Jaottomat polynomit

LuK-tutkielma
Johanna Hynynen
Y62368534
Matemaattisten tieteiden laitos
Oulun yliopisto
Syksy 2022

Sisällys

Johdanto

Käsittelen tutkielmassani jaottomia polynomeja. Ensin määrittelen polynomien suurimman yhteisen tekijän käsitteen, ja sen jälkeen käsittelen Eukleideen algoritmia, jota voidaan käyttää kahden polynomin suurimman yhteisen tekijän löytämiseen. Sen jälkeen Eukleideen algoritmin pohjalta todistan, että jokainen polynomi voidaan jakaa yksikäsitteisesti jaottomiin tekijöihin. Tämän jälkeen esittelen ja todistan erilaisia jaottomuuskriteereitä. Todistan, että kokonaislukukertoiminen polynomi on jaoton kokonaislukujen renkaassa jos ja vain jos se on jaoton rationaalilukujen renkaassa. Sitten todistan Eisensteinin kriteerin. Todistan, että kaikki muotoa $x^4+ax^2+b^2$, $a, b \in \mathbb{Z}$ olevat polynomit ovat jaollisia kaikkien alkulukujen jäännösluokissa. Todistan, että mikäli polynomi on jaoton mikäli se saavuttaa tarpeeksi pienen arvon tarpeeksi monessa eri kohdassa. Viimeiseksi käsittelen muotoa $x^n \pm x^m \pm x^p \pm 1$ olevien polynomien jaottomuutta, ja todistan lauseen jonka mukaan tätä muotoa oleva polynomi on jaoton mikäli sillä ei ole sellaisia juuria, jotka voidaan johonkin kokonaislukupotenssiin korottamalla saada ykköseksi. Tässä kandidaattitutkielmassa olen käyttänyt lähteenä teosta [1].

1 Polynomien jaottomuus

Määritelmä 1.1. Kunnassa K astetta n oleva polynomi on

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

missä $a_0, a_1, a_2, \ldots, a_n \in K$, $a_n \neq 0$ ja x on muuttuja.

Määritelmä 1.2. Olkoot f ja g saman muuttujan polynomeja samassa kunnassa. Polynomi f on *jaollinen polynomilla* g, mikäli $f = gh$, missä h on polynomi.

2 Polynomien jakaminen jaottomiin tekijöihin

2.1 Eukleideen algoritmi

Eräitä tärkeimmistä jaottomista polynomeista ovat polynomien jaottomat tekijät. Tässä kappaleessa osoitetaan, että kaikki polynomit voidaan yksikäsitteisesti jakaa jaottomiin tekijöihin.

Määritelmä 2.1. Polynomia d kutsutaan polynomien f ja g *yhteiseksi tekijäksi*, mikäli molemmat polynomit f ja g ovat jaollisia polynomilla d.

Määritelmä 2.2. Polynomien f ja g yhteinen tekijä d on niiden *suurin yhteinen tekijä*, mikäli se jakaa kaikki muut polynomien f ja g yhteiset tekijät. Polynomien f ja g suurinta yhteistä tekijää merkitään syt(f, g)

Kahden polynomin suurin yhteinen tekijä on mahdollista löytää Eukleideen algoritmilla.

Eukleideen algoritmi toimii seuraavasti. Olkoon f ja g saman muuttujan polynomeja samassa kunnassa. Oletetaan, että $\deg f > \deg g$. Olkoon r_1 jakojäännös, kun polynomi f jaetaan polynomilla g, r_2 jakojäännös kun polynomi g jaetaan jakojäännöksellä r_1, ja jokaisella $k = 1, 2, 3, \ldots$ polynomi r_{k+1} on jakojäännös, kun jakojäännös r_{k-1} jaetaan jakojäännöksellä r_k. Tällöin jakojäännöksien asteille $k = 1, 2, 3, \ldots$ pätee $\deg r_{k+1} < \deg r_k$, sillä polynomeja jaettaessa jakojäännös on aina asteeltaan pienempi kuin jakaja. Näin ollen on välttämättäkin olemassa sellainen n, että $r_{n+1} = 0$. Tämä johtuu siitä, että koska jakojäännöksien aste aina pienenee, niin lopulta on tultava tilanne jossa jakojäännös on nollapolynomi, sillä muuten jakojäännöksen aste olisi sama kuin jakajan. Nyt selvästikin r_n jakaa jakojäännöksen r_{n-1}, sillä tämän jakolaskun jakojäännös on 0. Tällöin $r_{n-1} = p_1 r_n$ jollakin polynomilla p_1. Lisäksi

$$r_{n-2} = p_2 r_{n-1} + r_n = p_2 p_1 r_n + r_n = (p_1 p_2 + 1) r_n$$

jollakin p_2, ja näin ollen r_{n-2} on jaollinen jakojäännöksellä r_n. Tällöin

$$r_{n-3} = p_3 r_{n-2} + r_{n-1} = p_3(p_1 p_2 + 1) r_n + p_1 r_n = (p_1 p_2 p_3 + p_1 + p_3) r_n$$

jollakin p_3, ja näin ollen r_{n-3} on jaollinen jakojäännöksellä r_n. Kun tätä jatketaan, nähdään että r_n jakaa kaikki jakojäännökset $r_{n-1}, r_{n-2}, \ldots$. Näin ollen se jakaa myös polynomit f ja g.

Osoitetaan vielä, että jos molemmat f ja g ovat jaollisia polynomilla h, eli h on polynomien f ja g yhteinen tekijä, niin tällöin myös r_n on oltava

jaollinen polynomilla h. Mikäli Eukleideen algoritmia tarkastellaan toiseen suuntaan, nähdään että

$$r_n = p_2 r_{n-1} - r_{n-2},\ r_{n-1} = p_3 r_{n-2} - r_{n-3},\ \ldots,\ r_1 = p_n g - f.$$

Siispä on oltava olemassa sellaiset luvut a ja b, että r_n voidaan esittää muodossa $r_n = af + bg$. Mikäli h jakaa molemmat polynomit f ja g, on olemassa sellaiset c ja d että $f = ch$ ja $g = dh$. Tällöin

$$r_n = af + bg = ach + bdh = (ac + bd)h,$$

ja näin ollen r_n on jaollinen polynomilla h.

Esimerkki 2.3. Etsitään polynomien $f(x) = x^3 + 5x^2 - 29x - 105$ ja $g(x) = x^2 - 4x - 5$ suurin yhteinen tekijä. Nyt

$$x^3 + 5x^2 - 29x - 105 = (x + 9)(x^2 - 4x - 5) + (12x - 60),$$

eli jakojäännökseksi saadaan $12x - 60$. Otetaan tästä kerroin 12 ulos, jolloin saadaan $12x - 60 = 12(x - 5)$. Merkitään nyt $r_1 = x - 5$. Nyt

$$x^2 - 4x - 5 = (x + 1)(x - 5).$$

Näin ollen $r_2 = 0$ ja $\text{syt}(f, g) = x - 5$.

Euklideen algoritmista saadaan tärkeä seuraus, joka esitetään seuraavassa lauseessa.

Lause 2.4. *Jos d on polynomien f ja g suurin yhteinen tekijä, niin tällöin on olemassa sellaiset polynomit a ja b, että $d = af + bg$.*

Lause seuraa suoraan Eukleideen algoritmista.

Määritelmä 2.5. Olkoon f polynomi, jonka kaikki kertoimet ovat renkaasta K. Sitä kutsutaan *jaolliseksi* renkaassa K mikäli $f = gh$, jossa g ja h ovat asteeltaan positiivisia polynomeja, joiden kertoimet ovat renkaasta K. Muuten f on *jaoton* renkaassa K.

Määritelmä 2.6. *Pääpolynomi* on polynomi, jonka asteeltaan suurimman termin kerroin on 1.

Olkoon $f = f_1 \cdot \ldots \cdot f_s$ polynomin f tekijöihin jako kunnassa K tekijöihin $f_1, \ldots, f_s$, jotka ovat polynomeja kunnassa K. Tästä mielivaltaiset kertoimet omaavasta tekijöihin jaosta voidaan muodostaa tekijöihin jako, joka koostuu pääpolynomeista. Kun $f_i = a_i x^i + \ldots$ on polynomi kunnassa K, niin tällöin $g_i = \frac{f_i}{a_i}$ on pääpolynomi kunnassa k, sillä sen asteeltaan suurimman termin kerroin on $\frac{a_i}{a_i} = 1$. Näin ollen voimme korvata tekijöihin jaon $f = f_1 \cdot \ldots \cdot f_s$ tekijöihin jaolla $f = a g_1 \cdot \ldots \cdot g_s$, jossa $a = a_1 \cdot \ldots \cdot a_s$. Kahta tekijöihin jakoa pidetään samana, mikäli ne eroavat toisistaan vain tekijöiden järjestyksellä.

Lemma 2.7. *Mikäli polynomi qr on jaollinen millä tahansa jaottomalla polynomilla p, niin tällöin joko q tai r on jaollinen polynomilla p.*

Todistus. Oletetaan, että polynomi q ei ole jaollinen polynomilla p. Tällöin $\text{syt}(p, q) = 1$, eli Lauseen 2.4 mukaan on olemassa sellaiset polynomit a ja b, että $ap+bq = 1$. Kun tämän yhtälön molemmat puolet kerrotaan polynomilla r, niin tällöin saadaan yhtälö $apr + bqr = r$. Nyt polynomit pr ja qr ovat jaollisia polynomilla p, ja näin ollen kahden polynomilla p jaollisen polynomin summana myös polynomi r on jaollinen polynomilla p. □

Lause 2.8. *Olkoon K kunta. Tällöin polynomi $f \in K[x]$ voidaan jakaa jaottomiin tekijöihin. Tällainen tekijöihin jako on yksikäsitteinen. Se voidaan siis yksikäsitteisesti esittää tiettyjen pääpolynomien ja vakion tulona.*

Todistus. Tällaisen tekijöihin jaon olemassaolo voidaan todistaa induktiolla asteen $n = \deg f$ suhteen. Huomioidaan ensin, että mikäli f on jaoton polynomi, haluttu tekijöihin jako on polynomi f itsessään. Koska f on jaoton, on tämä tekijöihin jako selvästi jako jaottomiin tekijöihin. Lisäksi jako on selkeästi yksikäsitteinen.

