JYVÄSKYLÄN YLIOPISTO
MATEMATIIKAN JA TILASTO-
TIETEEN LAITOS

Pro gradu-tutkielma

Primitiiviset juuret ja niiden sovellukset

Matti Mörsky

1. kesäkuuta 2024

Tekijä
Matti Mörsky

Otsikko
Primitiiviset juuret ja niiden sovellukset (engl. Primitive roots and their applications)

Tutkinto-ohjelma
Matematiikan aineenopettajan maisteriohjelma

Päivämäärä	**Sivumäärä**
1. kesäkuuta 2024	41

Tiivistelmä

Tässä työssä tutkitaan primitiivisiä juuria ja niiden erilaisia sovelluksia. Sovelluksissa käydään läpi rationaalilukujen desimaaliesityksen ominaisuuksia, näennäissatunnauslukugeneraattorin teoriaa ja indeksiaritmetiikkaa.

Aluksi työssä käydään läpi olennaisia määritelmiä, esimerkkejä ja lauseita, joiden jälkeen määritellään primitiivinen juuri. Primitiivinen juuri on yksiköiden ryhmän U_n virittävä alkio. Tällöin yksiköiden ryhmä on syklinen. Hyödyllisen apulauseen avulla voidaan testata, onko jokin alkio primitiivinen juuri. Seuraavaksi tutkitaan syklisiä yksiköiden ryhmiä ja todistetaan, että alkuluvuille p löytyy aina primitiivinen juuri yksiköiden ryhmästä U_p. Lisäksi huomataan syklisten ryhmien välisiä yhteyksiä ja määritetään primitiivisten juurien määrä Eulerin funktion avulla.

Primitiivisten juurten sovelluksissa tutkitaan rationaalilukujen desimaaliesityksien jaksollisuutta. Ensin selvitetään, milloin rationaaliluku on päättyvä. Huomataan, että jos luvun $1/n$ desimaaliesitys on päättymätön, niin se on jaksollinen ja sen jakson pituus on korkeintaan $n - 1$. Lisäksi, jos 10 on primitiivinen juuri modulo n, niin desimaaliesityksen pituus on kertaluku $\phi(n)$.

Tämän jälkeen tarkastellaan näennäissatunnaislukuja tuottavaa menetelmää ja primitiivisten juurten käyttöä näennäissatunnaisgeneraattorissa. Hyödyllisen lauseen avulla voidaan löytää primitiivisen juuren potensseista vielä suurempia primitiivisiä juuria, jolloin näennäissatunnaislukujen löytäminen vaikeutuu. Lopuksi hyödynnetään vielä primitiivisiä juuria määrittelemään indeksi, jota voidaan hyödyntää kongruenssiyhtälöiden ratkaisemisessa sekä määrittäessä onko kongruenssiyhtälöllä ratkaisua ja kuinka monta niitä on.

Sisällys

Johdanto

Tämän tutkielman tarkoituksena on tutkia primitiivisiä juuria ja niiden erilaisia käyttötarkoituksia. Esitietokappaleessa pyritään käymään tärkeimmät määritelmät ja lauseet työssä käsiteltävien aiheiden kannalta. Lukijan oletetaan kuitenkin tuntevan Lukuteorian ja Algebran perusteita. Erityisesti näistä aihealueista tärkeitä ovat jaollisuus, suurin yhteinen tekijä, alkuluvut, kongruenssit, jäännösluokat, ryhmät ja yksiköt. Näihin aiheisiin voi tutustua lähdeluettelosta löytyvien *Dudleyn* [1], *D&F*:n [2] ja *H&W*:n [3] kirjojen avulla.

Alkio a renkaassa Z_n on yksikkö, jos ja vain jos $\text{syt}(a, n) = 1$. Primitiivinen juuri on yksiköiden ryhmän U_n virittävä alkio. Primitiivisiä juuria voidaan tarkastella syklisten yksiköiden ryhmien avulla. Yksiköiden ryhmä U_n on syklinen, jos jokin sen alkio virittää koko tämän ryhmän. Tällöin yksiköiden määrä on $|U_n| = \phi(n)$, missä $\phi(n)$ on Eulerin funktio. Syklisen ryhmän U_n virittäjien etsiminen on kuitenkin työläs tapa etsiä primitiivisiä juuria. Apulauseen avulla saadaan, että alkio $a \in U_n$ on primitiivinen juuri, jos ja vain jos $a^{\phi(n)/q} \not\equiv 1 \pmod{n}$, kaikilla alkuluvuilla q, jotka jakavat luvun $\phi(n)$. Tällöin esimerkiksi ryhmälle $|U_5| = \phi(5) = 4$ alkio 2 on primitiivinen juuri, sillä ainoa alkuluku, joka jakaa kertaluvun $\phi(5)$ on $q = 2$ ja tällöin $2^{4/2} = 2^2 = 4 \not\equiv 1 (\text{mod } n)$.

Seuraavaksi käydään läpi millä luvuilla n yksiköiden ryhmä U_n on syklinen. Havaitaan, että kun p on alkuluku, niin yksiköiden ryhmä U_p on syklinen. Lisäksi huomataan, että yksiköiden ryhmät U_{p^e} ovat syklisiä, kun p on pariton alkuluku. Tästä päästään hyödylliseen tulokseen, jonka mukaan löydettäessä primitiivinen juuri $g \pmod{p}$ riittää näyttää, että se on primitiivinen juuri $g \pmod{p^2}$, niin se on primitiivinen juuri myös $g \pmod{p^e}$ kaikilla kokonaisluvuilla $e \geq 1$. Nämä Lauseet 3.1 – 3.3 ovat työn teoreettisia päätuloksia. Lisäksi m alkion syklisellä ryhmällä on $\phi(n)$ virittäjää. Jos luvulla n on primitiivinen juuri, niin yksiköiden ryhmä U_n on $\phi(n)$ alkion syklinen ryhmä. Siis luvulla n on $\phi(\phi(n))$ primitiivistä juurta.

Tutkielmassa tutustutaan primitiivisten juurten sovelluksiin. Näitä ovat rationaaliluvun desimaaliesityksen jakso, näennäissatunnaisluvut ja indeksiaritmetiikka. Aluksi tutkitaan rationaaliluvun desimaaliesitystä $1/n$ ja erityisesti nimittäjää n. Rationaaliluvun $1/n$ desimaaliesitys on päättyvä, jos ja vain jos $n = 2^a 5^b$, missä $a, b \in \mathbb{N}$. Jos taas luvun $1/n$ desimaaliesitys on päättymätön, niin se on jaksollinen ja jakson pituus on korkeintaan $n - 1$. Esimerkiksi desimaaliesitys rationaaliluvulle $1/17 =, \overline{0588235294117647}$, missä

jakson pituus on $17-1=16$. Työssä havaitaan myös, että jos 10 on primitiivinen juuri modulo n, niin luvun $1/n$ desimaaliesityksen pituus on kertaluku $\phi(n)$ ja muutoin se on tätä lyhyempi. Erityisesti siis, jos 10 on primitiivinen juuri modulo p, missä p on alkuluku, niin luvun $1/p$ desimaaliesityksen jakson pituus $\phi(p) = p - 1$.

Salausavaimissa ja salausprotokollissa hyödynnetään näennäissatunnaislukuja. Näennäissatunnaisluvut ovat jollain menetelmällä tuotettuja kokonaislukujonoja, joissa luvut vaikuttavat täysin satunnaisilta. Eräs tälläinen menetelmä on puhtaasti multiplikatiivinen kongruenssimenetelmä, johon tutustutaan tässä tutkielmassa. Siinä satunnaisluvut tuotetaan rekursiivisella kongruenssiyhtälöllä, johon primitiivisten juurten käyttö soveltuu hyvin sen maksimaalisen jakson pituuden ansiosta. Esimerkiksi käyttämällä Mersennen alkulukua $M_{31} = 2^{31} - 1$ kongruenssiyhtälön modulona ja etsimällä tälle primitiivinen juuri a generaattoriksi saadaan tuotettua näennäissatunnaislukuja. Lisäksi hyödynnetään lausetta, jonka mukaan löydetään primitiivisen juuren modulo m potensseista r^u suurempia primitiivisiä juuria, jos $\text{syt}(u, \phi(m)) = 1$. Tuotetut näennäissatunnaisluvut saadaan vielä välille $[0, 1]$, kun jaetaan ne luvulla m.

Primitiivisiä juuria hyödynnetään myös vaikeampien kongruenssiyhtälöiden ratkaisemisessa määrittelemällä indeksi $\text{ind}_r\, a$, joka kertoo millä primitiivisen juuren r potenssilla saadaan alkio a modulossa n. Esimerkiksi, kun 3 on primitiivinen juuri modulo 5 ja $3^2 \equiv 4 \pmod 5$, niin $\text{ind}_3\, 4 = 2$. Indekseille määritellään myös hyödyllisiä laskuominaisuuksia, joita käytetään kongruenssiyhtälöiden ratkaisemisessa. Lopuksi vielä määritellään kongruenssiyhtälö $x^k \equiv a \pmod n$, missä k on positiivinen kokonaisluku ja $\text{syt}(a, n) = 1$. Jos tälläisellä yhtälöllä on ratkaisu, niin yksikkö a on k:s potenssijäännös modulo n. Tällöin saadaan myös tulos, jonka mukaan tällä kongruenssiyhtälöllä on ratkaisu, jos ja vain jos $a^{\phi(n)/d} \equiv 1 \pmod n$, missä $d = \text{syt}(k, \phi(n))$. Näitä ratkaisuja on täsmälleen d kappaletta.

1 Esitiedot

Ensimmäiseen lukuun on kerätty tarpeelliset tiedot Lukuteorian ja Algebran tuloksista. Näihin tuloksiin voi perehtyä paremmin teoksista *J&J* [4] ja *Rosen* [5].

Määritelmä 1.1. Olkoot a, b ja n kokonaislukuja sekä $n > 0$. Luku a on *kongruentti* luvun b kanssa modulo n, jos n jakaa luvun $a - b$.

Tällöin merkitään $a \equiv b \pmod{n}$. Luku a on siis kongruentti luvun b kanssa modulo n, jos on olemassa $k \in \mathbb{Z}$ siten, että $a - b = kn$.

Esimerkki 1.2. $27 \equiv 7 \pmod{10}$, sillä $27 - 7 = 20 = 2 \cdot 10$

Lemma 1.3. *Jos kokonaisluvuille* a, b, c, n *sekä* $n > 0$ *pätee* $\text{syt}(c, n) = 1$ *ja* $ac \equiv bc \pmod{n}$*, niin* $a \equiv b \pmod{n}$.

