TAMPEREEN YLIOPISTO
Pro gradu - tutkielma

Riku Jokinen

Katsaus lukuteoriaan ja kryptografiaan

Matematiikan, tilastotieteen ja filosofian laitos
Matematiikka
Syyskuu 2004

Sisältö

Johdanto

Tässä tutkielmassa perehdytään lukuteorian perusteisiin sekä lukuteorian tärkeimpään käytännön sovellutukseen, kryptografiaan. Tarkoituksena on antaa kattava yleiskuva lukuteorian alkeista ja soveltaa niitä käytäntöön. Lukijan esitiedoiksi oletetaan lukion laajan matematiikan oppimäärä. Lisäksi lukijan tulee ymmärtää matemaattista tekstiä ja tuntea matematiikan yleisimpiä merkintätapoja.

Luvussa 1, Valmistelevia tarkasteluja, käydään läpi joitakin peruskäsitteitä, kuten jaollisuus ja määritellään alkuluvut. Luvussa 2, Kongruensseista, esitellään jaollisuuden sovellus, kongruenssit ja sen johdannaisia, kuten kiinalainen jäännöslause ja Fermat'n pieni lause. Lisäksi määritellään valealkuluvut. Luvussa 3, Primitiiviset juuret, esitellään aluksi Eulerin φ-funktio ja siitä seuraava Eulerin lause. Tämän jälkeen määritellään kokonaisluvun kertaluku sekä sovelletaan Eulerin lausetta siihen. Lopuksi esitellään primitiiviset juuret. Luvussa 4, Neliönjäännökset, määritellään neliönjäännökset ja Legendren symboli sekä todistetaan Eulerin kriteeri. Lisäksi esitellään ja todistetaan Gaussin lemma ja neliönjäännösten resiprookkilaki. Luvussa 5, Kryptografia, sovelletaan luvuissa 1 - 4 esiteltyjä asioita erilaisiin salausjärjestelmiin. Erityisen mielenkiinnon kohteena ovat julkisen avaimen salausjärjestelmät, kuten Fermat'n pientä lausetta soveltava RSA-salausjärjestelmä sekä primitiivisiä juuria soveltava ElGamal-salausjärjestelmä.

Tämän tutkielman rakenne noudattelee pääosin Kenneth H. Rosen teosta *Elementary Number Theory and Its Applications*, joka on ollut myös tärkein lähdeteos. Tärkeinä lähteinä ovat olleet myös James J. Tattersallin kirja *Elemetary Number Theory in Nine Chapters* sekä Melvyn B. Nathansonin kirja *Elementary Methods in Number Theory*. Muita lähteitä on käytetty lähinnä yksittäisissä todistuksissa. On huomattava, että kirjallisuusluettelossa mainittu *Topics in Number Theory, lecture notes and handouts* on tohtori D. W. Sharpin Sheffieldin yliopistossa syksyllä 2000 luennoima lukuteorian kurssi. Kyseessä ovat siis luentomuistiinpanot ja luennoilla jaettu materiaali, joita on käytetty paikoin todistuksissa. Näin ollen viittauksissa niihin ei ole mainittu sivunumeroita, sillä niitä ei ole olemassa.

Mainittakoon vielä, että aina, kun todistuksen kohdalla ei ole mainintaa lähdeteoksesta, on kyseessä tekijän itse todistama lause. Tämä ei tarkoita

sitä, etteikö kyseisiä lauseita olisi todistettu missään lähdeteoksista. Kaikki esimerkit ovat tekijän itsensä ratkaisemia, vaikkakin moniin niistä on otettu mallia lähdeteosten vastaavanlaisista esimerkeistä.

1 Valmistelevia tarkasteluja

1.1 Jaollisuudesta

Määritelmä 1.1 *Olkoot a ja b kokonaislukuja. Tällöin sanotaan, että luku b on luvun a* jakaja *ja luku a on luvun b* kerrannainen*, jos on olemassa sellainen kokonaisluku q, että*

$$a = bq.$$

Jos luku b jakaa luvun a, voidaan kirjoittaa

$$b|a,$$

ja sanotaan, että luku a on jaollinen luvulla b. Vastaavasti, jos luku b ei jaa lukua a, kirjoitetaan

$$b \not| a.$$

Huomautus 1.1 Jaollisuus on transitiivinen relaatio, eli $(a|b \text{ ja } b|c) \Rightarrow (a|c)$.