Kun $n = 1$, niin tällöin polynomi f on jaoton, sillä sitä on mahdotonta esittää kahden pienempää astetta olevan polynomin tulona. Olkoon nyt tekijöihin jako olemassa mille tahansa polynomille, jonka aste on pienempi kuin n. Olkoon lisäksi $\deg f = n$. Voimme olettaa, että f on jaollinen, eli $f = gh$, missä $\deg g < n$ ja $\deg h < n$. Induktiohypoteesin nojalla polynomien g ja h tekijöihinjaot ovat olemassa, sillä niiden asteet ovat pienemmät kun n. Näin ollen kun polynomin g jako jaottomiin tekijöihin on $g = g_1 \cdot g_2 \cdot \ldots \cdot g_n$ ja polynomin h vastaava jako on $h = h_1 \cdot h_2 \cdot \ldots \cdot h_n$, niin tällöin

$$f = gh = g_1 \cdot g_2 \cdot \ldots \cdot g_n \cdot h_1 \cdot h_2 \cdot \ldots \cdot h_n$$

on polynomin f jako jaottomiin tekijöihin, ja tällainen tekijöihin jako on siis olemassa.

Osoitetaan seuraavaksi tällaisen tekijöihin jaon yksikäsitteisyys. Olkoon $ag_1 \cdot \ldots \cdot g_s = bh_1 \cdot \ldots \cdot h_t$, missä $a, b \in k$ ja $g_1, \ldots, g_s, h_1, \ldots, h_t$ ovat jaottomia pääpolynomeja kunnassa K. Tässä tapauksessa $a = b$, sillä polynomien $g_1, \ldots, g_s$, $h_1, \ldots, h_t$ ollessa pääpolynomeja niiden kaikkien asteeltaan suurimpien termien kertoimet ovat 1, ja näin ollen yhtäsuuruus voi pitää paikkansa vain, jos $a = b$. Polynomi $g_1 \ldots g_s$ on jaollinen jaottomalla polynomilla h_1. Lemman 2.7 mukaan tämä tarkoittaa, että yksi polynomeista $g_1, \ldots, g_s$ on jaollinen polynomilla h_1.

Olkoon nyt johdonmukaisuuden vuoksi polynomi g_1 jaollinen polynomilla h_1. Ottaen huomioon, että g_1 ja h_1 ovat jaottomia pääpolynomeja, päättelemme että $g_1 = h_1$. Yksinkertaistetaan yhtälöä $g_1 \cdot \ldots \cdot g_s = h_1 \cdot \ldots \cdot h_t$

jakamalla se termillä $g_1 = h_1$. Useiden tällaisten operaatioiden jälkeen päättelemme, että $s = t$ ja $g_1 = h_{i_1}, \ldots, g_s = h_{i_s}$, missä $\{i_1, \ldots, i_s\}$ on joukon $\{1, \ldots, s\}$ permutaatio. Näin ollen siis nämä kaksi tekijöihinjakoa ovat yksi ja sama, ja siispä kysytty tekijöihin jako on yksikäsitteinen. □

Polynomien jaottomuus kokonaislukujen renkaassa $\mathbb{Z}$ on määritelty täsmälleen samalla tavalla kuin polynomien jaottomuus kunnissa, eli $f \in \mathbb{Z}[x]$ on jaoton renkaassa $\mathbb{Z}$ mikäli sitä ei voida esittää kokonaislukukertoimisten, positiivisasteisten polynomien tulona. Kun polynomin kertoimet kuuluvat renkaaseen, niitä ei aina voida jakaa polynomin suurimmalla kertoimella, vaan ne voidaan jakaa vain polynomien kertoimien suurimmalla yhteisellä tekijällä. Tästä pääsemme seuraavaan määritelmään.

Määritelmä 2.9. Olkoon $f(x) = \sum a_i x^i$, missä $a_i \in \mathbb{Z}$. Kertoimien $a_0, \ldots, a_n$ suurinta yhteistä tekijää merkitään $\mathrm{cont}(f)$.

Lemma 2.10. *$cont(fg) = cont(f)cont(g)$.*

Todistus. Selvästi mille tahansa kokonaislukukertoimiselle polynomille a on olemassa sellainen polynomi b renkaassa $\mathbb{Z}$, jolle $\mathrm{cont}(b) = 1$, että $a(x) = \mathrm{cont}(a)b(x)$.

Olkoot nyt f ja g sellaiset polynomit, että $\mathrm{cont}(f) = \mathrm{cont}(g) = 1$ ja $\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g)$. Lisäksi olkoot h ja j sellaisia polynomeja, että $h(x) = \mathrm{cont}(h)f(x)$ ja $j(x) = \mathrm{cont}(j)g(x)$. Täten

$$\begin{aligned}\mathrm{cont}(hj) &= \mathrm{cont}(\mathrm{cont}(h)f(x) \cdot \mathrm{cont}(j)g(x)) \\ &= \mathrm{cont}(\mathrm{cont}(h)\mathrm{cont}(j) \cdot f(x)g(x)) = \mathrm{cont}(h)\mathrm{cont}(j)\mathrm{cont}(fg) \\ &= \mathrm{cont}(h)\mathrm{cont}(j) \cdot 1 = \mathrm{cont}(h)\mathrm{cont}(j),\end{aligned}$$

eli $\mathrm{cont}(hj) = \mathrm{cont}(h)\mathrm{cont}(j)$. Riittää siis tutkia tapausta, jossa $\mathrm{cont}(f) = \mathrm{cont}(g) = 1$, koska muissa tapauksissa polynomin f kertoimet voidaan jakaa luvulla $\mathrm{cont}(f)$ ja vastaavasti polynomin g kertoimet voidaan jakaa luvulla $\mathrm{cont}(g)$.

Olkoon $f(x) = \sum a_i x^i$, $g(x) = \sum b_i x^i$, $(fg)(x) = \sum c_i x^i$. Oletetaan, että $\mathrm{cont}(fg) = d > 1$ ja p on luvun d alkulukutekijä. Tällöin kaikki polynomin fg kertoimet ovat jaollisia luvulla p, kun taas polynomeissa f ja g on kertoimia, jotka eivät ole jaollisia luvulla p. Olkoon a_r ensimmäinen polynomin f kerroin, joka ei ole jaollinen luvulla p, ja b_s ensimmäinen polynomin g kerroin, joka ei ole jaollinen luvulla p. Tällöin

$$\begin{aligned}c_{r+s} = a_r b_s + a_{r+1}b_{s-1} + a_{r+2}b_{s-2} + \ldots + a_{r-1}b_{s+1} + a_{r-2}b_{s+2} + \ldots \\ \equiv a_r b_s \not\equiv 0 \pmod{p},\end{aligned}$$

sillä

$$b_{s-1} \equiv b_{s-2} \equiv \ldots \equiv b_0 \equiv 0 \pmod{p},$$

$$a_{r-1} \equiv a_{r-2} \equiv a_0 \equiv 0 \pmod{p}.$$

Näin ollen kyseessä on ristiriita, ja täytyy olla $\text{cont}(fg) = d = 1$. Siispä, koska

$$\text{cont}(f)\text{cont}(g) = 1 \cdot 1 = 1,$$

niin $\text{cont}(fg) = \text{cont}(f)\text{cont}(g)$. □

Seuraus 2.11. *Kokonaislukukertoiminen polynomi on jaoton renkaassa $\mathbb{Z}[x]$ jos ja vain jos se on jaoton renkaassa $\mathbb{Q}[x]$.*

Todistus. Olkoon $f \in \mathbb{Z}[x]$ ja $f = gh$, missä $g, h \in \mathbb{Q}[x]$. Oletetaan, että $\text{cont}(f) = 1$. Valitaan sellainen positiivinen luku m että $mg \in \mathbb{Z}[x]$. Olkoon $n = \text{cont}(mg)$. Tällöin rationaaliluvulle $r = \frac{m}{n}$ pätee $rg \in \mathbb{Z}[x]$ ja $\text{cont}(rg) = 1$. Valitaan lisäksi sellainen kokonaisluku o, että $oh \in \mathbb{Z}[x]$. Olkoon $p = \text{cont}(oh)$, jolloin rationaaliluvulle $s = \frac{o}{p}$ pätee $sh \in \mathbb{Z}[x]$ ja $\text{cont}(sh) = 1$. Osoitetaan, että tässä tapauksessa $rs = 1$, eli että polynomin $f = (rg)(sh)$ tekijöihinjako on tekijöihinjako renkaassa $\mathbb{Z}$. Lemman 2.10 perusteella $\text{cont}(rg)\text{cont}(sh) = \text{cont}(rsgh)$, eli $1 = \text{cont}(rsf)$ Koska $\text{cont}(f) = 1$, päättelemme että $rs = 1$. □

Kronecker ehdotti seuraavaa algoritmia minkä tahansa polynomin $f \in \mathbb{Z}[x]$ jakamiseksi jaottomiin tekijöihin *(Kroneckerin algoritmi)*. Olkoon $\deg f = n$ ja $r = \left[\frac{n}{2}\right]$, eli r on yhtä suuri kuin $\frac{n}{2}$ pyöristettynä lähimpään kokonaislukuun. Siispä mikäli n on parillinen, niin $r = \frac{n}{2}$, ja mikäli n on pariton, niin $r = \frac{n+1}{2}$. Jos $f(x)$ on jaollinen, sen jakajan $g(x)$ aste ei ole suurempi kuin r.

