mid n \\ ab>1}} f(a)f(b)f^{-1}(m/a)f^{-1}(n/b) \\
&= -f^{-1}(m)\sum_{\substack{b \mid n \\ b>1}} f(b)f^{-1}(n/b) - f^{-1}(n)\sum_{\substack{a \mid m \\ a>1}} f(a)f^{-1}(m/a) \\
&\quad -\sum_{\substack{a \mid m \\ a>1}} f(a)f^{-1}(m/a)\sum_{\substack{b \mid n \\ b>1}} f(b)f^{-1}(n/b) \\
&= f^{-1}(m)f^{-1}(n) + f^{-1}(m)f^{-1}(n) - f^{-1}(m)f^{-1}(n) \\
&= f^{-1}(m)f^{-1}(n).
\end{aligned}$$

Näin olemme todistaneet lauseen 4.3.3. □

Merkintä Kirjaimella $\mathcal{M}$ merkitään kaikkien multiplikatiivisten funktioiden joukkoa.

Lause 4.3.4 *Pari* $(\mathcal{M}, *)$ *on Abelin ryhmä.*

Todistus Harjoitustehtävä.

4.4 Möbiuksen funktio

Määritelmä *Möbiuksen funktio* μ on sellainen multiplikatiivinen funktio, että

$$\mu(p^a) = \begin{cases} -1, & \text{kun } p \text{ on alkuluku ja } a = 1, \\ 0, & \text{kun } p \text{ on alkuluku ja } a > 1. \end{cases}$$

Lause 4.4.1 *Möbiuksen funktio* μ *on funktion* ζ *käänteisfunktio Dirichlet'n konvoluution suhteen, ts.* $\zeta^{-1} = \mu$.

Todistus Harjoitustehtävä. Vihje: Kommutatiivisuuden nojalla riittää todistaa, että $(\zeta * \mu)(n) = \delta(n)$, kun $n \in \mathbf{Z}^+$. Multiplikatiivisuuden nojalla riittää tutkia tapausta, jossa n on alkuluvun potenssi.

Lause 4.4.2 (Möbiuksen käänteiskaava) *Olkoot f ja g aritmeettisia funktioita. Silloin*

$$f(n) = \sum_{d|n} g(d) \ \forall n \in \mathbf{Z}^+ \iff g(n) = \sum_{d|n} f(d)\mu(n/d) \ \forall n \in \mathbf{Z}^+. \tag{4.4.1}$$

Todistus Yhtälö $f(n) = \sum_{d|n} g(d) \ \forall n \in \mathbf{Z}^+$ voidaan kirjoittaa Dirichlet'n tulon avulla muodossa $f = g * \zeta$. Kertomalla jälkimmäinen yhtälö oikealta puolittain Möbiuksen funktiolla μ saadaan yhtälö $f * \mu = (g * \zeta) * \mu$. Lauseiden 4.2.1 ja 4.4.1 perusteella saadaan yhtälö $f * \mu = g$, joka on sama kuin yhtälö $g(n) = \sum_{d|n} f(d)\mu(n/d) \ \forall n \in \mathbf{Z}^+$. □

4.5 Eulerin funktio

Määritelmä *Eulerin funktio* ϕ määritellään kaavalla

$$\phi(n) = |\{a : \ 1 \leq a \leq n, \ (a, n) = 1\}|, \ n \in \mathbf{Z}^+.$$

(Ks. §1.1.)

Lause 4.5.1 *Eulerin funktio ϕ toteuttaa kaavan $\phi = N * \mu$.*

Todistus Olkoon $n \in \mathbf{Z}^+$. Eulerin funktion määritelmä voidaan kirjoittaa muodossa

$$\phi(n) = \sum_{a=1}^{n} \delta((a, n)).$$

Lauseen 4.4.1 nojalla

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

Muuttamalla summausjärjestystä saadaan

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

Selvästi

$$\sum_{\substack{a=1 \\ d|a}}^{n} 1 = n/d.$$

(Totea!) Näin ollen

$$\phi(n) = \sum_{d|n} \mu(d)n/d = (\mu * N)(n) = (N * \mu)(n).$$

Siis $\phi = N * \mu$, joten olemme todistaneet lauseen 4.5.1. □

Seuraus Kun p on alkuluku ja $a \in \mathbf{Z}^+$, niin $\phi(p^a) = p^a - p^{a-1}$.

Lause 4.5.2 *Eulerin funktio ϕ on multiplikatiivinen.*

Todistus Lause 4.5.2 seuraa suoraan lauseista 4.5.1 ja 4.3.2. □

Seuraus Eulerin funktio ϕ toteuttaa kaavan

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \ n \in \mathbf{Z}^+.$$

4.6 Tekijäfunktio

Määritelmä Olkoon $\alpha \in \mathbf{R}$. *Tekijäfunktio σ_α* on sellainen aritmeettinen funktio, että

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

ts.

$$\sigma_\alpha = N^\alpha * \zeta.$$

Huomautus Tekijäfunktion arvo $\sigma_0(n)$ ilmaisee luvun n positiivisten tekijöiden lukumäärän, ja tekijäfunktion arvo $\sigma_1(n)$ ilmaisee luvun n positiivisten tekijöiden summan. Joskus merkitään lyhyesti $\sigma_0 = d$ ja $\sigma_1 = \sigma$, vrt. luku 5.