Todistus. Ks. [5] s. 31

Hyvinjärjestysperiaate osoittaa, että jokainen epätyhjä alhaalta rajoitettu kokonaislukujoukko sisältää pienimmän alkion. Tähän perustuu seuraava lause.

Lause 1.1 *Olkoon a kokonaisluku ja olkoon b positiivinen kokonaisluku. Tällöin ovat olemassa sellaiset yksikäsitteiset kokonaisluvut q ja r, että*

$$a = bq + r$$

ja

$$0 \leq r \leq b - 1.$$

Todistus. Ks. [4] s. 4

Kokonaislukua q kutsutaan tällöin *osamääräksi* ja kokonaislukua r *jäännökseksi* jaettaessa lukua a luvulla b.

1.2 Suurin yhteinen tekijä

Määritelmä 1.2 *Olkoot a ja b kokonaislukuja. Lukujen a ja b* suurin yhteinen tekijä *on suurin kokonaisluku c, joka jakaa sekä luvun a että luvun b. Tällöin merkitään* $(a, b) = c$.

Suurimman yhteisen tekijän löytäminen on helppoa päässälaskulla, kun on kyse pienistä kokonaisluvuista. Suurempien lukujen tapauksiin on kehitetty erilaisia apumenetelmiä, joista tunnetuin on Eukleideen algoritmia (Ks. [2] s. 12).

Määritelmä 1.3 *Kokonaisluvut a ja b ovat* keskenään jaottomia*, jos*

$$(a, b) = 1.$$

Lause 1.2 (Eukleideen lemma) *Jos luku jakaa kahden luvun tulon ja se on keskenään jaoton näistä toisen kanssa, se jakaa jäljelle jääneen luvun.*

Todistus. Ks. [1] s. 12.

1.3 Alkuluvuista

Lukuteoria käsittelee kokonaislukuja. Erityisen mielenkiinnon kohteena ovat alkuluvut.

Määritelmä 1.4 *Olkoon p lukua 1 suurempi kokonaisluku. Jos p on jaollinen ainoastaan itsellään ja luvulla* 1*, sekä näiden vastaluvuilla, kutsutaan sitä tällöin* alkuluvuksi.

Pienimmät alkuluvut ovat siis 2, 3, 5, 7, 11, 13 ja 17. Koska kaikki parilliset luvut ovat jaollisia luvulla 2, on luku 2 ainoa parillinen alkuluku.

Lause 1.3 (Aritmetiikan peruslause) *Jokainen positiivinen kokonaisluku voidaan kirjoittaa yksikäsitteisesti alkulukujen tulona.*

Todistus. Ks. [4] s. 27.

Esimerkki 1.1 Selvästi $198 = 2 \cdot 3 \cdot 3 \cdot 11$.

Lause 1.4 (Eukleideen lause) *Alkulukuja on ääreton määrä.*

Todistus. Vrt. [4] s. 33. Olkoon $p_1, p_2, \ldots, p_n$ jokin äärellinen alkulukujen joukko. Tarkastellaan kokonaislukua

$$N = p_1 p_2 \cdots p_n + 1.$$

Koska $N > 1$, aritmetiikan peruslauseen mukaan N on jaollinen jollakin alkuluvulla p. Jos $p = p_i$ jollakin luvulla $i = 1, 2, \ldots, n$, niin p jakaa luvun $N - p_1 p_2 \cdots p_n = 1$. Tämä on mahdotonta, sillä p on alkulukuna suurempi kuin 1. Täten, $p \neq p_i$ aina, kun $i = 1, 2, \ldots, n$. Toisin sanoen, kaikille äärellisille alkulukujen joukoille on aina olemassa alkuluku, joka ei kuulu tähän joukkoon. Siis alkulukujen joukko on ääretön. □

2 Kongruensseista

2.1 Johdanto kongruensseihin

Määritelmä 2.1 *Olkoon m positiivinen kokonaisluku. Jos a ja b ovat sellaisia kokonaislukuja, että $m|(a-b)$, niin luvun a sanotaan olevan* kongruentti *luvun b kanssa modulo m. Tällöin kirjoitetaan*

$$a \equiv b \pmod{m}.$$

Esimerkki 2.1 Selvästi $2 \equiv -8 \pmod 5$, sillä $5|(2-(-8)) = 10$. Vastaavasti $7 \equiv 1 \pmod 3$ ja $99 \equiv 55 \pmod{11}$. Kaikki parilliset kokonaisluvut ovat kongruentteja luvun 0 suhteen modulo 2 ja kaikki parittomat kokonaisluvut ovat kongruentteja luvun 1 suhteen modulo 2.