Jakajan $g(x)$ löytämiseksi tutkitaan lukuja $c_j = f(j)$, jossa $j = 0, 1, \ldots, r$. Jos $c_j = 0$, niin tällöin $x - j$ jakaa polynomin $g(x)$. Jos taas $c_j \neq 0$, niin luku $g(j)$ jakaa luvun c_j. Jokaista lukujen $c_0, \ldots, c_r$ jakajien joukkoa $d_0, \ldots, d_r$ vastaa täsmälleen yksi korkeintaan astetta r oleva polynomi $g(x)$, jolle $g(j) = d_j$ kaikille $j = 0, 1, \ldots, r$. Erityisesti,

$$g(x) = \sum_{j=0}^{r} d_j g_j(x), \quad \text{missä} \quad g_j(x) = \prod_{0 \leq k \leq r, k \neq j} \left(\frac{x-k}{j-k} \right).$$

Jokaisen tällaisen polynomin tapauksessa on tarkistettava että sen polynomit ovat kokonaislukuja, ja että se oikeasti jakaa polynomin $f(x)$.

Esimerkki 2.12. Olkoon $f(x) = 2x^3 - x^2 + 2x - 1$. Tällöin $\deg f = 3$ ja $r = \left[\frac{3}{2}\right] = 2$. Nyt

$$\begin{aligned}
c_0 &= f(0) = 2 \cdot 0^3 - 0^2 + 2 \cdot 0 - 1 = 0 - 0 + 0 - 1 = -1, \\
c_1 &= f(1) = 2 \cdot 1^3 - 1^2 + 2 \cdot 1 - 1 = 2 - 1 + 2 - 1 = 2, \\
c_2 &= f(2) = 2 \cdot 2^3 - 2^2 + 2 \cdot 2 - 1 = 16 - 4 + 4 - 1 = 15.
\end{aligned}$$

Luvun -1 tekijöihinjako voi olla vain $(-1) \cdot 1$, luvun 2 taas joko $2 \cdot 1$ tai $(-2) \cdot (-1)$, ja luvun 15 joko $5 \cdot 3$, $(-5) \cdot (-3)$, $15 \cdot 1$ tai $(-15) \cdot 1$. Näin ollen joko $d_0 = -1$ tai $d_0 = 1$, $d_1 = 2$, $d_1 = 1$, $d_1 = -2$ tai $d_1 = 2$, jne. Lisäksi

$$\begin{aligned}
g_0(x) &= \prod_{0 \le k \le r, k \neq 0} \left(\frac{x-k}{0-k}\right) = \left(\frac{x-1}{0-1}\right) \cdot \left(\frac{x-2}{0-2}\right) = (-x+1)\left(\frac{x-2}{-2}\right), \\
&= (-x+1)\left(-\frac{1}{2}x + 1\right) = \frac{1}{2}x^2 - x - \frac{1}{2}x + 1 = \frac{1}{2}x^2 - \frac{3}{2}x + 1 \\
g_1(x) &= \prod_{0 \le k \le r, k \neq 1} \left(\frac{x-k}{1-k}\right) = \left(\frac{x-0}{1-0}\right)\left(\frac{x-2}{1-2}\right) = x\left(\frac{x-2}{-1}\right), \\
&= x(-x+2) = -x^2 + 2x \\
g_2(x) &= \prod_{0 \le k \le r, k \neq 2} \left(\frac{x-k}{2-k}\right) = \left(\frac{x-0}{2-0}\right)\left(\frac{x-1}{2-1}\right) = \left(\frac{1}{2}x\right)(x-1) \\
&= \frac{1}{2}x^2 - \frac{1}{2}x.
\end{aligned}$$

Kun kokeillaan asettaa eri vaihtoehtoja luvuille d_0, d_1 ja d_2 kaavaan $g(x) = \sum_{j=0}^{r} d_j g_j(x)$, lopulta todetaan sopiviksi luvuiksi $d_0 = -1$, $d_1 = 1$ ja $d_2 = 3$. Tällöin saadaan

$$\begin{aligned}
g(x) &= \sum_{j=0}^{r} d_j g_j(x) \\
&= (-1) \cdot \left(\frac{1}{2}x^2 - \frac{3}{2}x + 1\right) + 1 \cdot \left(-x^2 + 2x\right) + 3 \cdot \left(\frac{1}{2}x^2 - \frac{1}{2}x\right) \\
&= -\frac{1}{2}x^2 + \frac{3}{2}x - 1 - x^2 + 2x + \frac{3}{2}x^2 - \frac{3}{2}x \\
&= \left(-\frac{1}{2} - 1 + \frac{3}{2}\right)x^2 + \left(\frac{3}{2} + 2 - \frac{3}{2}\right)x + (-1) = 2x - 1.
\end{aligned}$$

Kun jaetaan polynomi f polynomilla $2x - 1$, nähdään että

$$2x^3 - x^2 + 2x - 1 = (x^2 + 1)(2x - 1).$$

Nyt, sekä $2x-1$ että x^2+1 ovat jaottomia polynomeja. Näin ollen polynomin f jako jaottomiin tekijöihin on

$$f(x) = (x^2 + 1)(2x - 1).$$

3 Jaottomuuskriteerit

3.1 Eisensteinin kriteeri

Yksi parhaiten tunnetuista polynomien jaottomuuskriteereistä on seuraava Eisensteinin kriteeri, joka osoittaa tiettyä muotoa olevien polynomien jaottomuuden.

Lause 3.1. ***(Eisensteinin kriteeri).*** *Olkoon $f(x) = a_0 + a_1x + \ldots + a_nx^n$ sellainen kokonaislukukertoiminen polynomi, että kerroin a_n ei ole jaollinen alkuluvulla p, kun taas kertoimet $a_0, \ldots, a_{n-1}$ ovat jaollisia alkuluvulla p mutta a_0 ei ole jaollinen luvulla p^2. Tällöin f on jaoton renkaassa $\mathbb{Z}$.*

Todistus. Olkoon

$$f = gh = \left(\sum b_k x^k\right)\left(\sum c_l x^l\right),$$

missä g ja h ovat positiivisasteisia, kokonaislukukertoimisia polynomeja. Luku $b_0c_0 = a_0$ on jaollinen luvulla p, ja näin ollen toisen luvuista b_0 ja c_0 on oltava jaollinen luvulla p. Olkoon johdonmukaisuuden vuoksi luku b_0 jaollinen luvulla p. Tällöin c_0 ei ole jaollinen luvulla p, sillä $a_0 = b_0c_0$ ei ole jaollinen luvulla p^2. Jos kaikki luvut b_i ovat jaollisia luvulla p, niin tällöin myös a_n on jaollinen luvulla p. Näin ollen on oltava olemassa sellainen i, että b_i ei ole jaollinen luvulla p, mille $0 < i \leq \deg g < n$. Oletetaan, että i on pienin indeksi, jolla luku b_i ei ole jaollinen luvulla p.

Nyt, luku a_i on oletukselta jaollinen luvulla p, mutta toisaalta $a_i = b_ic_0 + b_{i-1}c_1 + \ldots + b_0c_i$, missä kaikki yhteenlaskettavat luvut $b_{i-1}c_1, \ldots, b_0c_i$ ovat jaollisia luvulla p, mutta b_ic_0 ei ole jaollinen luvulla p. Koska b_ic_0 ei ole jaollinen luvulla p, niin tällöin myöskään a_i ei ole jaollinen luvulla p. Näin ollen syntyy ristiriita, ja siispä ei voi olla olemassa sellaisia polynomeja g ja h, joille pätisi $f = gh$. Näin ollen polynomi f on jaoton. □

Esimerkki 3.2. Polynomi $f = x^4 + 6x^3 + 9x^2 + 12x + 3$ on jaoton.

Todistus. Olkoon $p = 3$. Nyt, luku 1 ei ole jaollinen luvulla p, mutta luvut 6, 9, 12 ja 3 ovat. Lisäksi luku 3 ei ole jaollinen luvulla $p^2 = 9$. Näin ollen f on Lauseen 3.1 mukaan jaoton. □

Esimerkki 3.3. Mille tahansa alkuluvulle p, polynomi

$$f(x) = 1 + x + \frac{x^2}{2!} + \ldots + \frac{x^p}{p!}$$

on jaoton.

Todistus. Riittää osoittaa, että polynomi

$$p!f(x) = x^p + px^{p-1} + p(p-1)x^{p-2} + \ldots + p!$$

on jaoton.

Nyt, selkeästikään alkuluku p ei jaa lukua 1. Se kuitenkin jakaa kaikki luvut $p, p(p-1), \ldots, p!$, sillä se on jokaisen niistä tekijä. Pitää vain siis osoittaa, että p^2 ei jaa lukua $p!$. Nyt,

$$p! = p(p-1) \cdot (p-2) \cdot \ldots \cdot 2 \cdot 1.$$

□

Koska $p > p-1 > p-2 > \ldots > 2 > 1$, ei p jaa mitään luvuista $p-1, p-2, \ldots, 2, 1$. Jotta luku p^2 jakaisi luvun $p!$, tulee alkuluvun p jakaa luku $\frac{p!}{p} = (p-1) \cdot (p-2) \cdot \ldots \cdot 2 \cdot 1$. Kuitenkaan alkuluku p ei jaa yhtäkään tämän luvun tekijöistä, jolloin se ei jaa itse lukua. Näin ollen p ei jaa lukua $\frac{p!}{p}$, ja näin ollen p^2 ei jaa lukua $p!$.

Näin ollen alkuluku p ei jaa lukua 1, se jakaa luvut $p, p(p-1), \ldots, p!$, ja luku p^2 ei jaa lukua $p!$. Näin ollen Lauseen 3.1 mukaan polynomi $p!f(x)$ on jaoton. Siispä polynomi f on jaoton.

3.2 Jaottomuus modulo p

Olkoon p alkuluku ja $\mathbb{F}_p$ jäännösluokka modulo p. Jokainen kokonaislukukertoiminen polynomi voidaan myös esittää polynomina, jonka kertoimet on saatu jäännösluokasta $\mathbb{F}_p$. Renkaassa $\mathbb{Z}[x]$ jaoton polynomi voi muuttua jaolliseksi jäännösluokkarenkaassa $\mathbb{F}_p[x]$ jokaiselle alkuluvulle p, ja tämän osoittava esimerkki perustuu seuraavaan lauseeseen.