Lause 4.6.1 *Tekijäfunktio σ_α on multiplikatiivinen.*

Todistus Lause 4.6.1 seuraa suoraan tekijäfunktion määritelmästä ja lauseesta 4.3.2. □

4.7 Mangoldtin funktio

Määritelmä *Mangoldtin funktio* Λ määritellään kaavalla

$$\Lambda(n) = \begin{cases} \log p, & \text{kun } n = p^a, \text{ missä } a \geq 1, \\ 0 & \text{muulloin.} \end{cases}$$

Lause 4.7.1 *Kun* $n \geq 1$*, niin*

$$\log n = \sum_{d|n} \Lambda(d). \tag{4.7.1}$$

Todistus Lause on voimassa, kun $n = 1$. (Totea!) Oletetaan, että $n > 1$, ja kirjoitetaan $n = \prod_{k=1}^{r} p_k^{a_k}$. Silloin

$$\log n = \sum_{k=1}^{r} a_k \log p_k.$$

Tarkastellaan yhtälön (4.7.1) oikeaa puolta. Nollasta poikkeavat termit saadaan, kun d on muotoa p_k^m, missä $k = 1, 2, \ldots, r$ ja $m = 1, 2, \ldots, a_k$. Näin ollen

$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^{r} a_k \log p_k = \log n.$$

Näin olemme todistaneet lauseen 4.7.1. □

Lause 4.7.2 *Kun* $n \geq 1$*, niin*

$$\Lambda(n) = \sum_{d|n} \log(d)\mu(n/d) = \sum_{d|n} \mu(d) \log(n/d) = -\sum_{d|n} \mu(d) \log(d). \tag{4.7.2}$$

Todistus Lause 4.7.2 seuraa lauseesta 4.7.1 Möbiuksen käänteiskaavan avulla. □

Huomautus Mangoldtin funktio Λ ei ole multiplikatiivinen. (Totea!)

4.8 Täydellisesti multiplikatiiviset funktiot

Määritelmä Aritmeettista funktiota f sanotaan *täydellisesti multiplikatiiviseksi*, jos $f(1) = 1$ ja $f(mn) = f(m)f(n)$ aina, kun $m, n \in \mathbf{Z}^+$.

Huomautus Täydellisesti multiplikatiivinen funktio on multiplikatiivinen.

Esimerkki 4.8.1 Aritmeettiset funktiot N^α, δ ja λ ovat täydellisesti multiplikatiivisia.

Lause 4.8.1 *Multiplikatiivinen funktio f on täydellisesti multiplikatiivinen, jos ja vain jos*

$$f(p^a) = f(p)^a \tag{4.8.1}$$

aina, kun p on alkuluku ja $a \geq 1$.

Todistus Harjoitustehtävä.

Lause 4.8.2 *Multiplikatiivinen funktio f on täydellisesti multiplikatiivinen, jos ja vain jos*

$$f^{-1} = \mu f. \tag{4.8.2}$$

Todistus Oletetaan, että f on täydellisesti multiplikatiivinen. Silloin

$$(\mu f * f)(n) = \sum_{d|n} \mu(d) f(d) f(n/d) = f(n) \sum_{d|n} \mu(d) = f(n)\delta(n) = \delta(n).$$

Näin ollen $f^{-1} = \mu f$.

Oletetaan käänteisesti, että yhtälö (4.8.2) on voimassa. Todistetaan, että silloin yhtälö (4.8.1) on voimassa. Yhtälön (4.8.2) nojalla

$$\sum_{d|p^a} \mu(d) f(d) f(p^a/d) = 0$$

eli

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

Näin ollen

$$f(p^a) = f(p) f(p^{a-1}).$$

Jatkamalla induktiivisesti todetaan, että yhtälö (4.8.1) on voimassa. Koska funktio f on multiplikatiivinen, niin lauseen 4.8.1 perusteella funktio f on täydellisesti multiplikatiivinen. □

Lause 4.8.3 *Multiplikatiivinen funktio f on täydellisesti multiplikatiivinen, jos ja vain jos*

$$f(g * h) = (fg) * (fh) \tag{4.8.3}$$

aina, kun g ja h ovat aritmeettisia funktioita.

Todistus Harjoitustehtävä.

4.9 Muodollinen potenssisarja

Lukujonon $(a_k)_{k=0}^{\infty}$ *muodollinen potenssisarja* on lauseke

$$\sum_{k=0}^{\infty} a_k x^k. \tag{4.9.1}$$

Joskus jonon $(a_k)_{k=0}^{\infty}$ muodollista potenssisarjaa merkitään lyhyesti symbolilla $a(x)$, ts.

$$a(x) = \sum_{k=0}^{\infty} a_k x^k = a_0 + a_1 x + a_2 x^2 + \cdots \tag{4.9.2}$$

Kaavassa (4.9.2) symbolille x ei anneta lukuarvoja, vaan symbolin x potenssi ilmaisee kertoimensa paikan lukujonossa. Muodollinen potenssisarja on siis itse asiassa lukujonon uudenlainen esitysmuoto, jota on helppo käsitellä joissakin tilanteissa.