Huomautus 2.1 Jos $m \not| (a-b)$, niin kirjoitetaan $a \not\equiv b \pmod m$, ja sanotaan, että a ja b ovat *inkongruentteja* modulo m.

Kongruenssien kanssa työskentely voi olla joskus helpompaa, jos ne voidaan kääntää tavallisiksi yhtälöiksi. Seuraava lause kertoo, kuinka se tehdään.

Lause 2.1 *Olkoot a ja b kokonaislukuja. Tällöin $a \equiv b \pmod m$, jos ja vain jos on olemassa sellainen kokonaisluku k, että $a = b + km$.*

Todistus. Vrt. [5] s. 129. Jos $a \equiv b \pmod m$, niin $m|(a-b)$. Jaollisuuden määritelmän mukaan on olemassa sellainen kokonaisluku k, että $km = a - b$. Siis $a = b + km$.

Käänteisesti, jos on olemassa sellainen kokonaisluku k, että $a = b + km$, niin $km = a - b$. Siis $m|(a-b)$. Tästä seuraa, että $a \equiv b \pmod{\text{m}}$. □

Esimerkki 2.2 Kongruenssi $20 \equiv -6 \pmod{13}$ kääntyy muotoon $20 = -6 + 2 \cdot 13$

Seuraava lause esittelee joitakin kongruenssin tärkeimpiä ominaisuuksia.

Lause 2.2 *Olkoot a, b, c, d, n ja m kokonaislukuja, olkoot k ja q positiivisia kokonaislukuja ja olkoon p alkuluku. Tällöin ovat voimassa seuraavat ominaisuudet:*

(i) $a \equiv a \pmod{m}$

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

(iii) $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

(iv) $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$ ja $ac \equiv bd \pmod{m}$

(v) $a \equiv b \pmod{m} \Rightarrow a^k \equiv b^k \pmod{m}$

(vi) $a \equiv b \pmod{m} \Rightarrow ca \equiv cb \pmod{m}$

(vii) $qa \equiv qb \pmod{qm} \Leftrightarrow a \equiv b \pmod{m}$

(viii) $ab \equiv 0 \pmod{p} \Rightarrow a \equiv 0 \pmod{p}$ tai $b \equiv 0 \pmod{p}$

(ix) $a \equiv b \pmod{m}$ ja $a \equiv b \pmod{n} \Rightarrow a \equiv b \pmod{mn}$ aina, kun $(m, n) = 1$

(x) $ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m/d}$ aina, kun $d = (c, m)$.

Todistus. Ominaisuudet (i) ja (ii) seuraavat suoraan määritelmästä.

(iii) Vrt. [4] s. 45. Jos $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$, niin ovat olemassa sellaiset kokonaisluvut x ja y, että $a - b = mx$ ja $b - c = my$. Koska

$$a - c = (a - b) + (b - c) = mx + my = m(x + y),$$

niin $a \equiv c \pmod{m}$.

(iv) Jos $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$, niin $a = b + km$ ja $c = d + lm$, kun $k, l \in \mathbf{Z}$. Nyt

$$a + c = b + km + d + lm = b + d + m(k + l)$$

ja

$$ac = (b + km)(d + lm) = b + d + m(bl + kd + klm).$$

Siis $a + c \equiv b + d \pmod{m}$ ja $ac \equiv bd \pmod{m}$.

(v) Vrt. [5] s. 133. Jos $a \equiv b \pmod{m}$, niin $m|(a-b)$. Koska

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

niin $(a-b)|(a^k - b^k)$. Nyt, ominaisuuden (iii) mukaan, $m|(a^k - b^k)$. Näin ollen $a^k \equiv b^k \pmod{m}$.