Todistus. Katso [5, Corollary 4.4.1.].

□

Esimerkki 1.4. $\text{syt}(3, 7) = 1$ ja $27 \cdot 3 \equiv 6 \cdot 3 \pmod{7}$, niin $27 \equiv 6 \pmod{7}$, sillä

$$27 \cdot 3 - 6 \cdot 3 = 81 - 18 = 63 \equiv 0 \pmod{7} \text{ ja } 27 - 6 = 21 \equiv 0 \pmod{7}.$$

Määritelmä 1.5. Olkoot a ja n kokonaislukuja ja $n > 0$. Luvun a *jäännösluokka* modulo n on niiden kokonaislukujen joukko, jotka ovat kongruentit luvun a kanssa modulo n.

Tällöin merkitään

$$\begin{aligned}[a]_n &= \{b \in \mathbb{Z} : b \equiv a \pmod{n}\} \\ &= \{b \in \mathbb{Z} : b = a + kn, \text{ jollakin } k \in \mathbb{Z}\}.\end{aligned}$$

Esimerkki 1.6. Jäännösluokat, kun $n = 5$:

$$[0]_5 = \{\dots, -15, -10, -5,\ 0,\ 5,\ 10,\ 15, \dots\},$$
$$[1]_5 = \{\dots, -14, -9, -4,\ 1,\ 6,\ 11,\ 16, \dots\},$$
$$[2]_5 = \{\dots, -13, -8, -3,\ 2,\ 7,\ 12,\ 17, \dots\},$$
$$[3]_5 = \{\dots, -12, -7, -2,\ 3,\ 8,\ 13,\ 18, \dots\},$$
$$[4]_5 = \{\dots, -11, -6, -1,\ 4,\ 9,\ 14,\ 19, \dots\}.$$

Tästä eteenpäin jäännösluokat ovat samoja joukkoja, kun aiemmat. Esimerkiksi

$$[5]_5 = \{\dots, -10, -5,\ 0,\ 5,\ 10,\ 15,\ 20 \dots\} = [0]_5 \text{ ja}$$
$$[6]_5 = \{\dots, -9, -4,\ 1,\ 6,\ 11,\ 16,\ 21 \dots\} = [1]_5.$$

Myös negatiiviset jäännösluokat ovat näitä samoja joukkoja. Esimerkiksi

$$[-1]_5 = \{\dots, -16, -11, -6, -1,\ 4,\ 9,\ 14 \dots\} = [4]_5 \text{ ja}$$
$$[-2]_5 = \{\dots, -17, -12, -7, -2,\ 3,\ 8,\ 13 \dots\} = [3]_5.$$

Merkintä 1.7. Kaikkien jäännösluokkien joukkoa modulo n merkitään symbolilla

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}.$$

Esimerkki 1.8. Joukko $\mathbb{Z}_5$ koostuu alkioista $[0]_5$, $[1]_5$, $[2]_5$, $[3]_5$ ja $[4]_5$.

Jatkossa, jos luku n on asiayhteydestä selvä merkitään lyhyemmin $[a]_n = [a]$.

Määritelmä 1.9. Laskutoimituksilla $\oplus$ ja $\odot$ varustettua joukkoa $\mathbb{Z}_n$ kutsutaan *jäännösluokkarenkaaksi.*

Esimerkki 1.10. Jäännösluokassa $\mathbb{Z}_5$ yhteenlaskussa $[2] \oplus [7] = [2+7] = [9] = [2]$ ja kertolaskussa $[4] \odot [6] = [4 \cdot 6] = [24] = [4]$.

Määritelmä 1.11. *Yksiköiden* joukko on

$$U_n = \{[a]_n \in \mathbb{Z}_n : \text{syt}(a, n) = 1\} \subset \mathbb{Z}_n\}.$$

Siispä, kun $\text{syt}(b, n) = 1$ seuraa, että on $b \in \mathbb{Z}$, jolle $[a][b] = 1$. Tällöin $[b]$ on $[a]$:n käänteisalkio.

Lemma 1.12. *U_n on kommutatiivinen ryhmä varustettuna kongruenssiluokkien kertolaskulla [4, Lemma 6.1].*

Kommutatiivisuus tarkoittaa, että ryhmän alkiot ovat vaihdannaisia eli $ab = ba$, kaikille $a, b \in U_n$.

Esimerkki 1.13. Mahdollisia U_{10} joukon muodostavia jäännösluokkia ovat

$$[0], [1], [2], [3], [4], [5], [6], [7], [8], [9].$$

Nyt tarkastellaan jäännösluokkien joukon alkioiden suurinta yhteistä tekijää luvun $n = 10$ kanssa:

$$\text{syt}(0, 10) = 10,\ \text{syt}(1, 10) = 1,\ \text{syt}(2, 10) = 5,\ \text{syt}(3, 10) = 1,\ \text{syt}(4, 10) = 2,$$
$$\text{syt}(5, 10) = 5,\ \text{syt}(6, 10) = 2,\ \text{syt}(7, 10) = 1,\ \text{syt}(8, 10) = 2 \ \text{ ja } \ \text{syt}(9, 10) = 1.$$

Yksiköiden joukko on siis $U_{10} = \{[1], [3], [7], [9]\}$.

Määritelmä 1.14. Olkoon a ja n positiivisia kokonaislukuja, joille $\text{syt}(a, n) = 1$. Tällöin pienin positiivinen kokonaisluku x, jolle pätee $a^x \equiv 1 \pmod{n}$ on *kertaluku* $\text{ord}_n a$.

Esimerkki 1.15. Luvulle 3 modulo 10 saadaan laskemalla

$$3^1 \equiv 3 \pmod{10},\ 3^2 \equiv 9 \pmod{10},$$
$$3^3 = 27 \equiv 7 \pmod{10}, 3^4 = 81 \equiv 1 \pmod{10}.$$

Siispä kertaluku $\text{ord}_{10} 3 = 4$.

Määritelmä 1.16. Kertaluku $\phi(n) = |U_n|$ on yksiköiden lukumäärä renkaassa $\mathbb{Z}_n$.

Tätä funktiota $\phi : \mathbb{N} - \{0\} \to \mathbb{N}$ kutsutaan Eulerin funktioksi.

Esimerkki 1.17. $U_7 = \{[1], [2], [3], [4], [5], [6]\}$, joten $\phi(7) = |U_7| = 6$.

Lemma 1.18. *Jos $n = p^e$, missä p on alkuluku, niin*

$$\phi(p^e) = p^{e-1}(p-1).$$

Todistus. Katso [4, Lemma 5.4]. □

Yksiköiden joukoille U_p kertaluku $\phi(p) = p - 1$, kun p on alkuluku.

Esimerkki 1.19. Ryhmän U_{13} kertaluku $\phi(13) = 13 - 1 = 12$.

Määritelmä 1.20. Ryhmä G on syklinen, jos $G = \{a^k : k \in \mathbb{Z}\}$, jollain $a \in G$.

Esimerkki 1.21. Ryhmän $U_5 = \{[1], [2], [3], [4]\}$ alkiolle pätee

$$[2]^1 = [2],\ [2]^2 = [4],\ [2]^3 = [8] = [3],\ [2]^4 = [16] = [1].$$

Siispä kaikki ryhmän U_5 alkiot ovat muotoa $[2]^k$ ja ryhmä on syklinen.

Lause 1.22. *Jos p on on alkuluku ja $a \not\equiv 0 \pmod{p}$, niin*

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

Todistus. Katso [4, Theorem 4.3]. □

Tämä lause tunnetaan myös nimellä Fermat'n pieni lause.

Lause 1.23. *Jos* $n \geq 1$*, niin*

$$\sum_{d|n} \phi(d) = n,$$

missä summa on yli kaikkien positiivisten lukujen d*, jotka jakavat luvun* n*.*

Todistus. Katso [4, Theorem 5.8]. □

Lause 1.24. *Jos* $\text{syt}(a, n) = 1$*, niin* $a^{\phi(n)} \equiv 1 \pmod{n}$ *[4, Theorem 5.3].*

Tämä lause tunnetaan myös Eulerin lauseena.

Lause 1.25. *Jos* $\text{syt}(a, n) = 1$*, niin* $a^i \equiv a^j \pmod{n}$*, missä* i *ja* j *ovat ei-negatiivisia kokonaislukuja, jos ja vain jos* $i \equiv j \pmod{\text{ord}_n a}$*.*

Todistus. Katso [5, Theorem 9.2]. □

Lause 1.26. *Olkoon* $n \in \mathbb{N} - \{0\}$ *ja* $a, b \in \mathbb{Z}$*,* $a \neq 0$*.*

1. *Jos* $\text{syt}(a, n) \nmid b$*, niin lineaarisella kongruenssiyhtälöllä*

   $$ax \equiv b \pmod{n}$$

   ei ole ratkaisua.

2. *Jos* $\text{syt}(a, n) \mid b$*, niin lineaarisella kongruenssiyhtälöllä*

   $$ax \equiv b \pmod{n}$$

   on $\text{syt}(a, n)$ *ratkaisua modulo* n*.*

Todistus. Katso [5, Theorem 4.10]. □

2 Primitiivinen juuri

Tässä luvussa määritellään luonnollisen luvun n primitiivinen juuri ja todistetaan Lemma 2.3, joka helpottaa primitiivisten juurien etsimistä. Lisäksi tutustutaan primitiivisiin juuriin erilaisten esimerkkien avulla.

Tutkitaan yksiköitä $a \in U_n$ laskemalla niiden kertalukuja määritelmän 1.14 mukaan. Tällöin pienin positiivinen kokonaisluku x, jolle pätee $a^x \equiv 1 \pmod{n}$ on kertaluku $\operatorname{ord}_n a$. Yksiköitä on $\phi(n)$ kappaletta määritelmän 1.16 mukaan. Nyt siis, koska yksiköille pätee $\operatorname{syt}(a, n) = 1$, niin Eulerin lauseen 1.24 nojalla $a^{\phi(n)} \equiv 1 \pmod{n}$.

Primitiivisten juurien löytämisessä tarvitaan siis apuna yksiköiden ryhmiä, joissa nimenomaan kokonaisluvut a ja n ovat keskenään jaottomat ja niitä on täsmälleen $\phi(n)$ kappaletta. Käydään nyt läpi eri tapoja selvittää primitiivisiä juuria [4].