Jos lukujonon jokin jäsen a_k on $= 0$, niin termi $a_k x^k$ jätetään kaavan (4.9.2) oikeanpuoleisesta lausekkeesta pois, ja jos $a_k = 1$, niin silloin merkitään $a_k x^k = x^k$. Esimerkiksi jonon (3, 2, 1, 0, 0, ...) muodollinen potenssisarja on $3 + 2x + x^2$. Äärellinen jono $(a_0, a_1, a_2, \ldots, a_n)$ samaistetaan äärettömän jonon $(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ kanssa.

Selvästi

$$a(x) = b(x) \Leftrightarrow a_k = b_k, \quad k = 0, 1, 2, \ldots \tag{4.9.3}$$

Muodollisten potenssisarjojen summa ja tulo määritellään kaavoilla

$$a(x) + b(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k, \tag{4.9.4}$$

$$a(x)b(x) = \sum_{k=0}^{\infty} (\sum_{i=0}^{k} a_i b_{k-i}) x^k. \tag{4.9.5}$$

Tuloa kutsutaan myös Cauchyn tuloksi. Abstraktin algebran kielellä voidaan sanoa, että muodolliset potenssisarjat muodostavat kommutatiivisen ykkösrenkaan summan ja tulon suhteen. Renkaan ykkösalkio on sarja 1 eli sarja $1+0x+0x^2+\cdots$. Sillä on ominaisuus $a(x)1 = 1a(x) = a(x)$ aina, kun $a(x)$ on muodollinen potenssisarja. Muodollinen potenssisarja $b(x)$ on muodollisen potenssisarjan $a(x)$ inverssi, jos $a(x)b(x) = b(x)a(x) = 1$. Silloin merkitään $b(x) = a(x)^{-1} = 1/a(x)$. Voidaan todistaa, että muodollisella potenssisarjalla $a(x)$ on inverssi, jos ja vain jos $a_0 \neq 0$.

Esimerkki 4.9.1

$$\sum_{k=0}^{\infty} a^k x^k = \frac{1}{1 - ax},$$

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Määritelmä Olkoon p alkuluku. Aritmeettisen funktion f Bellin sarja $f_p(x)$ modulo p on muodollinen potenssisarja, joka määritellään kaavalla

$$f_p(x) = \sum_{k=0}^{\infty} f(p^k)x^k. \tag{4.9.6}$$

Esimerkki 4.9.2 Möbiuksen funktion μ Bellin sarjan modulo p antaa kaava

$$\mu_p(x) = 1 - x.$$

Esimerkki 4.9.3 Funktion N Bellin sarjan modulo p antaa kaava

$$N_p(x) = \frac{1}{1-px}.$$

(Totea!)

Esimerkki 4.9.4 Funktion ζ Bellin sarjan modulo p antaa kaava

$$\zeta_p(x) = \frac{1}{1-x}.$$

(Totea!)

Lause 4.9.1 *Olkoot f ja g multiplikatiivisia funktioita. Silloin $f = g$, jos ja vain jos $f_p(x) = g_p(x)$ aina, kun p on alkuluku.*

Todistus Harjoitustehtävä.

Lause 4.9.2 *Olkoot f ja g aritmeettisia funktioita. Silloin $(f * g)_p(x) = f_p(x)g_p(x)$ aina, kun p on alkuluku.*

Todistus Muodollisen potenssisarjan $(f*g)_p(x)$ potenssin x^k kerroin on $\sum_{d|p^k} f(d)g(p^k/d)$ eli $\sum_{i=0}^{k} f(p^i)g(p^{k-i})$, joka on myös muodollisen potenssisarjan $f_p(x)g_p(x)$ potenssin x^k kerroin. □

Esimerkki 4.9.5 Eulerin funktion ϕ Bellin sarjan modulo p antaa kaava

$$\phi_p(x) = \frac{1-x}{1-px}.$$

Huomautus Olkoot f, g ja h sellaisia multiplikatiivisia funktioita, että $h_p(x) = f_p(x)g_p(x)$ aina, kun p on alkuluku. Silloin $h = f * g$. (Totea!)

Esimerkki 4.9.6 Olkoon $\theta(n) = 2^{\omega(n)}$. Silloin θ on multiplikatiivinen ja

$$\theta_p(x) = \frac{1+x}{1-x}$$

aina, kun p on alkuluku. (Totea!) Näin ollen

$$\theta_p(x) = (\mu^2)_p(x)\zeta_p(x)$$

aina, kun p on alkuluku. Koska funktiot θ, μ^2 ja ζ ovat multiplikatiivisia, niin

$$\theta = \mu^2 * \zeta.$$

Lause 4.9.3 *Olkoon f sellainen aritmeettinen funktio, että $f(1) \neq 0$. Silloin $(f^{-1})_p(x) = \frac{1}{f_p(x)}$ aina, kun p on alkuluku.*

Todistus Harjoitustehtävä.