Lause 3.4. *Polynomi $P(x) = x^4 + ax^2 + b^2$, jossa $a, b \in \mathbb{Z}$, on jaollinen kunnassa $\mathbb{F}_p$ kaikilla alkuluvuilla p.*

Todistus. Alkuluvulle $p = 2$ tätä muotoa olevia polynomea on vain neljä kappaletta, ja ne ovat

$$\begin{aligned}
&x^4 = x^2 \cdot x^2, \\
&x^4 + x^2 = x^2(x^2 + 1), \\
&x^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 1 = (x+1)^4, \\
&x^4 + x^2 + 1 = x^4 + 2x^3 + 3x^2 + 2x + 1 = (x^2 + x + 1)^2.
\end{aligned}$$

Nämä yhtäsuuruudet pitävät paikkansa, sillä kunnassa $\mathbb{F}_2[x]$ pätee $0 = 2 = 4 = 6$ ja $1 = 3$. Kuten nähdään, kaikki nämä polynomit ovat jaollisia.

Olkoon p pariton alkuluku. Tällöin voimme valita sellaisen kokonaisluvun s, että $a \equiv 2s \pmod{p}$. Siispä

$$\begin{aligned} P(x) = x^4 + ax^2 + b^2 &\equiv x^4 + 2sx^2 + b^2 \mod p \\ &\equiv x^4 + 2sx^2 + s^2 - s^2 + b^2 \mod p \\ &\equiv (x^2 + s)^2 - (s^2 - b^2) \mod p, \end{aligned}$$

$$\begin{aligned} P(x) = x^4 + ax^2 + b^2 &\equiv x^4 + 2sx^2 + b^2 \mod p \\ &\equiv x^4 + 2bx^2 + b^2 - 2bx^2 + 2sx^2 \mod p \\ &\equiv (x^2 + b)^2 - (2b - 2s)x^2 \mod p, \\ P(x) = x^4 + ax^2 + b^2 &\equiv x^4 + 2sx^2 + b^2 \mod p \\ &\equiv x^4 - 2bx^2 + b^2 + 2bx^2 + 2sx^2 \mod p \\ &\equiv (x^2 - b)^2 - (-2b - 2s)x^2 \mod p. \end{aligned}$$

Näin ollen riittää osoittaa, että jokin luvuista $s^2 - b^2$, $2b - 2s$, $-2b - 2s$ on neliöllinen jäännös modulo p, eli jokin kyseisistä luvuista on kongruentti jonkin kokonaisluvun neliön kanssa modulo p, sillä jos $s^2 - b^2 \equiv n^2 \mod p$ jollakin $n \in \mathbb{Z}$, niin tällöin

$$\begin{aligned} (x^2 + s)^2 - (s^2 - b^2) &\equiv (x^2 + s)^2 - n^2 \mod p, \\ (x^2 + s)^2 - n^2 &= ((x^2 + s) + n)((x^2 + s) - n), \end{aligned}$$

jolloin polynomi p on jaollinen kunnassa $\mathbb{F}_p$. Vastaavasti jos $(2b - 2s) \equiv n^2$, niin

$$\begin{aligned} (x^2 + b)^2 - (2b - 2s)x^2 &\equiv (x^2 + b)^2 - n^2x^2 \mod p, \\ (x^2 + b)^2 - n^2x^2 &= ((x^2 + b) + nx)((x^2 + b) - nx), \end{aligned}$$

jolloin polynomi p on jaollinen kunnassa $\mathbb{F}_p$, ja jos $(-2b - 2s)x^2 \equiv n^2$, niin

$$\begin{aligned} (x^2 - b)^2 - (-2b - 2s)x^2 &\equiv (x^2 - b)^2 - n^2x^2 \mod p, \\ (x^2 - b)^2 - n^2x^2 &= ((x^2 - b) + nx)((x^2 - b) - nx), \end{aligned}$$

jolloin polynomi p on jaollinen kunnassa $\mathbb{F}_p$.

Nyt, kuvauksessa $x \mapsto x^2$ sekä x että $-x$ kuvautuvat samaksi alkioksi. Näin ollen tällä kuvauksella nollasta poikkeavien alkioiden kuvajoukko koostuu $\frac{p-1}{2}$ alkiosta. Toisaalta, jos $x = y^2$, niin tällöin $x^{(p-1)/2} = y^{2\cdot((p-1)/2)} = y^{p-1} = 1$, eli kaikki $\frac{p-1}{2}$ alkiota toteuttavat yhtälön $x^{(p-1)/2} = 1$. Alkiot, jotka eivät kuulu muunnoksen $x \mapsto x^2$ kuvajoukkoon, toteuttavat yhtälön $x^{(p-1)/2} = -1$. Näin ollen, mikäli kaksi kokonaislukua eivät ole kokonaislukujen neliöitä modulo p, niin tällöin niiden tulo on kokonaisluvun neliö modulo p.

Oletetaan, että $2b - 2s$ ja $-2b - 2s$ eivät ole kokonaislukujen neliöitä modulo p. Tällöin niiden tulo $4(s^2 - b^2)$ on kokonaislukujen neliö modulo p, ja näin ollen niin on myös $s^2 - b^2$. Siispä $s^2 - b^2$ on kokonaislukujen neliö modulo p, ja siten polynomi p on jaollinen kunnassa $\mathbb{F}_p$. □

3.3 Pieniä arvoja saavuttavien polynomien jaottomuus

Joskus polynomin jaottomuus voidaan selvittää tarkastelemalla millaisia arvoja se saavuttaa. Esimerkiksi tässä kappaleessa esiteltävä lause osoittaa, että mikäli jollakin polynomilla on tarvittavan suuri määrä tarpeeksi pieniä arvoja jotka eivät ole sen juuria, on kyseinen polynomi jaoton.

Lemma 3.5. *Olkoon g k-asteinen, kokonaislukukertoiminen polynomi, ja olkoon $d_0 < d_1 < \ldots < d_n$ kokonaislukuja. Tällön $|g(d_i)| \geq k!2^{-k}$ jollakin i.*

Todistus. Tutkitaan polynomia

$$G(x) = (x - d_0) \cdot \ldots \cdot (x - d_k) \sum_{i=0}^{k} \frac{g(d_i)}{x - d_i} \prod_{j \neq i} \frac{1}{d_i - d_j}.$$

Nyt, kun $m = 0, \ldots, k$, niin tällöin $G(d_m) = g(d_m)$, sillä

$$\begin{aligned}
G(d_m) =& (d_m - d_0) \cdot \ldots \cdot (d_m - d_k) \sum_{i=0}^{k} \frac{g(d_i)}{d_m - d_i} \prod_{j \neq i} \frac{1}{d_i - d_j} \\
&= \prod_{i=0}^{k} (d_m - d_i) \sum_{i=0}^{k} \frac{g(d_i)}{d_m - d_i} \prod_{j \neq 0} \frac{1}{d_i - d_j} \\
&= \sum_{i=0}^{k} \frac{g(d_i)}{d_m - d_i} \prod_{i=0}^{k} (d_m - d_i) \prod_{j \neq 0} \frac{1}{d_i - d_j} \\
&= \sum_{i=0}^{k} \frac{g(d_i)}{d_m - d_i} (d_m - d_i) \prod_{j \neq i} (d_m - d_j) \cdot \frac{1}{d_i - d_j} \\
&= \sum_{i=0}^{k} g(d_i) \prod_{j \neq i} \frac{d_m - d_j}{d_i - d_j}.
\end{aligned}$$

Nyt, aina kun $i \neq m$, niin $g(d_i) \prod_{j \neq i} \frac{d_m - d_j}{d_i - d_j} = 0$, sillä tuloon $\prod_{j \neq i} \frac{d_m - d_j}{d_i - d_j}$

kuuluu termi $\frac{d_m-d_m}{d_i-d_m} = \frac{0}{d_i-d_m} = 0$. Näin ollen saadaan

$$\begin{aligned} G(d_m) &= g(d_m) \prod_{j\neq m} \frac{d_m - d_j}{d_m - d_j} \\ &= g(d_m) \cdot \frac{d_m - d_1}{d_m - d_1} \cdot \ldots \cdot \frac{d_m - d_{m-1}}{d_m - d_{m-1}} \cdot \frac{d_m - d_{m+1}}{d_m - d_{m+1}} \cdot \ldots \cdot \frac{d_m - d_k}{d_m - d_k} \\ &= g(d_m) \cdot 1 \cdot \ldots \cdot 1 \cdot 1 \cdot \ldots \cdot 1 = g(d_m). \end{aligned}$$

Lisäksi $\deg G \leq k$. Näin ollen nähdään, että $G(x) = g(x)$.