Määritelmä 2.1. Jos U_n on syklinen, niin U_n:n virittävät alkiot ovat *primitiivisiä juuria.*

Toisin sanoen, jos $\operatorname{syt}(a, n) = 1$ ja kertaluku $\operatorname{ord}_n a = \phi(n)$, niin a on primitiivinen juuri mod n. Tällöin yksikkö a virittää koko yksiköiden ryhmän ja ryhmä U_n on siis määritelmän 1.20 mukaan syklinen.

Esimerkki 2.2. Esimerkissä 1.21 todetaan, että ryhmä U_5 on syklinen. Nyt siis ryhmän alkioista primitiivisiä juuria ovat ne, jotka virittävät koko ryhmän U_5. Selvitetään kokeilemalla, mitkä alkioista tekevät näin:

[1] potenssiin mikä tahansa luku tuottaa vain alkion [1], joten $\operatorname{ord}_5 1 = 1 \neq \phi(5)$ ja [1] ei ole primitiivinen juuri.

$[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [8] = [3]$, $[2]^4 = [16] = [1]$, joten $\operatorname{ord}_5 2 = 4 = \phi(5)$ ja [2] on primitiivinen juuri.

$[3]^1 = [3]$, $[3]^2 = [9] = [4]$, $[3]^3 = [27] = [2]$, $[3]^4 = [81] = [1]$, joten $\operatorname{ord}_5 3 = 4 = \phi(5)$ ja [3] on primitiivinen juuri.

$[4]^1 = [4]$, $[4]^2 = [16] = [1]$, $[4]^3 = [64] = [4]$, $[4]^4 = [256] = [1]$, joten $\operatorname{ord}_5 4 = 2 \neq \phi(5)$ ja [4] ei ole primitiivinen juuri.

Jatkossa jätetään jäännösluokan merkintä [ ] pois helpottamaan merkintöjä.

Lemma 2.3. *Alkio $a \in U_n$ on primitiivinen juuri, jos ja vain jos*

$$a^{\phi(n)/q} \not\equiv 1 \bmod n,$$

kaikilla alkuluvuilla q, jotka jakavat luvun $\phi(n)$.

Todistus. ($\Leftarrow$) Jos a on primitiivinen juuri, niin sillä on kertaluku $\phi(n) = |U_n|$, niin että $a^i \neq 1 \pmod{n}$ kaikilla i, joille pätee $1 \leq i \leq \phi(n)$. Erityisesti $i = \phi(n)/q$ jokaiselle q, joka jakaa $\phi(n)$:n.
($\Rightarrow$) Jos a ei ole primitiivinen juuri, niin $\operatorname{ord}_n a$ on Lagrangen lauseen nojalla $\phi(n)$:n tekijä. Tällöin $\operatorname{ord}_n a \neq \phi(n)$. Tästä seuraa, että $\frac{\phi(n)}{\operatorname{ord}_n a} > 1$. Oletetaan nyt, että $q \mid \frac{\phi(n)}{\operatorname{ord}_n a}$, kun q on alkuluku. Nyt siis $\frac{\phi(n)}{\operatorname{ord}_n a} = q \cdot b$. Josta saadaan $\frac{\phi(n)}{q} = \operatorname{ord}_n a \cdot b$. Saadaan siis lopulta, että

$$a^{\phi(n)/q} = a^{\operatorname{ord}_n a \cdot b} = (a^{\operatorname{ord}_n a})^b \equiv 1^b = 1 \pmod{n}.$$

Tässä on ristiriita alkuperäiseen väitteeseen, joten a:n on oltava primitiivinen juuri.

□

Esimerkki 2.4. Etsitään primitiivisiä juuria, kun $n = 5$. Tälle lemman 1.18 nojalla $|U_5| = 5 - 1 = 4$. Ainoa alkuluku, joka jakaa luvun 4 on 2. Nyt siis

$$1^{4/2} = 1^2 = 1 \equiv 1 \pmod{5}$$

Siispä 1 ei ole primitiivinen juuri modulo 5. Edelleen

$$2^2 = 4 \not\equiv 1 \pmod{5}$$

Siispä 2 on primitiivinen juuri modulo 5.

$$3^2 = 9 \equiv 4 \not\equiv 1 \pmod{5}$$

Siispä 3 on primitiivinen juuri modulo 5.

$$4^2 = 16 \equiv 1 \pmod{5}$$

Siispä 4 ei ole primitiivinen juuri modulo 5.

Saadaan siis sama tulos kuin esimerkissä 2.2.

Esimerkki 2.5. Etsitään primitiivisiä juuria, kun $n = 19$. Tälle lemman 1.18 nojalla $|U_{19}| = 18$. Alkuluvut, jotka jakavat luvun 18 ovat 2 ja 3. Nyt siis

$$2^{18/2} = 2^9 = 512 \equiv 18 \not\equiv 1 \pmod{19}$$
$$2^{18/3} = 2^6 = 64 \equiv 7 \not\equiv 1 \pmod{19}$$

Siispä 2 on primitiivinen juuri modulo 19.

$$3^9 = 19\,683 \equiv 18 \not\equiv 1 \pmod{19}$$
$$3^6 = 729 \equiv 7 \not\equiv 1 \pmod{19}$$

Siispä 3 on primitiivinen juuri modulo 19.

$$4^9 = 262\,144 \equiv 1 \equiv 1 \pmod{19}$$
$$4^6 = 4096 \equiv 11 \not\equiv 1 \pmod{19}$$

Siispä 4 ei ole primitiivinen juuri modulo 19.

Samaan tapaan seuraava primitiivinen juuri löytyy, kun $n = 10$, sillä

$$10^9 = 1\,000\,000\,000 \equiv 18 \not\equiv 1 \pmod{19}$$
$$10^6 = 1\,000\,000 \equiv 11 \not\equiv 1 \pmod{19}$$

Siispä 10 on primitiivinen juuri modulo 19.

Muita primitiivisiä juuria modulo 19 ovat 13, 14 ja 15.

3 Sykliset yksiköiden ryhmät

Tässä luvussa todistetaan työn keskeisimmät tulokset Lauseet 3.1 – 3.3 ja luvun tärkein lähde on *J&J* [4].

Kappaleessa 2 määriteltiin, että jos yksiköiden ryhmä U_n on syklinen, niin sen virittävät alkiot ovat primitiivisiä juuria. Käydään seuraavaksi läpi, millä luvuilla n yksiköiden ryhmä U_n on syklinen ja todistetaan osa näistä tapauksista.

Lause 3.1. *Jos p on alkuluku, niin U_p on syklinen.*

Tämän todistamiseen tarvitaan toista lausetta. Sovelletaan sitä lauseen 3.1 todistamiseen valinnalla $d = p - 1$.

Lause 3.2. *Jos p on alkuluku ja $d \mid p-1$, niin ryhmässä U_p on $\phi(d)$ alkiota, jonka kertaluku on d.*

Toisin sanoen edellinen lause sanoo, että ryhmässä U_p on $\phi(p-1)$ alkiota, jonka kertaluku on $p-1$. Nämä alkiot ovat siis ryhmän U_p virittäjiä.

Lauseen 3.2 todistus. Määritellään jokaiselle d, joka jakaa $p-1$:n joukko

$$\Omega_d = \{a \in U_p : \operatorname{ord} a = d\}$$

ja merkitään $\omega(d) = |\Omega_d|$.

Tavoitteena on osoittaa, että $\omega(d) = \phi(d)$ kaikilla d. Määritelmän 1.22 avulla tiedetään, että $\operatorname{ord} a \mid |U_p|$. Nyt, jos $b \in U_p$, niin $\operatorname{ord} b \mid |U_p| = p - 1$. Tästä seuraa, että ryhmä voidaan kirjoittaa erillisenä yhdisteenä

$$U_p = \bigsqcup_{d|p-1} \Omega_d \Rightarrow \sum_{d|p-1} \omega(d) = p - 1.$$

Lauseen 1.23 nojalla

$$\sum_{d|p-1} \phi(d) = p - 1.$$

Näistä saadaan siis

$$\sum_{d|p-1} (\phi(d) - \omega(d)) = 0.$$

Nyt, jos pystytään näyttämään, että $\phi(d) \geq \omega(d)$ kaikilla d, niin $\phi(d) = \omega(d)$. Oletetaan, että $a \in \Omega_d$. Tällöin $a^i \neq a^j$ kaikilla $1 \leq i < j \leq d$. Lisäksi pätee $(a^i)^d = a^{id} = (a^d)^i = 1$. Tästä seuraa, että a^i on polynomin $f(x) = x^d - 1$ juuri ryhmässä $\mathbb{Z}_p$. Juuria on korkeintaan d kappaletta, joten kaikki juuret ovat $\{a^1, \ldots, a^d\}$. Katso todistus [5, Theorem 9.7].

Osoitetaan nyt, että $\Omega_d = \{a^i : \text{syt}(i, d) = 1\}$. Jos $b \in \Omega_d$, niin

$$f(b) = b^d - 1 = 0.$$

Siispä $b = a^i$ jollain $1 \leq i \leq d$ ja

$$b^{d/\,\text{syt}(i,d)} = a^{\frac{id}{\text{syt}(i,d)}} = (a^d)^{\frac{i}{\text{syt}(i,d)}} = 1.$$

Jos $\text{syt}(i, d) \geq 1$, niin $\text{ord}(b) \neq d$. Tästä seuraisi, että $b \notin \Omega_d$. Mutta oletuksen mukaan $b \in \Omega_d$, joten $\text{syt}(i, d) = 1$. Nyt on osoitettu siis, että pätee

$$\Omega_d = \{a^i : \text{syt}(i, d) = 1\}.$$

Tästä seuraa, että $\omega(d) \leq \phi(d)$, jolloin lause on todistettu. □

Lause 3.3. *Jos p on pariton alkuluku ($p > 2$), niin U_{p^e} on syklinen ja sillä on $\phi(p^e)$ alkiota.*

Todistus. Lauseen 3.1 todistus käsittelee tapauksen $e = 1$. Oletetaan siis, että $e \geq 2$. Käytetään kolmivaiheista strategiaa, jotta löydetään primitiivinen juuri mod p^e:

1. valitaan primitiivinen juuri g mod p
2. näytetään, että joko g tai $g + p$ on primitiivinen juuri mod p^2
3. näytetään, että jos h on mikään primitiivinen juuri mod p^2, niin h on primitiivinen juuri mod p^e kaikille $e \geq 2$

Valitaan g mod p, missä $g \in \mathbb{Z}$. Tällöin $\operatorname{ord}_p g = p - 1$. Vaihe 1 on siis tehty.