Esimerkki 4.9.7 Möbiuksen funktion μ käänteisfunktion Bellin sarjan modulo p antaa kaava

$$(\mu^{-1})_p(x) = \frac{1}{1-x} \ (= \zeta_p(x)).$$

Huomautus Olkoot f ja g sellaisia multiplikatiivisia funktioita, että $f_p(x)g_p(x) = 1$ aina, kun p on alkuluku. Silloin $g = f^{-1}$. (Totea!)

Esimerkki 4.9.8 Koska $(\mu^2)_p(x) = 1 + x$ ja $\lambda_p(x) = \frac{1}{1+x}$ aina, kun p on alkuluku (totea!), ja koska funktiot μ^2 ja λ ovat multiplikatiivisia, niin

$$\mu^2 = \lambda^{-1}.$$

4.10 Identiteettejä

Kaksi luontevaa tapaa todistaa aritmeettisia identiteettejä on käyttää apuna multiplikatiivisuutta ja Dirichlet'n tuloa. Havainnollistetaan asiaa kahdella esimerkillä.

Esimerkki 4.10.1 Todistetaan, että

$$\frac{n}{\phi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}. \tag{4.10.1}$$

Merkitään $L(n) = \frac{n}{\phi(n)}$ ja $R(n) = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}$. Silloin L ja R ovat multiplikatiivisia funktioita. Täten lauseen 4.3.1 nojalla yhtälö (4.10.1) riittää osoittaa oikeaksi, kun n on alkuluvun potenssi p^a, $a \geq 1$. Selvästi

$$L(p^a) = \frac{p^a}{p^a - p^{a-1}} = \frac{p}{p-1}$$

ja

$$R(p^a) = 1 + \frac{1}{p-1} = \frac{p}{p-1}.$$

Näin ollen yhtälö (4.10.1) on voimassa.

Esimerkki 4.10.2 Todistetaan, että

$$\sigma_1(n) = \sum_{d|n} \phi(d)\sigma_0(n/d). \tag{4.10.2}$$

Merkitään $R(n) = \sum_{d|n} \phi(d)\sigma_0(n/d)$. Silloin

$$R(n) = (\phi * \sigma_0)(n) = (N * \mu * \zeta * \zeta)(n).$$

Koska $\mu * \zeta = \delta$, missä δ on ykkösfunktio, niin

$$R(n) = (N * \zeta)(n) = \sigma_1(n).$$

Näin ollen yhtälö (4.10.2) on voimassa.

4.11 Analogioita ja yleistyksiä

Määritelmä Luvun n tekijää d sanotaan luvun n *unitaaritekijäksi*, jos $(d, n/d) = 1$. Jos d on luvun n unitaaritekijä, niin merkitään $d \| n$.

Esimerkki 4.11.1 Olkoon $n = p^a q^b$, missä p ja q ovat erisuuria alkulukuja. Silloin luvun n unitaaritekijät ovat 1, p^a, q^b ja n. Yleisesti, jos luvun n kanoninen esitys on $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, niin mitkä ovat luvun n unitaaritekijät?

Määritelmä Aritmeettisten funktioitten f ja g *unitaaritulo* (eli unitaarikonvoluutio) $f \oplus g$ on sellainen aritmeettinen funktio, että

$$(f \oplus g)(n) = \sum_{d \| n} f(d) g(n/d).$$

Lause 4.11.1 *Pari* $(\mathcal{A}_0, \oplus)$ *on Abelin ryhmä.*

Todistus Harjoitustehtävä. (Pitkä.)

Lause 4.11.2 *Pari* $(\mathcal{M}, \oplus)$ *on Abelin ryhmä.*

Todistus Harjoitustehtävä. (Pitkä.)

Määritelmä *Möbiuksen funktion unitaarianalogia* $\mu^{\oplus}$ on funktion ζ käänteisfunktio unitaaritulon suhteen.

Määritelmä Merkintä $(m, n)^{\oplus}$ tarkoittaa luvun m suurinta (tavallista) tekijää, joka on luvun n unitaaritekijä.

Esimerkki 4.11.2 Olkoon $m = p^2 q^2$ ja $n = p^3 q$, missä p ja q ovat erisuuria alkulukuja. Silloin $(m, n)^{\oplus} = q$.

Määritelmä *Eulerin funktion unitaarianalogia* $\phi^{\oplus}$ määritellään kaavalla

$$\phi^{\oplus}(n) = |\{a : \ 1 \le a \le n, \ (a, n)^{\oplus} = 1\}|.$$

Lause 4.11.3 *Eulerin funktion unitaarianalogia toteuttaa kaavan* $\phi^{\oplus} = N \oplus \mu^{\oplus}$.

Todistus Harjoitustehtävä.