(vi) Vrt. [5] s. 130. Selvästi $ac - bc = c(a-b)$. Koska $m|(a-b)$, niin $m|c(a-b)$ ja edelleen $ac \equiv bc \pmod{m}$.

(vii) Jos $a \equiv b \pmod{m}$, niin $m|(a-b)$. Siis $qm|q(a-b)$ ja edelleen $qm|(qa-qb)$. Siis $qa \equiv qb \pmod{qm}$. Todistus toiseen suuntaan menee vastaavasti.

(viii) Lähde [7]. Koska $ab \equiv 0 \pmod{p}$, niin $p|ab$. Siis $p|a$ tai $p|b$. Näin ollen $a \equiv 0 \pmod{p}$ tai $b \equiv 0 \pmod{p}$.

(ix) Lähde [7]. Koska $(m,n) = 1$, niin on olemassa sellaiset kokonaisluvut s ja t, että $sm+tn = 1$. Siis $sm(a-b)+tn(a-b) = (a-b)$. Koska $a \equiv b \pmod{m}$ ja $a \equiv b \pmod{n}$, niin $m|(a-b)$ ja $n|(a-b)$. Siis $mn|(sm(a-b)+tn(a-b))$. Siis $a \equiv b \pmod{mn}$.

(x) Vrt. [5] s. 131. Koska $ac \equiv bc \pmod{m}$, niin $m|(ac-bc) = c(a-b)$. Siis on olemassa sellainen kokonaisluku k, että $c(a-b) = km$. Kun nyt jaetaan puolittain luvulla d, saadaan $(c/d)(a-b) = k(m/d)$. Koska $(m/d, c/d) = 1$, niin $(m/d)|(a-b)$. Siis $a \equiv b \pmod{m/d}$. □

Huomautus 2.2 Edellisen lauseen kohtien (i), (ii) ja (iii) mukaan kongruenssi on refleksiivinen, symmetrinen ja transitiivinen. Toisin sanoen kongruenssi on ekvivalenssirelaatio.

Esimerkki 2.3 Koska $11 \equiv 7 \pmod{4}$, niin lauseen 2.2 ominaisuuden (v) mukaan

$$121 = 11^2 \equiv 7^2 = 49 \pmod{4},$$

ominaisuuden (vi) mukaan

$$33 = 3 \cdot 11 \equiv 3 \cdot 7 = 21 \pmod{4}$$

ja ominaisuuden (vii) mukaan

$$44 = 4 \cdot 11 \equiv 4 \cdot 7 = 28 \pmod{16}.$$

2.2 Lineaarikongruensseista

Muotoa

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

olevaa kongruenssia kutsutaan *yhden muuttujan lineaarikongruenssiksi*. Toisin sanoen lineaarikongruenssit ovat ensimmäisen asteen kongruenssiyhtälöitä. Seuraavassa esimerkissä näitä hahmotetaan käytännön tasolla.

Esimerkki 2.4 Ratkaistaan kongruenssi $97x \equiv 129 \pmod{44}$. Määritelmään perustuen voidaan luvuista 97 ja 129 poistaa modulon kerrannaisia. Siis

$$(97 - 2 \cdot 44)x \equiv (129 - 2 \cdot 44) \pmod{44},$$

josta saadaan

$$9x \equiv 41 \pmod{44}.$$

Lauseen 2.2 ominaisuuden (vi) mukaan, luvut $9x$ ja 41 voidaan kertoa luvulla 5, jolloin saadaan

$$45x = 5 \cdot 9x \equiv 5 \cdot 41 = 205 \pmod{44}.$$

Kun supistetaan jälleen modulon kerrannaisia, saadaan

$$x \equiv 29 \pmod{44},$$

joka on lineaarikongruenssin $97x \equiv 129 \pmod{44}$ ratkaisu.

Kaikilla lineaarikongruensseilla ei ole ratkaisua. Esimerkiksi kongruenssiyhtä löllä $98x \equiv 129 \pmod{44}$ ei ole ratkaisua, sillä edellisen esimerkin tapaan ratkaistaessa päädytään tulokseen $0 \equiv 22 \pmod{44}$, joka on selvästi mahdotonta. Seuraava lause kertoo, millaisilla lineaarikongruensseilla on ratkaisu.