Käydään seuraavaksi läpi vaihe 2. Koska g on primitiivinen juuri $\bmod p$, niin $g \in U_p$. Tällöin $\operatorname{syt}(g, p) = 1$ ja edelleen $\operatorname{syt}(g, p^2) = 1$. Voidaan siis päätellä, että $g \in U_{p^2}$. Lauseen 1.24 nojalla $\operatorname{ord}_{p^2} g \mid \phi(p^2) = p(p-1)$ ja kertaluvulle $\phi(p^2)$ pätee siis $g^{\phi(p^2)} \equiv 1 \pmod{p^2}$. Tällöin myös $g^{\operatorname{ord}_{p^2} g} \equiv 1 \pmod{p(p-1)}$ ja edelleen $g^{\operatorname{ord}_{p^2} g} \equiv 1 \pmod{p}$. Nyt, koska g:n kertaluku mod p on $p - 1$, niin $p - 1 \mid \operatorname{ord}_{p^2} g$. Lisäksi p on alkuluku, joten $\operatorname{ord}_{p^2} g = p(p-1)$ tai $\operatorname{ord}_{p^2} g = p - 1$. Jos $\operatorname{ord}_{p^2} g = p(p-1) = \phi(p^2)$, niin g on primitiivinen juuri mod p^2, kuten halutaan. Käydään siis läpi toinen vaihtoehto eli oletetaan, että $\operatorname{ord}_{p^2} g = p-1$. Olkoon $h = g+p$. Tällöin siis $h \equiv g \pmod{p}$, jolloin h on primitiivinen juuri $\bmod p$. Siis samoin perustein kun edellä $\operatorname{ord}_{p^2} h = p(p-1)$ tai $\operatorname{ord}_{p^2} h = p - 1$. Nyt saadaan

$$\begin{aligned} h^{p-1} &= (g+p)^{p-1} \\ &= g^{p-1} + (p-1)g^{p-2}p + \cdots + p^{p-1} \\ &= g^{p-1} + p^2 g^{p-2} - g^{p-2}p + \cdots + p^{p-1} \\ &\equiv 1 - pg^{p-2} \pmod{p^2} \not\equiv 1 \pmod{p^2}, \end{aligned}$$

koska p ei jaa g:tä. Tämä tarkoittaa, että $\operatorname{ord}_{p^2} h \neq p - 1$, joten täytyy olla $\operatorname{ord}_{p^2} h = p(p-1) = \phi(p^2)$. Siispä h:lla on primitiivinen juuri. Vaihe 2 on siis saatu osoitettua.

Siirrytään vaiheeseen 3. Olkoon h mikä tahansa primitiivinen juuri mod p^2. Käytetään induktiota todistamisessa. Oletetaan nyt, että h on primitiivinen juuri mod p^e kaikilla $e \geq 2$. Olkoon kertaluku $d = \operatorname{ord}_{p^{e+1}} h$. Nyt samaan tapaan, kun kohdassa 2 saadaan

$$d \mid \phi(p^{e+1}) = p^e(p-1).$$

Tällöin myös

$$\phi(p^e) = p^{e-1}(p-1) \mid d,$$

joten $d = p^e(p-1)$ tai $d = p^{e-1}(p-1)$. Jos $d = p^e(p-1)$, niin h on primitiivinen juuri mod p^{e+1}, kuten haluttiin. Tutkitaan siis toista tapausta $d = p^{e-1}(p-1)$.

Oletuksen mukaan h on primitiivinen juuri mod p^e. Tällöin sillä on kertaluku $\phi(p^e) = \operatorname{ord}_{p^e} h = p^{e-1}(p-1)$ ryhmässä U_{p^e}, joten kertaluvun määritelmän nojalla $h^{p^{e-2}(p-1)} \not\equiv 1 \pmod{p^e}$.

Toisaalta $\phi(p^{e-1}) = p^{e-2}(p-1)$, joten lauseen 1.24 nojalla

$$h^{p^{e-2}(p-1)} \equiv 1 \bmod p^{e-1}.$$

Nämä yhdistämällä saadaan $h^{p^{e-2}(p-1)} = 1 + kp^{e-1}$, missä luvulle k pätee $\operatorname{syt}(k,p) = 1$. Tällöin binomilauseen mukaan

$$\begin{aligned} h^{p^{e-1}(p-1)} &= (1+kp^{e-1})^p \\ &= 1 + \binom{p}{1} kp^{e-1} + \binom{p}{2} (kp^{e-1})^2 + \dots \\ &= 1 + p \cdot kp^{e-1} + \frac{p(p-1)}{2} kp^{2e-2} + \dots \\ &= 1 + kp^e + \frac{1}{2} k^2 p^{2e-1}(p-1) + \dots \end{aligned}$$

Nyt koska kolmella pisteellä merkityt suuremmat termit ovat jaollisia luvulla $(p^{e-1})^3$, niin ne ovat jaollisia myös luvulla p^{e+1}, sillä $3(e-1) \geq e+1$, kaikilla $e \geq 2$. Siispä

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e + \frac{1}{2}k^2p^{2e-1}(p-1) \pmod{p^{e+1}}.$$

Koska p on pariton, niin termi $\frac{1}{2}k^2p^{2e-1}(p-1)$ on jaollinen luvulla p^{e+1}, sillä $2e-1 \geq e+1$ kaikilla $e \geq 2$. Tällöin siis

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e \pmod{p^{e+1}}.$$

Tämä osoittaa, että $h^{p^{e-1}(p-1)} \not\equiv 1 \pmod{p^{e+1}}$ ja kohta 3 on osoitettu. Tällöin löydetään primitiivinen juuri mod p^e kaikilla $e \geq 1$, joten näiden virittämä ryhmä U_{p^e} on syklinen määritelmän 2.1 mukaan.

□

Esimerkki 3.4. Näytetään, että $g = 2$ on primitiivinen juuri mod 3^e kaikilla $e \geq 1$. Koska $p = 3$ on alkuluku ja $g = 2$ virittää selvästi U_3:n, niin $g = 2$ primitiivinen juuri mod 3. Nyt riittää näyttää vielä, että g on primitiivinen juuri mod p^2, niin g on primitiivinen juuri mod p^e. Siispä, kun $e = 2$, niin selvitetään onko $g = 2$ primitiivinen juuri mod 9. Lauseen 3.3 vaiheen 2 todistuksen mukaan tällöin kertaluvun U_9:ssä täytyy olla $d = 3(3-1) = 6$ tai $d = 3 - 1 = 2$. Nyt $2^2 = 4 \not\equiv 1 \pmod 9$ ja $2^3 = 8 \not\equiv 1 \pmod 9$, joten Lemman 2.3 nojalla $g = 2$ on primitiivinen juuri modulo 9 ja kertaluku $d = \phi(9) = 6$. Siispä $g = 2$ on primitiivinen juuri mod 3^2 ja Lauseen 3.3 nojalla siten myös primitiivinen juuri mod 3^e kaikilla $e \geq 1$.

Esimerkki 3.5. Myös $g = 7$ on primitiivinen juuri mod 5, sillä

$$7^1 = 7 \equiv 2 \pmod 5,\ 7^2 = 49 \equiv 4 \pmod 5,$$
$$7^3 = 343 \equiv 3 \pmod 5 \text{ ja } 7^4 = 2401 \equiv 1 \pmod 5$$

Kuitenkin $g = 7$ ei ole primitiivinen juuri mod 25, sillä

$$7^4 = 2401 \equiv 1 \pmod{25}, \text{ joten } \operatorname{ord}_{25} 7 = 4 \neq |U_{25}| = 20.$$

Tällöin vaiheen 2 mukaan täytyy olla, että $g + p = 7 + 5 = 12$ on primitiivinen juuri. Tarkistetaan vielä tämä. Kertaluvun $\phi(25) = |U_{25}| = 20$ jakavat alkuluvut ovat 2 ja 5, joten

$$12^{20/2} = 12^{10} \equiv 24 \not\equiv 1 \pmod{25} \text{ ja}$$
$$12^{20/5} = 12^4 \equiv 11 \not\equiv 1 \pmod{25}.$$

Siispä 12 tosiaan on primitiivinen juuri mod 25.

Esimerkki 3.6. Luvulle $g = 10$, joka on primitiivinen juuri mod 487 pätee $\phi(487) = 486$, koska 487 on alkuluku lasku osoittaa, että

$$10^{486} \equiv 1 \pmod{487^2}.$$

Nyt kuitenkin $\phi(487^2) \neq 486$, joten 10 ei ole primitiivinen juuri, mutta Lauseen 3.3 todistuksen nojalla $10 + 487 = 497$ on primitiivinen juuri mod 487^2.

Muita tapauksia syklisistä yksiköiden ryhmistä on ryhmä $U_4 = U_{2^2}$. Ryhmä U_{2^e} on kuitenkin syklinen ainoastaan, jos $e = 1$ tai $e = 2$. Jos $e \geq 3$, niin $U_{2^e} = \{\pm 5^i : 0 \leq i < 2^{e-2}\}$ [4, Theorem 6.10].

Esimerkki 3.7. Ryhmä $U_2 = \{1\}$, joten se on selvästi syklinen. Edelleen ryhmä $U_4 = \{1, 3\}$, jolle

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

U_4 on siis syklinen. Ryhmä $U_8 = \{1, 3, 5, 7\}$, jolle

$$3^1 = 3 \pmod 8,\ 3^2 = 9 \equiv 1 \pmod 8.$$

Lisäksi

$$5^1 = 5 \pmod 8,\ 5^2 = 25 \equiv 1 \pmod 8 \text{ ja}$$
$$7^1 = 7 \pmod 8,\ 7^2 = 49 \equiv 1 \pmod 8.$$

U_8 ei siis ole syklinen.

Lause 3.8. *Jos $e \geq 3$, niin U_{2^e} on isomorfinen ryhmän $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{e-2}\mathbb{Z})$ kanssa [4, Theorem 6.10, Comment].*

Esimerkki 3.9. Ryhmä $U_{16} = \{1, 3, 5, 7, 9, 11, 13, 15\}$, jolle

$$\begin{aligned}
5^1 = 5 \pmod{16},\ 5^2 = 25 \equiv 9 \pmod{16},\\
5^3 = 125 \equiv 13 \pmod{16},\ 5^4 = 625 \equiv 1 \pmod{16},\\
-5^1 = -5 \equiv 11 \pmod{16},\ -5^2 = -25 \equiv 7 \pmod{16},\\
-5^3 = -125 \equiv 3 \pmod{16},\ -5^4 = -625 \equiv 15 \pmod{16}.
\end{aligned}$$

Lause 3.10. *Yksiköiden ryhmä U_n on syklinen, jos ja vain jos $n = 1, 2, 4, p^e$ tai $2p^e$, missä p on pariton alkuluku.*

Todistus. Katso [4, Theorem 6.11]. □

Jos $n = p$ on alkuluku, niin $\phi(p) = p-1$, joten tämä erikoistapaus on todistettu Lauseessa 3.2. Primitiivisten juurien määrä saadaan seuraavasta lauseesta.