Määritelmä Olkoon $u \in \mathbf{Z}^+$. *Jordanin funktio* J_u määritellään kaavalla

$$J_u(n) = |\{(a_1, a_2, \ldots, a_u) : \ 1 \leq a_1, a_2, \ldots, a_u \leq n, \ \text{syt}(a_1, a_2, \ldots, a_u, n) = 1\}|.$$

Huomautus Kun $u = 1$, niin $J_u = \phi$. Siis J_u on Eulerin funktion yleistys.

Lause 4.11.4 *Jordanin funktio toteuttaa kaavan* $J_u = N^u * \mu$.

Todistus Harjoitustehtävä.

Määritelmä Olkoon $K(n, d)$ reaaliarvoinen (tai kompleksiarvoinen) funktio sellaisten järjestettyjen parien (n, d) joukossa, missä $d|n$. Silloin aritmeettisten funktioitten f ja g *K-tulo* (eli K-konvoluutio) $f *_K g$ on sellainen aritmeettinen funktio, että

$$(f *_K g)(n) = \sum_{d|n} f(d)g(n/d)K(n, d).$$

Esimerkki 4.11.3 Dirichlet'n tulo ja unitaaritulo ovat K-tulon erikoistapauksia. (Totea!) Siis K-tulo on Dirichlet'n tulon ja unitaaritulon yleistys.

Määritelmä Aritmeettista funktiota f sanotaan *additiiviseksi*, jos $f(1) = 0$ ja $f(mn) = f(m) + f(n)$ aina, kun $(m, n) = 1$. Aritmeettista funktiota f sanotaan *täydellisesti additiiviseksi*, jos $f(1) = 0$ ja $f(mn) = f(m) + f(n)$ aina, kun $m, n \in \mathbf{Z}^+$.

Huomautus Täydellisesti additiivinen funktio on additiivinen.

Esimerkki 4.11.4 Funktio $\log n$ on täydellisesti additiivinen.

5 Aritmeettisen funktion keskiarvo

5.1 Määritelmä

Määritelmä Olkoon f aritmeettinen funktio. Olkoon g sellainen reaalimuuttujan funktio, että

$$\lim_{x \to \infty} \frac{\frac{1}{x} \sum_{n \leq x} f(n)}{g(x)} = 1.$$

Silloin sanotaan, että funktion $f(n)$ *keskiarvo* on $g(n)$.

Määritelmä Olkoon f aritmeettinen funktio. Jos

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

niin sanotaan, että osasumman $\sum\limits_{n\le x} f(n)$ *asymptoottinen arvo* on $g(x)$. Erotusta

$$\sum_{n\le x} f(n) - g(x)$$

sanotaan *virhetermiksi* ja merkitään symbolilla $E(x)$.

Virhetermi esitetään usein käyttämällä apuna $\mathcal{O}$–merkintää, joka määritellään seuraavassa.

Määritelmä Olkoon $g(x) > 0$, kun $x \ge 1$. Merkintä

$$f(x) = \mathcal{O}(g(x))$$

tarkoittaa, että on olemassa sellaiset vakiot M ja a, että

$$|f(x)| \le Mg(x), \text{kun } x \ge a.$$

Merkintä

$$f(x) = h(x) + \mathcal{O}(g(x))$$

tarkoittaa, että

$$f(x) - h(x) = \mathcal{O}(g(x)).$$

Esimerkki 5.1.1 Dirichlet'n kaavan mukaan

$$\sum_{n\le x} d(n) = x\log x + (2C-1)x + \mathcal{O}(\sqrt{x}), \quad x \ge 1, \tag{5.1.1}$$

missä C on Eulerin vakio, joka määritellään kaavalla

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

Näin ollen tekijäfunktion $d(n)$ keskiarvo on $\log n$, osasumman $\sum\limits_{n\le x} d(n)$ asymptoottinen arvo on $x\log x$ ja kaavan (5.1.1) mukainen virhetermi on

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

Dirichlet'n kaavan virhetermiä voidaan parantaa. Toistaiseksi paras arvio on Iwaniecin ja Mozzochin (1988) tulos

$$E(x) = (2C-1)x + \mathcal{O}\left(x^{\frac{7}{22}+\varepsilon}\right)$$

aina, kun $\varepsilon > 0$. Tässä monisteessa todistamme Dirichlet'n kaavaa heikomman tuloksen

$$\sum_{n\leq x} d(n) = x\log x + \mathcal{O}(x),$$

ks. lause 5.4.1.

5.2 Abelin identiteetti

Abelin identiteetin erikoistapauksena saadaan Eulerin summakaava, jota käytetään apuna joidenkin asymptoottisten kaavojen johtamisessa.