Polynomin G korkeimman asteen kerroin on

$$\sum_{i=0}^{k} g(d_i) \prod_{j\neq i} \frac{1}{d_1 - d_j}.$$

Oletuksen perusteella tämä kerroin on nollasta eroava kokonaisluku, ja näin ollen sen itseisarvo on vähintään 1. Näin ollen jollekin i pätee

$$\begin{aligned} |g(d_i)| &\geq \frac{1}{\left|\sum_{0\leq i\leq k} \prod_{j\neq i} \frac{1}{|d_i-d_j|}\right|} \geq \frac{1}{\left|\sum_{0\leq i\leq k} \prod_{j\neq i} \frac{1}{|i-j|}\right|} \\ &= \frac{1}{\sum_{0\leq i\leq k} \frac{1}{|i|} \cdot \frac{1}{|i-1|} \cdot \ldots \cdot \frac{1}{|i-(i-1)|} \cdot \frac{1}{|i-(i+1)|} \cdot \ldots \cdot \frac{1}{|i-k|}} \\ &= \frac{1}{\sum_{0\leq i\leq k} \frac{1}{|i|} \cdot \frac{1}{|i-1|} \cdot \ldots \cdot \frac{1}{|1|} \cdot \frac{1}{|-1|} \cdot \ldots \cdot \frac{1}{|i-k|}} = \frac{1}{\sum_{0\leq i\leq k} \frac{1}{i!} \cdot \frac{1}{(k-i)!}} \\ &= \frac{1}{\sum_{0\leq i\leq k} \frac{1}{i!(k-i)!}} = \frac{k!}{\sum_{0\leq i\leq k} \frac{k!}{i!(k-1)!}} = \frac{k!}{\sum_{0\leq i\leq k} \binom{k}{i}} = \frac{k!}{2^k} = k!2^{-k} \end{aligned}$$

Siispä jollekin i pätee $|g(d_i)| \geq k!2^{-k}$. □

Lause 3.6. ***(Pólya)***. *Olkoon f n-asteinen, kokonaislukukertoiminen polynomi. Määritellään $m = \left[\frac{n+1}{2}\right]$, eli m on $\frac{n+1}{2}$ pyöristettynä lähimpään kokonaislukuun. Tämä tarkoittaa että mikäli $n+1$ on parillinen, niin $m = \frac{n+1}{2}$, ja mikäli se on pariton, niin $\frac{n+2}{2}$. Oletetaan, että on olemassa n eri kokonaislukua $a_1, \ldots, a_n$, joille pätee $|f(a_i)| < 2^{-m}m!$ ja luvut $a_1, \ldots, a_n$ eivät ole polynomin f juuria. Tällöin f on jaoton.*

Todistus. Tehdään vastaoletus, että $f = gh$, missä g ja h ovat kokonaislukukertoimisia polynomeja. Voimme olettaa, että $\deg h \leq \deg g = k$. Tällöin $m \leq k < n$. Nyt, kaikilla i pätee

$$f(a_i) = g(a_i)h(a_i), \ f(a_i) \neq 0.$$

Näin ollen $g(a_i) \neq 0$ ja luku $g(a_i)$ jakaa luvun $f(a_i)$. Siispä

$$|g(a_i)| \leq |f(a_i)| < \frac{m!}{2^m}.$$

Lemman 3.5 mukaan, $|g(a_i)| \geq 2^{-k}k!$ pätee eräälle a_i. Jos $m = k - r$, niin tällöin

$$\frac{m!}{k!} = \frac{(k-r)!}{k!} = \frac{1}{k} \cdot \frac{1}{k-1} \cdot \ldots \cdot \frac{1}{k-r-1} \leq \frac{1}{2^r} = \frac{2^{k-r}}{2^k} = \frac{2^m}{2^k}.$$

Näin ollen

$$\frac{2^{-m}m!}{2^{-k}k!} = \frac{2^{-m}}{2^{-k}}\frac{m!}{k!} \leq \frac{2^{-m}}{2^{-k}}\frac{2^m}{2^k} = 2^{-m-(-k)+m-k} = 2^{-m+k+m-k} = 2^0 = 1,$$

eli

$$\frac{2^{-m}m!}{2^{-k}k!} \leq 1 \iff 2^{-m}m! \leq 2^{-k}k!.$$

Näin ollen kaikille a_i pätee $|g(a_i)| < 2^{-k}k!$. Kyseessä on siis ristiriita, ja näin ollen polynomi f on jaoton. □

Esimerkki 3.7. Polynomi $f(x) = (x-1)\cdot(x-2)\cdot\ldots\cdot(x-n)+1$ on jaoton, kun $n \geq 5$.

Todistus. Nyt, polynomin f aste on n. Tämä voidaan jakaa kahteen tapaukseen: n on joko parillinen tai pariton.

Jos n on parillinen eli $n = 2p$ jollakin $p \in \mathbb{N}$, niin tällöin

$$m = \left\lceil \frac{n+1}{2} \right\rceil = \left\lceil \frac{2p+1}{2} \right\rceil = \left\lceil p + \frac{1}{2} \right\rceil = p+1.$$

Jos n on taas pariton eli $n = 2p+1$ jollakin $p \in \mathbb{N}$, niin tällöin

$$m = \left\lceil \frac{n+1}{2} \right\rceil = \left\lceil \frac{2p+1+1}{2} \right\rceil = \left\lceil \frac{2p+2}{2} \right\rceil = [p+1] = p+1.$$

Tällöin parillisessa tapauksessa saadaan $m = \frac{n}{2} + 1$ ja parittomassa $m = \frac{n}{2} + \frac{1}{2} < \frac{n}{2} + 1$.

Riittää siis löytää n sellaista kokonaislukua, jotka eivät ole polynomin f juuria ja joille pätee

$$|f(a_i)| < 2^{-m}m! \leq 2^{-\left(\frac{n}{2}+1\right)}\left(\frac{n}{2}+1\right)!$$

Nyt, jos termiä $2^{-\left(\frac{n}{2}+1\right)}\left(\frac{n}{2}+1\right)!$ tutkitaan muuttujan n funktiona, huomataan sen olevan kasvava funktio. Lisäksi huomataan, että

$$2^{-\left(\frac{5}{2}+1\right)}\left(\frac{5}{2}+1\right)! = \frac{\left(\frac{5}{2}+1\right)!}{8} > 1.$$

Näin ollen jos $n \geq 5$, niin tällöin

$$\begin{aligned}
|f(1)| &= |(1-1)\cdot(1-2)\cdot\ldots\cdot(1-n)+1| = 1 < 2^{-\left(\frac{n}{2}+1\right)}\left(\frac{n}{2}+1\right)!,\\
|f(2)| &= |(2-1)\cdot(2-2)\cdot\ldots\cdot(2-n)+1| = 1 < 2^{-\left(\frac{n}{2}+1\right)}\left(\frac{n}{2}+1\right)!,\\
&\vdots\\
|f(n)| &= |(n-1)\cdot(n-2)\cdot\ldots\cdot(n-n)+1| = 1 < 2^{-\left(\frac{n}{2}+1\right)}\left(\frac{n}{2}+1\right)!.
\end{aligned}$$

Näin ollen siis löytyy n sellaista arvoa a_i, joille pätee $|f(a_i)| < 2^{-m}m!$, ja siispä polynomi f on Lauseen 3.6 mukaan jaoton. □

4 Muotoa $x^n \pm x^m \pm x^p \pm 1$ olevien polynomien jaottomuus

Tutkitaan nyt viimeisenä muotoa $x^n \pm x^m \pm x^p \pm 1$ olevien polynomien jaottomuutta. Tällaiset polynomit voidaan esittää muodossa $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3$, kun $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm 1$ ja $\varepsilon_3 = \pm 1$. Osoitetaan ensin, että riittää tarkastella tapausta, missä $m + p \geq n$. Selvästi, f on jaoton jos ja vain jos polynomi

$$x^n f\left(\frac{1}{x}\right) = 1 + \varepsilon_1 x^{n-m} + \varepsilon_2 x^{n-p} + \varepsilon_3 x^n$$

on jaoton, sillä

$$x^n f\left(\frac{1}{x}\right) = g(x)h(x) \iff f\left(\frac{1}{x}\right) = \frac{1}{x^n} g(x)h(x).$$

Tällöin, jos $m + p < n$, niin $(n - m) + (n - p) > n$, sillä

$$(n - m) + (n - p) = n - m + n - p = 2n - (m + p) > 2n - n = n.$$

Siispä jokaiselle polynomille f, jolle pätee $m + p < n$, on olemassa sellainen polynomi jolle pätee $m+p \geq n$, joka on jaollinen jos ja vain jos f on jaollinen.

Voimme myös jättää tarkasteluista pois tapauksen jossa $n = m + p$ ja $\varepsilon_3 = \varepsilon_1 \varepsilon_2$, sillä tällöin

$$\begin{aligned} f(x) &= x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3 = x^{m+p} + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_1 \varepsilon_2 \\ &= (x^m + \varepsilon_2)(x^p + \varepsilon_1). \end{aligned}$$

Määritelmä 4.1. Astetta s oleva polynomi $\varphi(x)$ on *rekursiivinen*, mikäli

$$\varphi(x) = \pm x^s \varphi\left(\frac{1}{x}\right).$$

Lemma 4.2. *Olkoon $f(x) = \varphi(x)\psi(x)$, missä $\varphi(x)$ ja $\psi(x)$ ovat kokonaislukukertoimisia, positiivisasteisia pääpolynomeja. Tällöin ainakin toinen polynomeista $\varphi(x)$ ja $\psi(x)$ on rekursiivinen.*

Todistus. Olkoon $r = \deg \varphi$ ja $s = n - r = \deg \psi$. Tutkitaan polynomeja

$$\begin{aligned} f_1(x) &= x^r \varphi\left(\frac{1}{x}\right) \psi(x) = \sum_{i=0}^{n} c_i x^{n-i}, \\ f_2(x) &= x^s \psi\left(\frac{1}{x}\right) \varphi(x) = x^n \left(x^{-r} \varphi\left(\frac{1}{\frac{1}{x}}\right) \psi\left(\frac{1}{x}\right)\right) = x^n f_1\left(\frac{1}{x}\right) \\ &= \sum_{i=0}^{n} c_{n-i} x^{n-i}. \end{aligned}$$

Nyt

$$\begin{aligned} f_1(x)f_2(x) &= x^n f\left(\frac{1}{x}\right) = \left(x^r\varphi\left(\frac{1}{x}\right)\psi(x)\right)\left(x^s\psi\left(\frac{1}{x}\right)\varphi(x)\right) \\ &= x^{r+s}\varphi\left(\frac{1}{x}\right)\varphi(x)\psi\left(\frac{1}{x}\right)\psi(x) \\ &= x^n\left(\varphi\left(\frac{1}{x}\right)\psi\left(\frac{1}{x}\right)\right)(\varphi(x)\psi(x)) \\ &= f(x)x^n f\left(\frac{1}{x}\right) \\ &= (x^n+\varepsilon_1 x^m+\varepsilon_2 x^p+\varepsilon_3)x^n(x^{-n}+\varepsilon_1 x^{-m}+\varepsilon_2 x^{-p}+\varepsilon_3) \\ &= (x^n+\varepsilon_1 x^m+\varepsilon_2 x^p+\varepsilon_3)(\varepsilon_3 x^n+\varepsilon_2 x^{n-p}+\varepsilon_1 x^{n-m}+1). \end{aligned}$$