Lause 3.11. *Jos positiivisella kokonaisluvulla n on primitiivinen juuri, niin sillä on yhteensä $\phi(\phi(n))$ ei-kongruenttia primitiivistä juurta [5, Theorem 9.5].*

Tämä johtuu yleisestä tuloksesta, jonka mukaan syklisellä ryhmällä on $\phi(n)$ virittäjää [2, Proposition 6(2), Chapter 2.3].

Todistus. Syklinen ryhmä, jossa on n alkiota, on isomorfinen jäännösluokkien ryhmän $\mathbb{Z}_n$ kanssa. Jos $\text{syt}(a, n) = 1$, niin yhtälöllä $ka \equiv b \pmod{n}$, missä $k \in \mathbb{Z}$, on ratkaisu kaikilla $b \in \mathbb{Z}$, joten a on ryhmän $\mathbb{Z}_n$ virittäjä. Jos taas $\text{syt}(a, n) \neq 1$, niin yhtälöllä $ka \equiv 1 \pmod{n}$ ei ole ratkaisua ja a ei ole ryhmän $\mathbb{Z}_n$ virittäjä. Siispä virittäjiä on oltava tasan kertaluvun $\phi(n)$ verran. □

Esimerkki 3.12. Olkoon $n = 7$. Luku 3 on primitiivinen juuri mod 7, sillä

$$3^1 = 3 \pmod{7},\ 3^2 = 9 \equiv 2 \pmod{7},\ 3^3 = 27 \equiv 6 \pmod{7},$$
$$3^4 = 81 \equiv 4 \pmod{7},\ 3^5 = 243 \equiv 5 \pmod{7} \text{ ja } 3^6 = 729 \equiv 1 \pmod{7}.$$

Nyt $\phi(7) = 7 - 1 = 6$, koska 7 on alkuluku ja lauseen 3.10 mukaan ryhmälle U_7 on $\phi(\phi(7)) = \phi(6)$ virittäjää. Koska $U_6 = \{1, 5\}$, niin $\phi(6) = |U_6| = 2$. Luvulla 7 on siis 2 ei-kongruenttia primitiivistä juurta. Tiedämme, että 3 on toinen niistä. Etsitään vielä toinen:

$\phi(7) = 6$ ja sen jakaa alkuluvut $q = 2, 3$. Tällöin $2^{6/2} = 2^3 = 8 \equiv 1 \pmod{7}$, joten 2 ei ole primitiivinen juuri. Myös $4^3 = 64 \equiv 1 \pmod{7}$, joten 4 ei ole primitiivinen juuri. Kuitenkin

$$5^3 = 125 \equiv 6 \not\equiv 1 \pmod{7},\ 5^{6/3} = 5^2 = 25 \equiv 4 \not\equiv 1 \pmod{7},$$

joten 5 on primitiivinen juuri. Voidaan vielä tarkistaa, että $6^3 = 216 \equiv 6 \pmod{7}$ ja $6^2 = 36 \equiv 1 \pmod{7}$, joten 6 ei ole primitiivinen juuri. Löydettiin siis $\phi(\phi(7)) = \phi(6) = 2$ ei-kongruenttia primitiivistä juurta.

4 Sovellukset

Primitiivisistä juurista on paljon hyötyä erilaisissa matematiikan sovelluksissa. Tässä työssä tutustutaan sovelluksiin rationaaliluvun desimaaliesityksen jakson, näennäissatunnaislukujen ja indeksiaritmetiikan osalta.

4.1 Rationaaliluvun desimaaliesityksen jakso

Primitiivisiä juuria voidaan käyttää selvittämään mahdollisimman pitkä jakso desimaalikehitelmässä. Desimaaliluvut perustuvat kymmenjärjestelmään, joten kun tutkitaan lukua 10 primitiivisille juurille $\bmod p$ voidaan löytää luvun pisin $1/p$ desimaaliesitys.

Näytetään ensin, että murtoluku $1/n$ voidaan esittää päättyvänä ainoastaan, jos sen nimittäjä on jaollinen alkuluvuilla 2 ja 5 [1].

Lause 4.1. *Desimaaliesitys murtoluvulle* $1/n$ *on päättyvä, jos ja vain jos* $n = 2^a 5^b$ *joillakin* $a, b \in \mathbb{N}$.

Todistus. ($\Leftarrow$) Jos $1/n = 1/(2^a 5^b)$, niin laventamalla sitä joko luvulla 5^{a-b}, missä $a > b$ tai 2^{b-a}, missä $b > a$ saadaan

$$\frac{1}{n} = \frac{1}{2^a 5^b} = \frac{5^{a-b}}{2^a 5^b \cdot 5^{a-b}} = \frac{5^{a-b}}{2^a \cdot 5^{b+a-b}} = \frac{5^{a-b}}{2^a \cdot 5^a} = \frac{5^{a-b}}{(2 \cdot 5)^a} = \frac{5^{a-b}}{10^a}$$

tai

$$\frac{1}{n} = \frac{1}{2^a 5^b} = \frac{2^{b-a}}{2^a 5^b \cdot 2^{b-a}} = \frac{2^{b-a}}{5^b \cdot 2^{a+b-a}} = \frac{2^{b-a}}{5^b \cdot 2^b} = \frac{2^{b-a}}{(5 \cdot 2)^b} = \frac{2^{b-a}}{10^b}.$$

Näillä murtoluvuilla on selvästi päättyvä desimaaliesitys oli sitten a tai b suurempi.

($\Rightarrow$) Jos desimaaliesitys on päättyvä, niin

$$\begin{aligned}\frac{1}{n} &=, d_1 d_2 \dots d_k \\ &= \frac{d_1}{10} + \frac{d_2}{10^2} + \cdots + \frac{d_k}{10^k} \\ &= \frac{10^k 10^{-1} d_1}{10^k} + \frac{10^k 10^{-2} d_2}{10^k} + \cdots + \frac{d_k}{10^k} \\ &= \frac{10^{k-1} d_1 + 10^{k-2} d_2 + \cdots + d_k}{10^k} \\ &= \frac{m}{10^k},\end{aligned}$$

missä $m = 10^{k-1} d_1 + 10^{k-2} d_2 + \cdots + d_k$.

Tästä saadaan, että $mn = 10^k$, joten $n \mid 10^k$. Tällöin ainoat luvut, jotka jakavat luvun n ovat 2 ja 5. Siispä n on muotoa $2^a 5^b$. □

Jos luvun $1/n$ desimaaliesitys on päättymätön, niin se on jaksollinen ja sen jakson pituus on kertaluku luvulle 10 modulo n.

Käydään seuraavaksi läpi lause ja sen todistus jakson pituuden maksimille.

Lause 4.2. *Luvun $1/n$ desimaaliesityksen jakson pituus on korkeintaan $n-1$.*

Todistus. Oletetaan, että luvun $1/n$ desimaalikehitelmä ei ole päättyvä. Olkoon nyt t kokonaisluku siten, että $10^t < n < 10^{t+1}$. Käyttämällä nyt jakoalgoritmiä toistuvasti saadaan

$$\begin{aligned}10^{t+1} &= d_1 n + r_1,\ 0 < r_1 < n, \\ 10 r_1 &= d_2 n + r_2,\ 0 \le r_2 < n, \\ 10 r_2 &= d_3 n + r_3,\ 0 \le r_2 < n,\end{aligned}$$

$$\dots$$

$$10 r_k = d_{k+1} n + r_{k+1},\ 0 \le r_{k+1} < n,$$

$$\dots$$

Huomautuksena jokainen d_k on pienempää kuin 10, koska kaikille $k = 2, 3, \ldots,$

$$d_k n = 10r_{k-1} - r_k \leq 10r_{k-1} < 10n,$$

ja

$$d_1 n = 10^{t+1} - r_1 < 10^{t+1} = 10 \cdot 10^t < 10n.$$

Muokkaamalla aiempaa yleistä jakoalgoritmiä jakamalla se luvulla $10n$ saadaan

$$r_k/n = d_{k+1}/10 + r_{k+1}/10n.$$

Jos jaetaan molemmat puolet nyt jakoalgoritmin yhtälö luvulla $10^{t+1}n$ ja jatketaan sitä toistuvasti hyödyntäen yllä olevaa tietoa, niin saadaan

$$\begin{aligned} 1/n &= d_1/10^{t+1} + r_1/n10^{t+1} \\ &= d_1/10^{t+1} + d_2/10^{t+2} + r_2/n10^{t+2} \\ &= d_1/10^{t+1} + d_2/10^{t+2} + d_3/10^{t+3} + r_3/n10^{t+3} \\ &\ldots \\ &= d_1/10^{t+1} + d_2/10^{t+2} + d_3/10^{t+3} + d_4/n10^{t+4} + \ldots, \end{aligned}$$

missä $d_1, d_2, d_3, \ldots$ ovat luvun $1/n$ desimaaliesityksen numeroita. Jokainen jakojäännös $r_1, r_2, \ldots$ on jokin luvuista $1, 2, \ldots, n-1$. Näin ollen n kappaleen jakojäännösten $r_1, r_2, \ldots, r_n$ joukossa on kyyhkyslakkaperiaatteen nojalla kaksi samaa jakojäännöstä. Jos $r_i = r_j$, niin jakoalgoritmistä seuraa, että $d_{k+1} = d_{j+1}$, $d_{k+2} = d_{j+2}$, $\ldots$ ovat desimaaliesityksen numeroita, jotka toistuvat jakson pituudella, joka on aina pienempää kuin n.

□

Esimerkki 4.3. Olkoon $n = 17$, niin jakoalgoritmillä saadaan

$$\begin{aligned}
10 &= 0 \cdot 17 + 10 \\
100 &= 5 \cdot 17 + 15, \\
150 &= 8 \cdot 17 + 14, \\
140 &= 8 \cdot 17 + 4, \\
40 &= 2 \cdot 17 + 6, \\
60 &= 3 \cdot 17 + 9, \\
90 &= 5 \cdot 17 + 5, \\
50 &= 2 \cdot 17 + 16, \\
160 &= 9 \cdot 17 + 7, \\
70 &= 4 \cdot 17 + 2, \\
20 &= 1 \cdot 17 + 3, \\
30 &= 1 \cdot 17 + 13, \\
130 &= 7 \cdot 17 + 11, \\
110 &= 6 \cdot 17 + 8, \\
80 &= 4 \cdot 17 + 12, \\
120 &= 7 \cdot 17 + 1, \\
10 &= 0 \cdot 17 + 10, \\
&\ldots
\end{aligned}$$

Jakoalgoritmista siis nähdään, että desimaaliesitys $1/17 =, \overline{0588235294117647}$, missä jakson pituus on $16 = 17 - 1$.