Lause 5.2.1 (Abelin identiteetti) *Olkoon $a(n)$ aritmeettinen funktio. Merkitään*

$$A(x) = \sum_{n\leq x} a(n),$$

missä $A(x) = 0$, kun $x < 1$. Olkoon f funktio, jolla on jatkuva derivaatta välillä $[y, x]$, missä $0 < y < x$. Silloin

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)\,\mathrm{dt}.$$

Todistus Merkitään $[x] = k$ ja $[y] = m$, jolloin $A(x) = A(k)$ ja $A(y) = A(m)$. Silloin

$$\begin{aligned}
\sum_{y<n\leq x} a(n)f(n) &= \sum_{n=m+1}^{k} a(n)f(n) = \sum_{n=m+1}^{k} \{A(n) - A(n-1)\}f(n) \\
&= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1) \\
&= \sum_{n=m+1}^{k-1} A(n)\{f(n) - f(n+1)\} + A(k)f(k) - A(m)f(m+1) \\
&= -\sum_{n=m+1}^{k-1} A(n) \int_n^{n+1} f'(t)\,\mathrm{dt} + A(k)f(k) - A(m)f(m+1)
\end{aligned}$$

$$
\begin{aligned}
&= -\sum_{n=m+1}^{k-1} \int_n^{n+1} A(t)f'(t)\,\mathrm{dt} + A(k)f(k) - A(m)f(m+1) \\
&= -\int_{m+1}^{k} A(t)f'(t)\,\mathrm{dt} + A(x)f(x) - \int_k^x A(t)f'(t)\,\mathrm{dt} \\
&\qquad -A(y)f(y) - \int_y^{m+1} A(t)f'(t)\,\mathrm{dt} \\
&= A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)\,\mathrm{dt}.
\end{aligned}
$$

Näin lause 5.2.1 on todistettu. □

Lause 5.2.2 (Eulerin summakaava) *Olkoon f funktio, jolla on jatkuva derivaatta välillä $[y, x]$, missä $0 < y < x$. Silloin*

$$\sum_{y<n\le x} f(n) = \int_y^x f(t)\,\mathrm{dt} + \int_y^x (t - [t])f'(t)\,\mathrm{dt} + f(x)([x] - x) - f(y)([y] - y).$$

Todistus Harjoitustehtävä. Vihje: Asetetaan Abelin identiteetissä $a = \zeta$.

Seuraavat perustulokset ovat Eulerin summakaavan seurauksia.

Merkintä Riemannin zeta-funktio $\zeta(s)$, $s \in \mathbf{R}^+$, määritellään kaavalla

$$\zeta(s) = \begin{cases} \sum\limits_{n=1}^{\infty} n^{-s}, & \text{kun } s > 1, \\ \lim\limits_{x\to\infty} \left(\sum\limits_{n\le x} n^{-s} - x^{1-s}/(1-s) \right), & \text{kun } 0 < s < 1. \end{cases}$$

Riemannin zeta-funktiolle käytetään samaa merkintää kuin aritmeettiselle funktiolle ζ, missä $\zeta(n) = 1$ aina, kun $n \in \mathbf{Z}^+$.

Lause 5.2.3 *Olkoon $x \ge 1$. Silloin*

(a) $\sum\limits_{n\le x} n^{-1} = \log x + C + \mathcal{O}(x^{-1})$.

(b) $\sum\limits_{n\le x} n^{-s} = \frac{x^{1-s}}{1-s} + \zeta(s) + \mathcal{O}(x^{-s})$, *kun* $s > 0$, $s \ne 1$.

(c) $\sum\limits_{n>x} n^{-s} = \mathcal{O}(x^{1-s})$, *kun* $s > 1$.

(d) $\sum\limits_{n\le x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + \mathcal{O}(x^\alpha)$, *kun* $\alpha \ge 0$.

Todistus (a) Asetetaan Eulerin summakaavassa $y = 1$ ja $f(t) = 1/t$. Silloin

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

On tunnettua, että epäoleellinen integraali $\int\limits_1^\infty t^{-2}\,\mathrm{dt}$ on olemassa. Täten majoranttiperiaatteen nojalla epäoleellinen integraali $\int\limits_1^\infty (t-[t])t^{-2}\,\mathrm{dt}$ on olemassa. Lisäksi

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

Näin ollen

$$\sum_{n\le x}\frac{1}{n} = \log x + 1 - \int_1^\infty \frac{t-[t]}{t^2}\,\mathrm{dt} + \mathcal{O}\left(\frac{1}{x}\right). \tag{5.2.1}$$

Kun $x \to \infty$, niin saamme

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

Siis yhtälö (5.2.1) todistaa kohdan (a).