Kun tämä esitys kerrotaan auki, saadaan astetta $2n$ olevan termin kertoimeksi ε_3. Vastaavasti polynomilla f_1 astetta n olevan termin kerroin on $c_n x^{n-n} = c_n x^0 = c_n$ ja polynomilla f_2 puolestaan $c_{n-n}x^{n-n} = c_0 x^0 = c_0$. Näin ollen tutkittavan polynomin $f_1(x)f_2(x)$ astetta $2n$ olevan termin kerroin voidaan esittää myös muodossa c_0c_n. Tällöin siis $c_0c_n = \varepsilon_3$, ja näin ollen $c_0 = \pm 1$ ja $c_n = \pm 1$, sillä tosiaan $\varepsilon_3 = \pm 1$. Astetta n olevien termien vastaavanlainen kertoimien vertailu taas osoittaa, että

$$c_0^2 + c_1^2 + \ldots + c_{n-1}^2 + c_n^2 = 1 + \varepsilon_1^2 + \varepsilon_2^2 + \varepsilon_3^2 = 1 + (\pm 1)^2 + (\pm 1)^2 + (\pm 1)^2 = 4,$$

eli toisin sanoen

$$1 + c_1^2 + \ldots + c_{n-1}^2 + 1 = \iff c_1^2 + \ldots + c_{n-1}^2 + 2 = 4 \iff c_1^2 + \ldots + c_{n-1}^2 = 2.$$

Näin ollen, $c_0 = \pm 1$, $c_n = \pm 1$, $c_\alpha = \pm 1$ ja $c_\beta = \pm 1$ joillekin $1 \leq \alpha < \beta \leq n-1$, ja kaikki muut kertoimet c_i ovat nolla. Näin ollen $f_1(x)f_2(x)$ voidaan esittää seuraavilla kahdella tavalla:

$$\begin{aligned} &c_0c_nx^{2n} + c_\alpha c_n x^{2n-\alpha} + c_\beta c_n x^{2n-\beta} + c_0c_\alpha x^{n+\alpha} + c_0c_\beta x^{n+\beta} + c_0c_\alpha x^{n-\alpha} \\ &+ c_0c_\beta x^{n-\beta} + c_\alpha c_\beta x^{n+\beta-\alpha} + c_\alpha c_\beta x^{n+\alpha-\beta} + c_nc_\alpha x^\alpha + c_nc_\beta x^\beta + c_0c_n + 4x^n \end{aligned} \tag{1}$$

ja

$$\begin{aligned} &\varepsilon_3x^{2n} + \varepsilon_2x^{2n-p} + \varepsilon_1x^{2n-m} + \varepsilon_1\varepsilon_3x^{n+m} + \varepsilon_2\varepsilon_3x^{n+p} + \varepsilon_1\varepsilon_2x^{n+m-p} \\ &+ \varepsilon_1x^m + \varepsilon_2x^p + \varepsilon_1\varepsilon_2x^{n+p-m} + \varepsilon_2\varepsilon_3x^{n-p} + \varepsilon_1\varepsilon_3x^{n-m} + \varepsilon_3 + 4x^n. \end{aligned} \tag{2}$$

Tapojen (1) ja (2) vertailemiseksi, järjestellään monomit niiden asteiden perusteella, ottaen huomioon vain kolme korkeinta monomia. Muodolle (1)

saamme neljä vaihtoehtoa:

$$\begin{aligned}
\beta \le \frac{n}{2} &: 2n > 2n-\alpha > 2n-\beta,\\
\beta > \frac{n}{2},\ \alpha \le n-\beta &: 2n > 2n-\alpha \ge n+\beta,\\
\beta > \frac{m}{2},\ \frac{n}{2} \ge \alpha > n-\beta &: 2n > n+\beta > 2n-\alpha,\\
\beta > \frac{n}{2}, \alpha > \frac{n}{2} &: 2n > n+\beta > n+\alpha.
\end{aligned}$$

Tapaukselle (2) saamme taas kaksi vaihtoehtoa:

$$\begin{aligned}
n \ge 2m &: 2n > 2n-p > 2n-m,\\
2m > n \ge n+p &: 2n > 2n-p > n+m.
\end{aligned}$$

Kun verrataan kolmea korkeinta monomia vaihtoehdoissa (1) ja (2) saamme parin (α, β), ja seuraavat neljä mahdollisuutta:

$$(\alpha,\beta) = (p,m),\ (p,n-m),\ (m,n-p) \text{ tai } (n-m,n-p).$$

Jos $(\alpha,\beta) = (p,m)$, niin vaihtoehto (1) saadaan muotoon

$$\begin{aligned}
&c_0c_nx^{2n} + c_pc_nx^{2n-p} + c_mc_nx^{2n-m} + c_0c_px^{n+p} + c_0c_mx^{n+m} + c_0c_px^{n-p}\\
&+ c_0c_mx^{n-m} + c_pc_mx^{n+m-p} + c_pc_mx^{n+p-m} + c_nc_px^p + c_nc_mx^m + c_0c_n + 4x^n
\end{aligned}$$

ja vaihtoehto (2) on edelleen muodossa

$$\begin{aligned}
&\varepsilon_3x^{2n} + \varepsilon_2x^{2n-p} + \varepsilon_1x^{2n-m} + \varepsilon_1\varepsilon_3x^{n+m} + \varepsilon_2\varepsilon_3x^{n+p} + \varepsilon_1\varepsilon_2x^{n+m-p}\\
&+ \varepsilon_1x^m + \varepsilon_2x^p + \varepsilon_1\varepsilon_2x^{n+p-m} + \varepsilon_2\varepsilon_3x^{n-p} + \varepsilon_1\varepsilon_3x^{n-m} + \varepsilon_3 + 4x^n.
\end{aligned}$$

Näistä saadaan

$$c_0c_n = \varepsilon_3,\ c_pc_n = \varepsilon_2,\ c_mc_n = \varepsilon_1.$$

Näin ollen, koska $c_n = \pm 1$ ja täten $c_n^2 = 1$,

$$\begin{aligned}
f_1(x) &= c_0x^n + c_px^{n-p} + c_mx^{n-m} + c_n\\
&= c_n^2c_0x^n + c_n^2c_px^{n-p} + c_n^2c_mx^{n-m} + c_n^3\\
&= c_n(c_nc_0x^n + c_nc_px^{n-p} + c_nc_mx^{n-m} + c_n^2)\\
&= c_n(c_0c_nx^n + c_pc_nx^{n-p} + c_mc_nx^{n-m} + 1)\\
&= c_n(\varepsilon_3x^n + \varepsilon_2x^{n-p} + \varepsilon_1x^{n-m} + 1) = c_nx^nf\left(\frac{1}{x}\right),
\end{aligned}$$

ja siispä

$$x^r\varphi\left(\frac{1}{x}\right)\psi(x) = c_n x^n f\left(\frac{1}{x}\right) \iff \varphi\left(\frac{1}{x}\right)\psi(x) = c_n x^{n-r} f\left(\frac{1}{x}\right)$$
$$\iff \varphi\left(\frac{1}{x}\right)\psi(x) = c_n x^s \varphi\left(\frac{1}{x}\right)\psi\left(\frac{1}{x}\right) \iff \psi(x) = x_n x^s \psi\left(\frac{1}{x}\right),$$

ja näin ollen polynomi $\psi(x)$ on rekursiivinen.

Kun $(\alpha, \beta) = (n-m, n-p)$, niin tällöin vaihtoehto (1) saadaan muotoon

$$\begin{aligned} &c_0c_nx^{2n} + c_{n-m}c_nx^{n+m} + c_{n-p}c_nx^{n+p} + c_0c_{n-m}x^{2n-m} + c_0c_{n-p}x^{2n-p} \\ &+ c_0c_{n-m}x^m + c_0c_{n-p}x^p + c_{n-m}c_{n-p}x^{n-p+m} + c_{n-m}c_{-p}x^{n-m+p} \\ &+ c_nc_{n-m}x^{n-m} + c_nc_{n-p}x^{n-p} + c_0c_n + 4x^n \end{aligned}$$

ja vaihtoehto (2) on edelleen muodossa

$$\begin{aligned} &\varepsilon_3x^{2n} + \varepsilon_2x^{2n-p} + \varepsilon_1x^{2n-m} + \varepsilon_1\varepsilon_3x^{n+m} + \varepsilon_2\varepsilon_3x^{n+p} + \varepsilon_1\varepsilon_2x^{n+m-p} \\ &+ \varepsilon_1x^m + \varepsilon_2x^p + \varepsilon_1\varepsilon_2x^{n+p-m} + \varepsilon_2\varepsilon_3x^{n-p} + \varepsilon_1\varepsilon_3x^{n-m} + \varepsilon_3 + 4x^n. \end{aligned}$$

Näistä saadaan erityisesti

$$c_0c_n = \varepsilon_3,\ c_0c_{n-p} = \varepsilon_2 \text{ ja } c_0c_{n-m} = \varepsilon_1.$$

Nyt, kun muistetaan että $c_0 = \pm 1$, eli $c_0^2 = 1$, niin

$$\begin{aligned} f_1(x) &= c_0x^n + c_{n-m}x^{n-(n-m)}c_{n-p}x^{n-(n-p)} + c_n \\ &= c_0x^n + c_{n-m}x^m + c_{n-p}x^p + c_n \\ &= c_0^3x^n + c_0^2c_{n-m}x^m + c_0^2c_{n-p}c^p + c_0^2c_n \\ &= c_0(c_0^2x^n + c_0c_{n-m}x^m + c_0c_{n-p}x^p + c_0c_n) \\ &= c_0(x^n + \varepsilon_1x^p + \varepsilon_2x^m + \varepsilon_3) = c_0f(x). \end{aligned}$$

Siispä

$$f_1(x) = c_0f(x) \iff x^r\varphi\left(\frac{1}{x}\right)\psi(x) = c_0\varphi(x)\psi(x)$$
$$\iff x^r\varphi\left(\frac{1}{x}\right) = c_0\varphi(x).$$

Nyt, koska $c_0 = \pm 1$, niin

$$x^r\varphi\left(\frac{1}{x}\right) = c_0\varphi(x) \iff \varphi(x) = c_0x^r\varphi\left(\frac{1}{x}\right)$$

ja nähdään, että $\varphi(x)$ on rekursiivinen.