Lause 4.4. *Jos* $\text{syt}(n, 10) = 1$*, niin rationaaliluvun* $1/n$ *desimaaliesitys on jaksollinen ja jakson pituus on pienin positiivinen kokonaisluku* r*, jolle*

$$10^r \equiv 1 \pmod{n}.$$

Todistus. Jos $\text{syt}(n, 10) = 1$, niin määritelmän 1.11 nojalla 10 on yksikkö modulo n. Tällöin on olemassa pienin positiivinen kokonaisluku r, jolle $10^r \equiv 1 \pmod{n}$. Nyt siis $kn = 10^r - 1$, $k \in \mathbb{Z}$. Tästä saadaan $n = (10^r - 1)/k$ ja tällöin $1/n = k/(10^r - 1)$. Nähdään, että $k < 10^r$, joten se on kokonaisluku, jossa on korkeintaan r määrä numeroita. Olkoon k:n numerot järjestyksessä

$d_{r-1}, d_{r-2}, \ldots, d_0$. Tällöin

$$\begin{aligned}
\frac{1}{n} &= \frac{k}{10^r - 1} \\
&= \frac{d_{r-1}d_{r-2}\cdots d_0}{10^r - 1} \\
&= \frac{d_{r-1}d_{r-2}\cdots d_0}{10^r(1 - 10^{-r})} \\
&= \frac{d_{r-1}d_{r-2}\cdots d_0}{10^r} \cdot \frac{1}{1 - 10^{-r}} \\
&= (0, d_{r-1}d_{r-2}\ldots d_0)(1 + 10^{-r} + 10^{-2r} + \ldots) \\
&= 0, d_{r-1}d_{r-2}\ldots d_0 d_{r-1}d_{r-2}\ldots d_0 \ldots. \\
&=, \overline{d_{r-1}d_{r-2}\ldots d_0}.
\end{aligned}$$

Saadaan siis toistuva desimaaliesitys $, \overline{d_{r-1}d_{r-2}\ldots d_0}$ jakson pituudella r ja numeroilla $d_{s-1}, d_{r-2}, \ldots, d_0$. Nähdään myös, että lausekkeen osa $1 + 10^{-r} + 10^{-2r} + \ldots$ antaa päättymättömälle jaksolliselle desimaaliesitykselle $r - 1$ kappaletta nollaa peräkkäin ja ykkösen.

Näytetään vielä, että r on tosiaan pienin mahdollinen jakson pituus. Oletetaan, että desimaaliesityksellä $1/n$ on jakson pituus $s < r$. Näytetään, että $10^s \equiv 1 \bmod n$, jolloin saadaan ristiriita oletukselle ja alkuperäinen väite pätee. Lauseen 4.2 todistuksen jakoalgoritmin nojalla kaikille k pätee

$$10r_k \equiv r_{k+1} \pmod{n}.$$

Tällöin

$$10^2 r_k \equiv 10r_{k+1} \equiv r_{k+2} \pmod{n},$$

ja yleisesti

$$10^t r_k \equiv r_{k+t} \pmod{n},$$

kaikilla positiivisilla kokonaisluvuilla t. Jos $1/n$ on jaksollinen jakson pituudella s, niin $d_{k+s} = d_k$ kaikilla selvästi suuremmilla kokonaisluvuilla k. Tällöin myös $r_{k+s} = r_k$. Nyt siis

$$10^s r_k \equiv r_{k+s} \equiv r_k \pmod{n}. \tag{4.1}$$

Nyt pitää vielä näyttää, että $\text{syt}(r_k, n) = 1$, jolloin r_k voidaan supistaa yhtälöstä (4.1) ja seuraa $10^s \equiv 1 \pmod{n}$ ja väite on todistettu. Koska

$$10r_{k-1} = d_k n + r_k,$$

niin seuraa, että jos $p \mid r_k$ ja $p \mid n$, niin $p \mid 10r_{k-1}$, missä p on alkuluku. Koska $\text{syt}(10, n) = 1$, niin $p \mid r_{k-1}$. Kuitenkin myös

$$10^t = d_1 n + r_1,$$

josta saadaan, että $p \mid 10$, mikä ei ole mahdollista. Siispä $\text{syt}(r_k, n) = 1$ ja r on pienin positiivinen jakson pituus, jolle $10^s \equiv 1 \pmod{n}$.

□

Esimerkki 4.5. Luvulle $n = 7$ pätee, että $\text{syt}(7, 10) = 1$. Etsitään pienin r, jolle $10^r \equiv 1 \pmod{7}$. Nähdään, että

$$10^1 \equiv 3 \pmod{7},\ 10^2 = 100 \equiv 2 \pmod{7},$$
$$10^3 = 1000 \equiv 6 \pmod{7},\ 10^4 = 10\,000 \equiv 4 \pmod{7},$$
$$10^5 = 100\,000 \equiv 5 \pmod{7} \text{ ja } 10^6 = 1\,000\,000 \equiv 1 \pmod{7}.$$

Siispä $r = 6$ ja siis $10^6 - 1 = 999\,999 = 7 \cdot 142\,857$, jonka vuoksi

$$\frac{1}{7} = \frac{142857}{999999} = .\overline{142857}.$$

Esimerkki 4.6. Luvulle $n = 3$ pätee, että $\text{syt}(3, 10) = 1$. Etsitään pienin r, jolle $10^r \equiv 1 \pmod{3}$. Nähdään, että $10^1 \equiv 1 \pmod{3}$. Siispä $r = 1$ ja siis $10^1 - 1 = 9 = 3 \cdot 3$, jonka vuoksi

$$\frac{1}{3} = \frac{3}{9} = 0,333\cdots = 0,\overline{3}.$$

Koska kokonaisluvun kertaluku mod n on $\phi(n)$:n jakaja, niin luvun $1/n$ jakson pituus on $\phi(n)$:n jakaja. Esimerkiksi luvulle 5 jakson pituus on päättyvä, mutta luvulle 13 ei ole: $\phi(13) = 12$ ja $1/13 = .\overline{076923}$. Ei ole siis yhtä yhteistä sääntöä ennustaa desimaaliesityksen pituutta. Kuitenkin primitiivisen juuren avulla voidaan tutkia jakson pituutta tietyillä ehdoilla.

Seuraus 4.7. *Jos* 10 *on primitiivinen juuri* mod n*, niin luvun* $1/n$ *desimaaliesityksen jakson pituus on* $\phi(n)$ *ja muutoin se on lyhyempi.*

Esimerkki 4.8. $|U_{17}| = 16$. Tällöin $10^{16/2} = 10^8 \equiv 16 \not\equiv 1 \pmod{17}$. Siispä 10 on primitiivinen juuri mod 17. Nyt siis desimaaliesityksen jakson pituus on $\phi(17) = 17 - 1 = 16$ eli

$$\frac{1}{17} = 0,\overline{0588235294117647} \text{ kuten Esimerkissä 4.3.}$$

Esimerkki 4.9. $|U_{13}| = 12$. Tällöin $10^{12/2} = 10^6 \equiv 1 \pmod{13}$. Siispä 10 ei ole primitiivinen juuri mod 13. Nyt siis desimaaliesityksen jakson pituus on lyhyempi, kuin $\phi(13) = 13 - 1 = 12$ eli

$$\frac{1}{13} = 0,\overline{076923}.$$

Esimerkki 4.10. Esimerkiksi *Mathematica*-ohjelmalla saadaan, että luku 10 on primitiivinen juuri mod n, kun

$$\begin{aligned} n = {} & 17,\ 19,\ 23,\ 29,\ 47,\ 59,\ 61,\ 97,\ 109,\ 113,\ 131,\ 149,\ 167,\ 179,\ 181, \\ & 193,\ 223,\ 229,\ 233,\ 257,\ 263,\ 269,\ 313,\ 337,\ 367,\ 379,\ 383,\ \ldots \end{aligned}$$

4.2 Näennäissatunnaisluvut

Salausavaimissa ja salausprotokollissa tarvitaan satunnaisten lukujen luomista. Yksi primitiivisten juurten sovellus on *näennäissatunnaisluvut*. Näennäissatunnaisluvut ovat jollain menetelmällä tuotettuja kokonaislukujonoja, joissa luvut vaikuttavat täysin satunnaisilta. Näin tuotetut luvut ovat kuitenkin riittävän satunnaisia moniin käyttötarkoituksiin.

Eräs satunnaislukuja tuottava menetelmä on puhtaasti multiplikatiivinen kongruenssimenetelmä. Siinä satunnaisluvut tuotetaan rekursiivisesti kongruenssiyhtälöllä

$$x_{n+1} \equiv ax_n \pmod{m},\ 0 < x_{n+1} < m.$$

Yleisesti tämä voidaan ilmaista *generaattorin* a ja alkuarvon x_0 avulla

$$x_n \equiv a^n x_0 \pmod{m},\ 0 < x_{n+1} < m.$$

Jos l on lukujonon jakson pituus, niin se on pienin positiivinen kokonaisluku, jolla

$$x_0 \equiv a^l x_0 \pmod{m}.$$

Jos $\text{syt}(x_0, m) = 1$, niin Lemman 1.3 nojalla

$$a^l \equiv 1 \pmod{m}.$$

Tästä kongruenssiyhtälöstä tiedetään, että pisin mahdollinen jakson pituus on minimaalinen universaali eksponentti $\lambda(m)$, joka on primitiivisille juurille sama kuin kertaluku $\phi(m)$. Universaalista eksponentsta löytyy enemmän tietoa lähteestä Rosen [5, Chapter 9.6].

Monissa sovelluksissa käytetään puhtaasti multiplikatiivisena generaattoria modulo m *Mersennen alkulukua* $M_{31} = 2^{31} - 1$. Kun m on alkuluku, niin jakson maksimipituus on $m - 1$ ja tätä käytetään, kun jokin kokonaisluku a on primitiivinen juuri modulo m. Halutaan siis löytää nyt jokin primitiivinen juuri modulo M_{31}. Yksi tälläinen luku on 7 [5].

Lause 4.11. *Kokonaisluku* 7 *on primitiivinen juuri* mod M_{31}.