(b) Asetetaan nyt Eulerin summakaavassa $y = 1$ ja $f(t) = t^{-s}$, missä $s > 0$, $s \ne 1$. Silloin

$$\begin{aligned}\sum_{n\le x}\frac{1}{n^s} &= \int_1^x \frac{1}{t^s}\,\mathrm{dt} - s\int_1^x \frac{t-[t]}{t^{s+1}}\,\mathrm{dt} + 1 - \frac{x-[x]}{x^s}\\ &= \frac{x^{1-s}}{1-s} - \frac{1}{1-s} + 1 - s\int_1^\infty \frac{t-[t]}{t^{s+1}}\,\mathrm{dt} + \mathcal{O}\left(x^{-s}\right).\end{aligned}$$

Siis

$$\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + C(s) + \mathcal{O}\left(x^{-s}\right), \tag{5.2.2}$$

missä

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

Jos $s > 1$, niin yhtälön (5.2.2) vasen puoli lähestyy lukua $\zeta(s)$ ja termit x^{1-s} ja x^{-s} lähestyvät lukua 0, kun $x \to \infty$. Näin ollen $C(s) = \zeta(s)$, kun $s > 1$. Jos $0 < s < 1$, niin $x^{-s} \to 0$ ja (5.2.2) osoittaa, että

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

Näin ollen $C(s) = \zeta(s)$, kun $0 < s < 1$. Siis $C(s) = \zeta(s)$ aina, kun $s > 0$, $s \neq 1$, ja täten yhtälö (5.2.2) todistaa kohdan (b).

(c) Olkoon $s > 1$. Silloin

$$\sum_{n>x}\frac{1}{n^s} = \zeta(s) - \sum_{n\le x}\frac{1}{n^s}.$$

Kohdan (b) mukaan

$$\zeta(s) - \sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{s-1} + \mathcal{O}\left(x^{-s}\right).$$

Koska $x^{-s} \le x^{1-s}$, niin

$$\frac{x^{1-s}}{s-1} + \mathcal{O}\left(x^{-s}\right) = \mathcal{O}\left(x^{1-s}\right).$$

Yhdistämällä yo. yhtälöt saamme kohdan (c).

(d) Asetetaan Eulerin summakaavassa $y = 1$ ja $f(t) = t^\alpha$, $\alpha \ge 0$. Silloin

$$\begin{aligned}\sum_{n\le x} n^\alpha &= \int_1^x t^\alpha\,\mathrm{dt} + \alpha\int_1^x t^{\alpha-1}(t-[t])\,\mathrm{dt} + 1 - (x-[x])x^\alpha \\ &= \frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + \mathcal{O}\left(\alpha\int_1^x t^{\alpha-1}\,\mathrm{dt}\right) + \mathcal{O}\left(x^\alpha\right) \\ &= \frac{x^{\alpha+1}}{\alpha+1} + \mathcal{O}\left(x^\alpha\right),\end{aligned}$$

mikä todistaa kohdan (d). Näin lause 5.2.3 on todistettu. □

5.3 Dirichlet'n tulon osasumma

Tässä pykälässä esitetään aputulos (lause 5.3.2), joka auttaa sellaisten aritmeettisten funktioiden asymptoottisen käyttäytymisen tutkimisessa, jotka ovat kahden sopivan funktion Dirichlet'n tuloja.

Määritelmä Olkoon F reaalimuuttujan x (≥ 1) funktio ja olkoon f aritmeettinen funktio. Silloin määritellään

$$(f \circ F)(x) = \sum_{n \leq x} f(n)F(x/n), \quad x \geq 1.$$

Huomautus Jos $F(x) = 0$, kun x ei ole positiivinen kokonaisluku, niin

$$(f \circ F)(m) = (f * F)(m),$$

kun $m \in \mathbf{Z}^+$.

Lause 5.3.1 *Jos f ja g ovat aritmeettisia funktioita, niin*

$$f \circ (g \circ F) = (f * g) \circ F.$$

Todistus Harjoitustehtävä.

Lause 5.3.2 *Olkoon $h = f * g$ ja merkitään*

$$H(x) = \sum_{n \leq x} h(n), \quad F(x) = \sum_{n \leq x} f(n), \quad G(x) = \sum_{n \leq x} g(n).$$

Silloin

$$H(x) = \sum_{n \leq x} f(n)G(x/n) = \sum_{n \leq x} g(n)F(x/n).$$

Todistus Merkitään $U(x) = 1$, $x \geq 1$. Silloin

$$H = h \circ U = (f * g) \circ U, \quad F = f \circ U, \quad G = g \circ U.$$

Täten lauseen 5.3.1 nojalla

$$H = (f * g) \circ U = f \circ (g \circ U) = f \circ G$$

eli

$$H(x) = \sum_{n \leq x} f(n)G(x/n).$$

Koska $f * g = g * f$, niin

$$H = (g * f) \circ U = g \circ (f \circ U) = g \circ F$$

eli

$$H(x) = \sum_{n \leq x} g(n)F(x/n).$$

Näin olemme todistaneet lauseen 5.3.2. □

5.4 Tekijäfunktion keskiarvo

Lause 5.4.1

$$\sum_{n\le x} d(n) = x\log x + \mathcal{O}(x).$$

Todistus Asetetaan lauseessa 5.3.2 $f = g = \zeta$, jolloin $h = d$. Näin ollen

$$\sum_{n\le x} d(n) = \sum_{n\le x}\sum_{m\le x/n} 1.$$

Lauseen 5.2.3 kohtien (d) ja (a) nojalla

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

Olemme siis todistaneet lauseen 5.4.1. □

Huomautus Funktion $d(n)$ keskiarvo on $\log n$.