Jos taas $(\alpha, \beta) = (p, n-m)$, tällöin tapauksessa (1) saamme polynomin

$$\begin{aligned} &c_0c_nx^{2n} + c_pc_nx^{2n-p} + c_{n-m}c_nx^{n+m} + c_0c_\alpha x^{n+p} \\ &+ c_0c_{n-m}x^{2n-m} + c_0c_px^{n-p} + c_0c_{n-m}x^m + c_pc_{n-m}x^{2n-m-p} \\ &+ c_pc_{n-m}x^{p+m} + c_nc_px^p + c_nc_{n-m}x^{n-m} + c_0c_n + 4x^n \end{aligned}$$

eli saamme monomit, joiden asteet ovat

$$2n,\ 2n-p,\ n+m,\ n+p,\ 2n-m,\ n-p,\ m,\ 2n-m-p,\ p+m,\ p,\ n-m,\ n,$$

ja tapauksessa (2) polynomi on edelleen muodossa

$$\begin{aligned} &\varepsilon_3x^{2n} + \varepsilon_2x^{2n-p} + \varepsilon_1x^{2n-m} + \varepsilon_1\varepsilon_3x^{n+m} + \varepsilon_2\varepsilon_3x^{n+p} + \varepsilon_1\varepsilon_2x^{n+m-p} \\ &+ \varepsilon_1x^m + \varepsilon_2x^p + \varepsilon_1\varepsilon_2x^{n+p-m} + \varepsilon_2\varepsilon_3x^{n-p} + \varepsilon_1\varepsilon_3x^{n-m} + \varepsilon_3 + 4x^n, \end{aligned}$$

jolloin taas saamme monomit, joiden asteet ovat

$$2n,\ 2n-p,\ 2n-m,\ n+m,\ n+p,\ n+m-p,\ m,\ p,\ n+p-m,\ n-p,\ n-m,\ n.$$

Näin ollen luku $2n-m-p$ on yhtä suuri kuin yksi luvuista $n+m$, $n+p$ ja $n+m-p$. Nyt

$$2n-m-p = n+m \iff n-2m-p = 0 \iff n = 2m+p > m+p$$

ja

$$2n-m-p = n+p \iff n-m-2p = 0 \iff n = m+2p > m+p,$$

joten yhtälöt $2n-m-p = n+m$ ja $2n-m-p = n+p$ ovat ristiriidasssa oletuksen $n \leq m+p$ kanssa, ja näin ollen siis $2n-m-p = n+m-p$ pitää paikkansa, eli

$$2n-m-p = n+m-p \iff n-2m = 0 \iff n = 2m.$$

Siispä $\beta = n-m = 2m-m = m$, jolloin $(\alpha, \beta) = (p, m)$, jolloin kuten aiemmin nähtiin, polynomi $\psi(x)$ on rekursiivinen.

Kun taas $(\alpha, \beta) = (m, n-p)$, niin tällöin tapauksesta (1) saamme

$$\begin{aligned} &c_0c_nx^{2n} + c_mc_nx^{2n-m} + c_{n-p}c_nx^{n+p} + c_0c_mx^{n+m} + c_0c_{n-p}x^{2n-p} \\ &+ c_0c_mx^{n-m} + c_0c_{n-p}x^p + c_mc_{n-p}x^{2n-p-m} + c_mc_{n-p}x^{m+p} + c_nc_mx^m \\ &+ c_nc_{n-p}x^{n-p} + c_0c_n + 4x^n \end{aligned}$$

eli monomit asteiltaan

$$2n,\ 2n-m,\ n+p,\ n+m,\ 2n-p,\ n-m,\ p,\ 2n-p-m,\ m+p,\ m,\ n-p,\ n.$$

Nämä ovat täsmälleen samat asteet kuin tapauksessa $(\alpha, \beta) = (p, n-m)$, joten tällöin saamme vastaavan tuloksen $n = 2m$. Tällöin $\alpha = m = 2m - m = n - m$, eli $(\alpha, \beta) = (n-m, n-p)$. Siispä, kuten aiemmin nähtiin, $\varphi(x)$ on rekursiivinen.

Tällöin on osoitettu, että jokaisessa mahdollisessa tilanteessa, joko $\varphi(x)$ tai $\varepsilon(x)$ on rekursiivinen. □

Lemma 4.3. *Olkoon λ ja λ^{-1} polynomin $f(x)$ juuria. Tällöin yksi ehtopari pitää paikkansa.*

$$\begin{aligned} &(I) \quad \lambda^n = -\varepsilon_3 \quad ja\ \lambda^{m-p} = -\varepsilon_1\varepsilon_2, \\ &(II) \quad \lambda^m = -\varepsilon_1\varepsilon_3\ ja\ \lambda^{n-p} = -\varepsilon_2, \\ &(III)\ \lambda^p = -\varepsilon_2\varepsilon_3\ ja\ \lambda^{n-m} = -\varepsilon_1. \end{aligned}$$

Todistus. Ehdot $f(\lambda) = 0$ ja $f(\lambda^{-1}) = 0$ voidaan esittää muodossa

$$\lambda^n + \varepsilon_1\lambda^m + \varepsilon_2\lambda^p + \varepsilon_3 = 0,\ \lambda^n + \varepsilon_2\varepsilon_3\lambda^{n-p} + \varepsilon_1\varepsilon_3\lambda^{n-m} + \varepsilon_3 = 0.$$

Vähentämällä ensimmäinen yhtälö toisesta, saamme

$$\begin{aligned} &\left(\lambda^n + \varepsilon_2\varepsilon_3\lambda^{n-p} + \varepsilon_1\varepsilon_3\lambda^{n-m} + \varepsilon_3\right) - \left(\lambda^n + \varepsilon_1\lambda^m + \varepsilon_2\lambda^p + \varepsilon_3\right) = 0 - 0 \\ &\Leftrightarrow \lambda^n + \varepsilon_2\varepsilon_3\lambda^{n-p} + \varepsilon_1\varepsilon_3\lambda^{n-m} + \varepsilon_3 - \lambda^n - \varepsilon_1\lambda^m - \varepsilon_2\lambda^p - \varepsilon_3 = 0 \\ &\Leftrightarrow \varepsilon_2\varepsilon_3\lambda^{n-p} + \varepsilon_1\varepsilon_3\lambda^{n-m} - \varepsilon_1\lambda^m - \varepsilon_2\lambda^p = 0 \\ &\Leftrightarrow \varepsilon_2\varepsilon_3\delta^{n-p} - \varepsilon_1\varepsilon_2^2\varepsilon^m + \varepsilon_1\varepsilon_3\delta^{n-m} - \varepsilon_1^2\varepsilon_2\delta^p = 0 \\ &\Leftrightarrow \left(\varepsilon_2\lambda^{m-p} + \varepsilon_1\right)\left(\varepsilon_3\lambda^{n-m} - \varepsilon_1\varepsilon_2\lambda^p\right) = 0. \end{aligned}$$

Näin ollen joko

$$\begin{aligned} &\varepsilon_2\lambda^{m-p} - \varepsilon_1 = 0 \iff \varepsilon_2\lambda^{m-p} = -\varepsilon_1 \iff \lambda^{m-p} = -\varepsilon_1\varepsilon_2 \\ &\iff \lambda^p = -\varepsilon_1\varepsilon_2\lambda^m \end{aligned}$$

tai

$$\varepsilon_3\lambda^{n-m} - \varepsilon_1\varepsilon_2\lambda^p = 0 \iff \varepsilon_3\lambda^{n-m} = \varepsilon_1\varepsilon_2\lambda^p \iff \lambda^p = \varepsilon_1\varepsilon_2\varepsilon_3\lambda^{n-m}.$$

Kun nämä muuttujan λ^p arvot laitetaan yhtälöön $f(\lambda) = 0$, saamme joko että

$$\begin{aligned} &f(\lambda) = 0 \iff \lambda^n + \varepsilon_1\lambda^m + \varepsilon_2\lambda^p + \varepsilon_3 = 0 \\ &\iff \lambda^n + \varepsilon_1\lambda^m + \varepsilon_2(-\varepsilon_1\varepsilon_2\lambda^m) + \varepsilon_3 = 0 \iff \lambda^n + \varepsilon_1\lambda^m - \varepsilon_1\varepsilon_2^2\lambda^m = -\varepsilon_3 \\ &\iff \lambda^n + \varepsilon_1\lambda^m - \varepsilon_1\lambda^m = -\varepsilon_3 \iff \lambda^n = -\varepsilon_3, \end{aligned}$$

jolloin siis molemmat $\lambda^n = -\varepsilon_3$ ja $\lambda^{m-p} = -\varepsilon_1\varepsilon_2$ pätevät ja (I) toteutuu, tai

$$\begin{aligned} f(\lambda) = 0 &\iff \lambda^n + \varepsilon_1\lambda^m + \varepsilon_2\lambda^p + \varepsilon_3 = 0 \\ &\iff \lambda^n + \varepsilon_1\lambda^m + \varepsilon_2(\varepsilon_1\varepsilon_2\varepsilon_3\lambda^{n-m}) + \varepsilon_3 = 0 \\ &\iff \lambda^n + \varepsilon_1\lambda^m + \varepsilon_1\varepsilon_2^2\varepsilon_3\lambda^{n-m} + \varepsilon_3 = 0 \\ &\iff \lambda^n + \varepsilon_1\lambda^m + \varepsilon_1\varepsilon_3\lambda^{n-m} + \varepsilon_3 = 0 \\ &\iff (\lambda^m + \varepsilon_1\varepsilon_3)\left(\lambda^{n-m} + \varepsilon_1\right) = 0. \end{aligned}$$