Todistus. Lemman 2.3 mukaan 7 on primitiivinen juuri mod M_{31}, jos

$$7^{(M_{31}-1)/q} \not\equiv 1 \pmod{M_{31}}$$

kaikilla alkuluvuilla q, jotka jakavat luvun $M_{31} - 1$. Tällöin myös osoitetaan, että kertaluku $\operatorname{ord}_{M_{31}} 7 = M_{31} - 1$. Jaetaan nyt kertaluku $M_{31} - 1$ alkutekijöihin:

$$\begin{aligned} M_{31} - 1 &= 2^{31} - 1 - 1 \\ &= 2^{31} - 2 \\ &= 2(2^{30} - 1) \\ &= 2(2^{15} - 1)(2^{15} + 1) \\ &= 2(2^5 - 1)(2^{10} + 2^5 + 1)(2^5 + 1)(2^{10} - 2^5 + 1) \\ &= 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331. \end{aligned}$$

Nyt siis täytyy näyttää, että

$$7^{(M_{31}-1)/q} \not\equiv 1 \pmod{M_{31}},$$

kun $q = 2, 3, 7, 11, 31, 151, 331$. Lähteen [5, Theorem 10.3] mukaan

$$\begin{aligned} 7^{(M_{31}-1)/2} &\equiv 2\ 147\ 483\ 646 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/3} &\equiv 1\ 513\ 477\ 735 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/7} &\equiv 120\ 536\ 285 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/11} &\equiv 1\ 969\ 212\ 174 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/31} &\equiv 512 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/151} &\equiv 535\ 044\ 134 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/331} &\equiv 1\ 761\ 885\ 083 \not\equiv 1 \pmod{M_{31}}. \end{aligned}$$

Nähdään siis, että 7 on primitiivinen juuri mod M_{31}.

□

Todellisuudessa ei kuitenkaan voida käyttää primitiivistä juurta 7, sillä siitä kehitetyt ensimmäiset kokonaisluvut ovat liian pieniä. Hyödynnetään lausetta, joka kertoo meille suuremman primitiivisen juuren samalla kantaluvulla.

Lause 4.12. *Olkoon r on primitiivinen juuri* mod n*, missä $n > 1$. Tällöin r^u on primitiivinen juuri* mod n*, jos ja vain jos* $\text{syt}(u, \phi(n)) = 1$.

Tämä todistamiseen tarvitaan seuraavaa hyödyllistä lemmaa:

Lemma 4.13. *Jos* $\text{ord}_m\, a = t$ *ja u on positiivinen kokonaisluku, niin*

$$\text{ord}_m(a^u) = \tfrac{t}{\text{syt}(t,u)}$$

Katso todistus Theorem 9.4 [5].

Lauseen 4.12 todistus. Lemman 4.13 mukaan tiedämme, että

$$\text{ord}_m\, r^u = \frac{\text{ord}_m\, r}{\text{syt}(\text{ord}_m\, r, u)}$$

Nyt koska r on primitiivinen juuri, niin $\text{ord}_m\, r = \phi(m)$. Tällöin

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

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

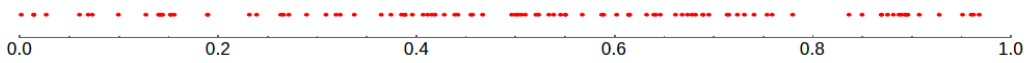
□

Nyt siis, kun etsitään jokin luku 7^k, missä $\text{syt}(k, M_{31} - 1) = 1$, saadaan suurempi primitiivinen juuri mod M_{31}.

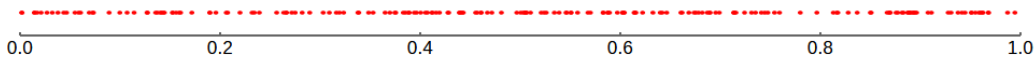
Esimerkki 4.14. Lauseen 4.11 nojalla 7 on primitiivinen juuri mod M_{31}. Koska syt$(5, M_{31} - 1) = 1$, niin Lauseen 4.12 nojalla $7^5 = 16\ 807$ on primitiivinen juuri mod M_{31}.

Tietokoneiden simulaatioihin tarvitaan kuitenkin vielä näistä satunnaisluvuista lukuja vain väliltä $[0, 1]$. Tälläisiä lukuja saadaan käyttämällä puhtaasti multiplikatiivista kongruenssigeneraattoria. Tuotetaan satunnaisluvut x_i, missä $i = 1, 2, 3, \ldots$ välillä $[0, m]$ ja jaetaan jokainen generaattorin antama luku luvulla m, jolloin saadaan lukujono x_i/m, joka on välillä $[0, 1]$.

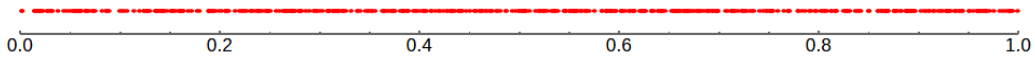
Esimerkki 4.15. Valitaan moduliksi 500. alkuluku $m = 3571$. Tällä on 768 primitiivistä juurta. Valitaan yksi näistä primitiivisistä juurista kertojaksi a ja valitaan jokin alkuarvo x_0. Tällöin saadaan generaattorin antamia lukuja, jotka edustavat luvun a^l kongruenssiluokkaa modulo m. Näiden avulla saadaan näennäislukuja välillä $[0, 1]$. Kuvista 4.1, 4.2 ja 4.3 nähdään, että mitä enemmän näennäislukuja tuotetaan, niin sitä paremmin se täyttää reaaliakselia välillä $[0, 1]$ ja on siten melko satunnainen.



Kuva 4.1: *Mathematica*-ohjelmalla saadut 100 näennäislukua.



Kuva 4.2: *Mathematica*-ohjelmalla saadut 200 näennäislukua.



Kuva 4.3: *Mathematica*-ohjelmalla saadut 500 näennäislukua.

4.3 Indeksiaritmetiikka

Primitiivisiä juuria voi käyttää myös apuna modulaariaritmetiikassa. Määritelmänsä nojalla tiedetään, että primitiivisen juuren potenssit muodostavat koko yksiköiden ryhmän

$$U_n = \{r^1, r^2, r^3, \ldots, r^{\phi(n)}\}.$$

Siis, jos kokonaisluvulle a pätee $\text{syt}(a, n) = 1$, niin on olemassa kokonaisluku x, jolle $1 \leq x \leq \phi(n)$ siten, että

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

Määritellään nyt tämmöiselle kokonaisluvulle x seuraavanlaiset ominaisuudet.

Määritelmä 4.16. Olkoon n positiivinen kokonaisluku, jolla on primitiivinen juuri r. Jos a on positiivinen kokonaisluku, jolle $\text{syt}(a, n) = 1$, niin kokonaisluku x, jolle $1 \leq x \leq \phi(n)$ ja $r^x \equiv a \pmod{n}$ on a:n *indeksi* kantaluvulla r modulo n.

Indeksiä merkitään jatkossa $x = \text{ind}_r\, a$ ja tällöin $r^{\text{ind}_r\, a} \equiv a \pmod{n}$.

Esimerkki 4.17. Olkoon $n = 5$. Esimerkissä 2.2 nähtiin, että 3 on primitiivinen juuri modulo 5, koska

$$3^1 = 3 \pmod{5},\ 3^2 = 9 \equiv 4 \pmod{5},$$
$$3^3 = 27 \equiv 2 \pmod{5} \text{ ja } 3^4 = 81 \equiv 1 \pmod{5}.$$

Siispä saadaan modulo 5:ssä indeksit

$$\text{ind}_3\, 1 = 4,\ \text{ind}_3\, 2 = 3,\ \text{ind}_3\, 3 = 1,\ \text{ind}_3\, 4 = 2.$$

Indeksi siis kertoo millä primitiivisen juuren r potenssilla saadaan kyseinen alkio a modulossa n.

Esimerkissä 3.5 löydettiin myös, että 7 on primitiivinen juuri modulo 5, koska

$$7^1 = 7 \equiv 2 \pmod 5,\ 7^2 = 49 \equiv 4 \pmod 5,$$
$$7^3 = 343 \equiv 3 \pmod 5 \text{ ja } 7^4 = 2401 \equiv 1 \pmod 5$$

Tällöin indeksit ovat

$$\operatorname{ind}_7 1 = 4,\ \operatorname{ind}_7 2 = 1,\ \operatorname{ind}_7 3 = 3,\ \operatorname{ind}_7 4 = 2.$$

Osoitetaan seuraavaksi näiden indeksien ominaisuuksia. Indeksi jakavat samoja ominaisuuksia kuin logaritmit erona vain se, että yhtäsuuruuksien tilalla on kongruenssit modulo $\phi(n)$. Siksi indeksejä kutsutaan myös nimellä *diskreetit logaritmit*. Seuraava lause antaa nämä ominaisuudet indekseille.

Lause 4.18. *Olkoon n positiivinen kokonaisluku primitiivisellä juurella r ja a, b kokonaislukuja, joille* $\operatorname{syt}(a, n) = 1$ *ja* $\operatorname{syt}(b, n) = 1$. *Tällöin*

(i) $\operatorname{ind}_r 1 \equiv 0 \pmod{\phi(n)}$

(ii) $\operatorname{ind}_r(ab) \equiv ind_r a + \operatorname{ind}_r b \pmod{\phi(n)}$

(iii) $\operatorname{ind}_r a^k \equiv k \cdot \operatorname{ind}_r a \pmod{\phi(n)}$, *jos k on positiivinen kokonaisluku.*

Todistus. *(i)*-kohta seuraa Eulerin lauseesta 1.24. Koska r on primitiivinen juuri pätee $\operatorname{syt}(r, n) = 1$ aina. Siispä $r^{\phi(n)} \equiv 1 \pmod n$. Nyt siis indeksi

$$\operatorname{ind}_r 1 \equiv \phi(n) \equiv 0 \pmod{\phi(n)}.$$

(ii)-kohdalle indeksin määritelmästä saadaan

$$r^{\operatorname{ind}_r(ab)} \equiv ab \pmod n \text{ ja}$$
$$r^{\operatorname{ind}_r a + \operatorname{ind}_r b} \equiv r^{\operatorname{ind}_r a} \cdot r^{\operatorname{ind}_r b} \equiv ab \pmod n$$

Nyt siis

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

Tästä saadaan Lauseen 1.25 nojalla

$$\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \pmod{\phi(n)},$$

sillä primitiiviselle juurelle $\operatorname{ord}_n r = \phi(n)$.