Lause 5.4.2 *Kun* $x \ge 1$,

$$\sum_{n\le x}\sigma_1(n) = \frac{1}{2}\zeta(2)x^2 + \mathcal{O}(x\log x).$$

Todistus Asetetaan lauseessa 5.3.2 $f = N$ ja $g = \zeta$. Silloin

$$\sum_{n\le x}\sigma_1(n) = \sum_{n\le x}\sum_{m\le x/n} m.$$

Lauseen 5.2.3 kohtien (d) ja (b) nojalla

$$\begin{aligned}\sum_{n\le x}\sigma_1(n) &= \sum_{n\le x}\left\{\frac{1}{2}(x/n)^2 + \mathcal{O}(x/n)\right\}\\ &= \frac{1}{2}x^2\sum_{n\le x} n^{-2} + \mathcal{O}\left(x\sum_{n\le x} n^{-1}\right)\\ &= \frac{1}{2}x^2\left\{-x^{-1} + \zeta(2) + \mathcal{O}\left(x^{-2}\right)\right\} + \mathcal{O}(x\log x)\\ &= \frac{1}{2}\zeta(2)x^2 + \mathcal{O}(x\log x).\end{aligned}$$

Näin olemme todistaneet lauseen 5.4.2. □

Huomautus Voidaan todistaa, että $\zeta(2) = \pi^2/6$. Näin ollen funktion $\sigma(n)$ keskiarvo on $\pi^2 n/12$.

Lause 5.4.3 *Jos $x \geq 1$ ja $\alpha > 0$, $\alpha \neq 1$, niin*

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

missä $\beta = \max\{1, \alpha\}$.

Todistus Harjoitustehtävä.

Lause 5.4.4 *Olkoon $\beta > 0$ ja merkitään $\delta = \max\{0, 1-\beta\}$. Jos $x > 1$, niin*

$$\sum_{n \leq x} \sigma_{-\beta}(n) = \begin{cases} \zeta(\beta+1)x + \mathcal{O}\left(x^\delta\right), & \text{kun } \beta \neq 1, \\ \zeta(2)x + \mathcal{O}(\log x), & \text{kun } \beta = 1. \end{cases}$$

Todistus Harjoitustehtävä.

5.5 Eulerin funktion keskiarvo

Apulause 5.5.1

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Todistus Sivuutetaan.

Lause 5.5.1

$$\sum_{n \leq x} \varphi(n) = \frac{3}{\pi^2} x^2 + \mathcal{O}(x \log x).$$

Todistus Asetetaan lauseessa 5.3.2 $f = \mu$ ja $g = N$, jolloin $h = \varphi$. Näin ollen lauseen 5.2.3 kohtien (d) ja (a) nojalla

$$\begin{aligned} \sum_{n \leq x} \varphi(n) &= \sum_{n \leq x} \mu(n) \sum_{m \leq x/n} m \\ &= \sum_{n \leq x} \mu(n) \left(\frac{1}{2} \left(\frac{x}{n} \right)^2 + \mathcal{O}\left(\frac{x}{n} \right) \right) \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2}x^2 \sum_{n\le x} \mu(n)/n^2 + \mathcal{O}\left(x \sum_{n\le x} \frac{1}{n}\right) \\
&= \frac{1}{2}x^2 \sum_{n\le x} \mu(n)/n^2 + \mathcal{O}(x \log x).
\end{aligned}
$$

Apulauseen 5.5.1 ja lauseen 5.2.3 kohdan (c) avulla saadaan

$$
\begin{aligned}
\sum_{n\le x} \frac{\mu(n)}{n^2} &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} - \sum_{n>x} \frac{\mu(n)}{n^2} \\
&= \frac{6}{\pi^2} + \mathcal{O}\left(\sum_{n>x} \frac{1}{n^2}\right) \\
&= \frac{6}{\pi^2} + \mathcal{O}\left(\frac{1}{x}\right).
\end{aligned}
$$

Siis

$$
\begin{aligned}
\sum_{n\le x} \varphi(n) &= \frac{1}{2}x^2 \left(\frac{6}{\pi^2} + \mathcal{O}\left(\frac{1}{x}\right)\right) + \mathcal{O}(x \log x) \\
&= \frac{3}{\pi^2}x^2 + \mathcal{O}(x \log x).
\end{aligned}
$$

Näin olemme todistaneet lauseen 5.5.1. □

Huomautus Funktion $\varphi(n)$ keskiarvo on $3n/\pi^2$.

Huomautus On tunnettua, että

$$
\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} \mu(n) = 0. \tag{5.5.1}
$$

Tällöin sanotaan, että Möbiuksen funktion $\mu(n)$ keskiarvo on $= 0$.

Voidaan todistaa, että (5.5.1) on yhtäpitävä ns. alkulukulauseen kanssa. Alkulukulauseen mukaan

$$
\lim_{x\to\infty} \frac{\pi(x) \log x}{x} = 1,
$$

missä $\pi(x) = |\{p : \ p \le x, \ \ p \text{ alkuluku}\}|$. Alkulukulauseen todistus on vaikea.