Tällöin joko $\lambda^m + \varepsilon_1\varepsilon_3 = 0$ tai $\lambda^{n-m} + \varepsilon_1 = 0$. Siispä joko

$$\begin{aligned} \lambda^m + \varepsilon_1\varepsilon_3 = 0 &\iff \lambda^m = -\varepsilon_1\varepsilon_3 \text{ ja } \lambda^p = \varepsilon_1\varepsilon_2\varepsilon_3\lambda^{n-m} \\ &\iff \lambda^{n-m} = \varepsilon_1\varepsilon_2\varepsilon_3\lambda^p = \varepsilon_1\varepsilon_2\varepsilon_3(-\varepsilon_1\varepsilon_3) = -\varepsilon_1^2\varepsilon_2\varepsilon_3^2 = -\varepsilon_2, \end{aligned}$$

jolloin $\lambda^m = -\varepsilon_1\varepsilon_2$ ja $\lambda^{n-p} = -\varepsilon_2$, eli (II) toteutuu. Tai vastaavasti

$$\begin{aligned} \lambda^{n-m} + \varepsilon_1 = 0 &\iff \lambda^{n-m} = -\varepsilon_1 \text{ ja} \\ \lambda^p = \varepsilon_1\varepsilon_2\varepsilon_3\lambda^{n-m} &= \varepsilon_1\varepsilon_2\varepsilon_3(-\varepsilon_1) = -\varepsilon_1^2\varepsilon_2\varepsilon_3 = -\varepsilon_2\varepsilon_3, \end{aligned}$$

jolloin $\lambda^p = -\varepsilon_2\varepsilon_3$ ja $\lambda^{n-m} = -\varepsilon_1$, eli (III) toteutuu.

Näin ollen siis aina joko (I) toteutuu, (II) toteutuu, tai (III) toteutuu. □

Lemmojen 4.2 ja 4.3 avulla on helppo osoittaa seuraavat kaksi lausetta, jotka vuorostaan johtavat täyteen kuvaukseen muotoa $x^n + \varepsilon x^m + \varepsilon_2 x^p + \varepsilon_3$ olevista jaottomista polynomeista. Molemmissa lauseissa (kuten myös Lemmoissa 4.2 ja 4.3) oletetaan, että $n \leq m + p$ ja $f(x) \neq (c^m + \varepsilon_2)(x^p + \varepsilon_1)$.

Määritelmä 4.4. Luku $c \in \mathbb{C}$ on *ykkösen juuri*, mikäli sille pätee $c^n = 1$ jollakin $n \in \mathbb{Z}_+$. [2]

Lause 4.5. *a) Mikäli polynomilla $f(x)$ ei ole juuria, jotka ovat ykkösen juuria niin polynomi $f(x)$ on jaoton.*

b) Mikäli polynomilla $f(x)$ on tasan q juurta jotka ovat ykkösen juuria, tällöin polynomi $f(x)$ voidaan esittää kahden kokonaislukukertoimisen polynomin tulona, joista toinen on astetta q ja jonka juuret ovat nämä ykkösen juuret, kun taas toinen on jaoton.

Todistus. Olkoon $f(x) = \varphi(x)\psi(x)$, missä $\varphi, \psi \in \mathbb{Z}[x]$. Lemman 4.2 perusteella jomman kumman polynomeista φ ja ψ on oltava rekursiivinen. Valitaan nämä polynomit niin, että φ on rekursiivinen. Tällöin voimme olettaa, että jos λ on polynomin φ juuri, niin tällöin myös λ^{-1} on polynomin φ juuri. Tämä johtuu siitä, että polynomin φ rekursiivisuuden perusteella jos $\varphi(\lambda) = 0$, niin $\pm x^s\varphi(\lambda^{-1}) = 0 \iff \varphi(\lambda^{-1}) = 0$.

Näin ollen Lemmasta 4.3 seuraa, että λ on ykkösen juuri. Tämä johtuu siitä, että välttämättä joko $\lambda^n = -\varepsilon_3 = \pm 1$ jolloin $\lambda^{2n} = 1$, $\lambda^m = -\varepsilon_1\varepsilon_3 = \pm 1$, jolloin $\lambda^{2m} = 1$ tai $\lambda^p = -\varepsilon_2\varepsilon_3 = \pm 1$, jolloin $\lambda^{2p} = 1$. Näin ollen nähdään, että mikäli polynomi f on jaollinen, on sillä oltava juuri, joka on ykkösen juuri. Siispä, jos polynomilla f ei ole ykkösen juuria, on se jaoton.

Jos kaikki polynomin f juurista eivät ole ykkösen juuria, niin tällöin polynomilla ψ on oltava juuria, jotka eivät ole ykkösen juuria. Tällöin joko polynomi ψ on jaoton kunnassa $\mathbb{Z}$ tai kuten polynomin f tapauksessa $\psi = \psi_1\psi_2$, jossa $\psi_1, \psi_2 \in \mathbb{Z}[x]$ ja kaikki polynomin ψ_1 juuret ovat ykkösen juuria, kun taas polynomilla ψ_2 on juuri, joka ei ole ykkösen juuri. Tällöin kaikki juuret $\varphi\psi_1$ ovat ykkösen juuria. Jatkamalla saman menetelmän käyttöä polynomiin ψ_2, saavutamme halutun polynomin f tekijöihin jaon. □

Pitää vielä määrittää, milloin polynomilla f on juuria, jotka ovat ykkösen juuria. Vastaus saadaan seuraavasta lauseesta.

Lause 4.6. $f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3$, $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm 1$, $\varepsilon_3 = \pm 1$.
Olkoon d lukujen n, m ja p suurin yhteinen tekijä. Asetetaan

$$n_1 = \frac{n}{d},\ m_1 = \frac{m}{d},\ p_1 = \frac{p}{d},$$
$$d_1 = \operatorname{syt}(n_1, m_1 - p_1),\ d_2 = \operatorname{syt}(m_1, n_1 - p_1),\ d_3 = \operatorname{syt}(p_1, n_1 - m_1).$$

Tällöin mikä tahansa ykkösen juuri, joka on polynomin f juuri, toteuttaa yhden yhtälöistä

$$x^{dd_1} = \pm 1,\ x^{dd_2} = \pm 1,\ x^{dd_3} = \pm 1$$

ja se on polynomin f yksinkertainen juuri.

Todistus. Olkoon λ ykkösen juuri, joka on polynomin f juuri. Tällöin λ^{-1} on myös polynomin f juuri. Lemma 4.3 antaa kolme mahdollista ehtoa luvulle λ. Tutkitaan ensin tapausta (I): $\lambda^n = -\varepsilon_3$ ja $\lambda^{m-p} = -\lambda_1\lambda_2$. Nyt

$$\operatorname{syt}(n, m-p) = \operatorname{syt}(d \cdot n_1, d \cdot m_1 - d \cdot p_1) = d \cdot \operatorname{syt}(n_1, m_1 - p_1) = dd_1,$$

ja näin ollen on olemassa sellaiset kokonaisluvut u ja v, että $dd_1 = nu + (m-p)v$. Näin ollen $\lambda^{dd_1} = \lambda^{nu+(m-p)v} = (\lambda^n)^u(\lambda^{m-p})^v = \pm 1$, sillä $\lambda^n = -\varepsilon_3 = \pm 1$ ja $\lambda^{m-p} = -\varepsilon_1\varepsilon_3 = \pm 1$. Tapaukset (II) saamme vastaavasti

$$\lambda^{dd_2} = \lambda^{mu+(n-p)v} = (\lambda^m)^u \left(\lambda^{n-p}\right)^v = \pm 1$$

ja tapauksessa (III) saamme

$$\lambda^{dd_3} = \lambda^{pu+(n-m)v} = (\lambda^p)^u \left(\lambda^{n-m}\right)^v = \pm 1.$$

Jää todistettavaksi vain, että λ on polynomin f yksinkertainen juuri, eli että

$$\lambda f'(\lambda) = n\lambda^n + \varepsilon_1 m\lambda^m + \varepsilon_2 p\lambda^p \neq 0.$$

Asettamalla ehdot (I), (II) ja (III) yhtälöön $n\lambda^n+\varepsilon_1 m\lambda^m+\varepsilon_2 p\lambda^p = 0$ saamme vastaavasti

$$\varepsilon_2\lambda^p(p-m) = n\varepsilon_3, \varepsilon_3\lambda^p(p-n) = m\varepsilon_3,\ \varepsilon_1\lambda^m(m-n) = p\varepsilon_2\varepsilon_3.$$

Yhtälöä $|\lambda| = 1$ ei voida saada ensimmäisestä tapauksesta, kun taas toisessa ja kolmannessa se tarkoittaa, että $n = m + p$. Jos $n = m + p$, tapauksen (II) yhtälöt ottavat muodot $\lambda^m = -\varepsilon_1\varepsilon_3$ ja $\lambda^m = -\varepsilon_2$, kun taas tapauksen (III) yhtälöt ottavat muodot $\lambda^p = -\varepsilon_2\varepsilon_3$ ja $\lambda^p = -\varepsilon_1$. Kummassakin tapauksessa $\varepsilon_3 = \varepsilon_1\varepsilon_2$, jolloin saadaan

$$\begin{aligned} f(x) &= x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3 = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_1\varepsilon_2 \\ &= \left(x^{n+p} + \varepsilon_2\right)\left(x^p + \varepsilon_1\right) = \left(x^m + \varepsilon_2\right)\left(x^p + \varepsilon_1\right) \end{aligned}$$

Tämä polynomi on kuitenkin aiemmin jätetty pois tarkastelusta, joten saavutaan ristiriitaan. Näin ollen λ on polynomin f yksinkertainen juuri. □

Lähdeluettelo

[1] Victor V. Prasolov: *Polynomials*. Moscow, 2004.

[2] Roots of Unity, Brilliant.org. Haettu 10.1.2023, https://brilliant.org/wiki/roots-of-unity/