(iii)-kohdalle indeksin määritelmästä saadaan

$$\begin{aligned} &r^{\operatorname{ind}_r a^k} \equiv a^k \pmod{n} \text{ ja} \\ &r^{k \cdot \operatorname{ind}_r a} = (r^{\operatorname{ind}_r a})^k \equiv a^k \pmod{n}. \end{aligned}$$

Siispä Lauseen 1.25 nojalla

$$\operatorname{ind}_r a^k \equiv k \cdot \operatorname{ind}_r a \pmod{\phi(n)}.$$

□

Esimerkki 4.19. Esimerkin 3.12 mukaan 5 on primitiivinen juuri modulo 7 ja kertaluku $\phi(7) = 6$. Nyt siis $\operatorname{ind}_5 1 = 6 \equiv 0 \pmod{6}$.

Koska

$5^3 = 125 \equiv 6 \pmod{7}$, $5^4 = 625 \equiv 2 \pmod{7}$, $5^5 = 3125 \equiv 3 \pmod{7}$, niin $\operatorname{ind}_5 6 = 3$, $\operatorname{ind}_5 2 = 4$ ja $\operatorname{ind}_5 3 = 5$.

Siispä lauseen 4.18 kohdan *(ii)* mukaan

$$\operatorname{ind}_5 6 = \operatorname{ind}_5(2 \cdot 3) = \operatorname{ind}_5 2 + \operatorname{ind}_5 3 = 4 + 5 = 9 \equiv 3 \pmod{6}.$$

Lauseen 4.18 kohdan *(iii)* mukaan

$$\operatorname{ind}_5 2^5 = 5 \cdot \operatorname{ind}_5 2 = 5 \cdot 4 = 20 \equiv 2 \pmod 6.$$

Toisaalta, koska $5^2 = 25 \equiv 32 \equiv 4 \pmod 7$, niin

$$\operatorname{ind}_5 2^5 = \operatorname{ind}_5 32 = \operatorname{ind}_5 4 = 2.$$

Indeksit voivat olla myös hyödyllisiä kongruenssiyhtälöiden ratkaisemisessa. Otetaan tästä yksi esimerkki.

Esimerkki 4.20. Ratkaistaan kongruenssiyhtälö $4x^6 \equiv 9 \pmod{13}$ indeksien avulla. Esimerkiksi Lemman 2.3 nojalla luku 2 on primitiivinen juuri modulo 13, sillä $\phi(13) = 12$,

$$2^{12/2} = 2^6 = 64 \equiv 12 \not\equiv 1 \pmod{13} \text{ ja } 2^{12/3} = 2^4 = 16 \equiv 3 \not\equiv 1 \pmod{13}.$$

Taulukoidaan primitiivisen juuren 2 kaikki indeksit modulo 13 taulukossa 1.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_2 a$	12	1	4	2	9	5	11	3	8	10	7	6

Taulukko 1: Indeksit kantaluvulla 2 modulo 13.

Nyt siis indeksien avulla ratkaistaan kogruenssiyhtälöä modulo $\phi(13) = 12$, jolloin

$$\operatorname{ind}_2(4x^7) \equiv \operatorname{ind}_2 9 = 8 \pmod{12}.$$

Käyttämällä nyt lauseen 4.18 kohtia *(ii)* ja *(iii)* saadaan

$$\operatorname{ind}_2(4x^7) \equiv \operatorname{ind}_2 4 + \operatorname{ind}_2(x^7) \equiv \operatorname{ind}_2 4 + 7 \cdot \operatorname{ind}_2 x \equiv 2 + 7 \cdot \operatorname{ind}_2 x \pmod{12}.$$

Tällöin yhdistämällä nämä tiedot saadaan

$$2 + 7 \cdot \operatorname{ind}_2 x \equiv 8 \pmod{12},$$

joka on sama kuin

$$7 \cdot \operatorname{ind}_2 x \equiv 6 \pmod{12}.$$

Koska $7 \in U_{12}$, niin kun kerrotaan molemmat puolet luvulla 7 huomataan, että saadaan

$$7 \cdot 7 \cdot \operatorname{ind}_2 x \equiv 7 \cdot 6 \pmod{12}$$

joka on sama kuin

$$49 \cdot \operatorname{ind}_2 x \equiv 42 \pmod{12}$$

ja edelleen

$$\operatorname{ind}_2 x \equiv 6 \pmod{12}.$$

Indeksien määritelmästä saadaan lopulta, että

$$x \equiv 2^6 \equiv 12 \pmod{13},$$

joka on ainoa ratkaisu kongruenssiyhtälölle.

Käydään myös läpi esimerkki eksponenttiyhtälön ratkaisemisesta.

Esimerkki 4.21. Ratkaistaan kongruenssiyhtälö $11^x \equiv 3 \pmod{13}$ indeksien avulla. Tällöin

$$\operatorname{ind}_2(11^x) \equiv \operatorname{ind}_2 3 = 4 \pmod{12}.$$

Käyttämällä nyt lauseen 4.18 kohtaa *(iii)* saadaan

$$\operatorname{ind}_2(11^x) \equiv x \cdot \operatorname{ind}_2 11 \equiv 7x \pmod{12}.$$

Tällöin yhdistämällä nämä tiedot saadaan

$$7x \equiv 4 \pmod{12}.$$

Koska luvun 7 käänteisalkio on 7 modulo 12, niin

$$7 \cdot 7x \equiv x \equiv 7 \cdot 4 = 28 \equiv 4 \pmod{12}.$$

Siispä kaikki kongruenssiyhtälön $11^x \equiv 3 \pmod{13}$ ratkaisut saadaan, kun

$$x \equiv 4 \pmod{12}.$$

Indeksejä voidaan käyttää myös $x^k \equiv a \pmod{n}$ muotoisten kongruenssiyhtälöiden ratkaisujen tutkimiseen. Määritellään ensin milloin tälläisella kongruenssiyhtälöllä on ratkaisu.

Määritelmä 4.22. Olkoon n ja k positiivisia kokonaislukuja ja $\operatorname{syt}(a, n) = 1$. Tällöin a on k:s *potenssijäännös* modulo n, jos konguenssiyhtälöllä $x^k \equiv a \pmod{n}$ on ratkaisu.

Potenssijäännösten erikoistapauksia ovat neliönjäännökset, joilla on Lukuteoriassa monia hyödyllisiä käyttötarkoituksia. Jos n:llä on primitiivinen juuri saadaan tästä seuraava hyödyllinen lause.

Lause 4.23. *Olkoon n kokonaisluku, jolla on primitiivinen juuri. Jos k on positiivinen kokonaisluku ja a on kokonaisluku, jolle* $\operatorname{syt}(a, n) = 1$*, niin kogruenssiyhtälöllä $x^k \equiv a \pmod{n}$ on ratkaisu, jos ja vain jos*

$$a^{\phi(n)/d} \equiv 1 \pmod{n},$$

missä $d = \operatorname{syt}(k, \phi(n))$. Tällöin on olemassa täsmälleen d ei-kongruenttia ratkaisua modulo n.

Todistus. Olkoon r primitiivinen juuri modulo n. Tällöin kongruenssiyhtälölle pätee Lauseen 4.18 ja Määritelmän 4.16 nojalla

$$x^k \equiv a \pmod{n},$$

jos ja vain jos

$$k \cdot \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{\phi(n)}. \tag{4.2}$$

Lauseen 1.26 nojalla, jos $\operatorname{syt}(k, \phi(n)) \nmid \operatorname{ind}_r a$, niin lineaarisella kongruenssiyhtälöllä

$$ky \equiv \operatorname{ind}_r a \pmod{\phi(n)} \tag{4.3}$$

ei ole ratkaisua. Jos $\operatorname{syt}(k, \phi(n)) \mid \operatorname{ind}_r a$, niin on $d = \operatorname{syt}(k, \phi(n))$ ratkaisua yhtälölle (4.3) modulo $\phi(n)$ ja siten myös d ratkaisua x yhtälölle (4.2) modulo n. Nyt vielä $d \mid \operatorname{ind}_r a$, jos ja vain jos

$$(\phi(n)/d) \operatorname{ind}_r a \equiv 0 \pmod{\phi(n)},$$

joka on Lauseen 4.18 kohdan *(iii)* nojalla sama kuin

$$\operatorname{ind}_r a^{\phi(n)/d} \equiv 0 \pmod{\phi(n)}.$$

Tämä pätee Lauseen 4.18 kohdan (i) nojalla, jos ja vain jos

$$a^{\phi(n)/d} \equiv 1 \pmod{n}.$$

□

Esimerkki 4.24. Tutkitaan onko luku 5 yhdeksäs potenssijäännös modulo 13 eli onko kongruenssiyhtälöllä

$$x^9 \equiv 5 \pmod{13}$$

ratkaisua. Nyt siis

$$5^{12/\operatorname{syt}(9,12)} = 5^{12/3} = 5^4 = 625 \equiv 1 \pmod{13},$$

joten kongruenssiyhtälöllä $x^9 \equiv 5 \pmod{13}$ on kolme ratkaisua.

A Merkintöjä

$\mathbb{N}$	Luonnollisten lukujen joukko $\{0,\ 1,\ 2,\ 3, \dots\}$
$\mathbb{Z}$	Kokonaislukujen joukko $\{\dots, -3, -2, -1,\ 0,\ 1,\ 2,\ 3, \dots\}$
$[a]$	Jäännösluokka $[a]_n = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$
$\mathrm{syt}(a, b)$	Suurin yhteinen tekijä luvuille a ja b
$\mathrm{ord}_n\, a$	Kertaluku alkiolle a modulo n
$\mathrm{ind}_r\, a$	Luvun a indeksi kantaluvulla r
ϕ	Eulerin funktio
$m \mid n$	m jakaa luvun n
$m \nmid n$	m ei jaa lukua n
$\bigsqcup_{i \in I} A_i$	Joukkojen A_i, $i \in I$, erillinen yhdiste

Viitteet

[1] Dudley, Underwood: *A Guide to Elementary Number Theory. Mathematical Association of America. 2009*

[2] Dummit, David S. ja Foote, Richard M.: *Abstract Algebra. John Wiley & Sons, Inc. 2004*

[3] Hardy, G.H. ja Wright, E.M.: *An Introduction to the Theory of Numbers. Oxford University Press. 6th edition. 2008*

[4] Jones, Gareth A. ja Jones, J. Mary: *Elementary Number Theory. Springer London. 1998.*

[5] Rosen, Kenneth H.: *Elementary Number Theory and its applications. Addison-Wesley. 4th edition. 1999.*