Lause 2.3 *Olkoot a ja b kokonaislukuja, olkoon m positiivinen kokonaisluku ja olkoon $d = (a, m)$. Kongruenssilla*

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

on ratkaisu, jos ja vain jos

$$b \equiv 0 \pmod{d}.$$

Toisin sanoen kongruenssilla on ratkaisu, jos ja vain jos

$$(a, m) | b.$$

Todistus. Lähde [7]. Oletetaan, että kongruenssilla on ratkaisu x. Tällöin on olemassa sellainen kokonaisluku k, että $ax - b = km$. Nyt $(a, m)|a$ ja $(a, m)|m$, joten $(a, m)|(ax - km)$. Siis $(a, m)|b$.

Käänteisesti, oletetaan, että $(a, m)|b$. Siis on olemassa sellainen kokonaisluku r, että $b = r(a, m)$. Nyt on olemassa sellaiset kokonaisluvut s ja t, että $(a, m) = sa + tm$, joten $b = r(sa + tm)$. Näin ollen $a(rs) \equiv b \pmod{m}$ ja $x = rs$ on kongruenssin ratkaisu. □

Esimerkki 2.5 Tarkastellaan kongruenssia $24x \equiv 57 \pmod{15}$. Nyt $(24, 15) = 3$, joka jakaa luvun 57. Siis kongruenssilla $24x \equiv 57 \pmod{15}$ on ratkaisu.

Huomautus 2.3 Jos luvut a ja m ovat keskenään jaottomia, niin kongruenssilla on aina ratkaisu, sillä jokainen luku on jaollinen luvulla 1.

Määritelmä 2.2 *Olkoot a ja m keskenään jaottomia kokonaislukuja. Konruenssiyhtälön*

$$ax \equiv 1 \pmod{m}$$

ratkaisua kutsutaan luvun a käänteisluvuksi mod m. *Tällöin merkitään joko $x = \overline{a}$ tai $x = a^{-1}$.*

Esimerkki 2.6 Selvästi $(5, 29) = 1$. Kongruenssin

$$5x \equiv 1 \pmod{29}$$

ratkaisu on

$$x \equiv 6 \pmod{29},$$

joten kaikki luvun 6 kanssa kongruentit kokonaisluvut modulo 29 ovat luvun 5 käänteislukuja modulo 29. Koska

$$5 \cdot 6 \equiv 1 \pmod{29},$$

niin myös kaikki luvun 5 kanssa kongruentit kokonaisluvut modulo 29 ovat luvun 6 käänteislukuja modulo 29.

2.3 Kongruenssiryhmistä

Lineaarikongruensseja, aivan kuten tavallisiakin yhtälöitä, voidaan käsitellä myös ryhmissä. Tunnetuin esimerkki kongruenssiryhmistä on vanha kiinalainen ongelma, jossa etsitään lukua, joka saa jäännöksen 1, kun jaetaan luvulla 3, jäännöksen 2, kun jaetaan luvulla 5 ja jäännöksen 3, kun jaetaan luvulla 7. Tästä saadaan lineaarikongruenssiryhmä $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$ ja $x \equiv 3 \pmod 7$. Tämä johtaa kiinalaisena jäännöslauseena tunnettuun yleistykseen. Sitä ennen esitellään kuitenkin apulause, jota kaytetään kiinalaisen jäännöslauseen todistamiseen.

Apulause 2.1 *Olkoot m ja n positiivisia kokonaislukuja. Kaikille kokonaisluvuille a ja b, on olemassa sellainen kokonaisluku x, että*

$$x \equiv a \pmod m$$

ja

$$x \equiv b \pmod n,$$

jos ja vain jos

$$a \equiv b \pmod{(m,n)}.$$

Jos x on tämän kongruenssiyhtälöryhmän ratkaisu, niin kokonaisluku y on myös ratkaisu, jos ja vain jos

$$x \equiv y \pmod{mn}.$$

Todistus. Ks. [4] s. 61.

Lause 2.4 (Kiinalainen jäännöslause) *Olkoon $k \geq 2$. Jos $a_1, a_2, \ldots, a_k$ ovat kokonaislukuja ja $m_1, m_2, \ldots, m_k$ ovat keskenään jaottomia kokonaislukuja, niin silloin on olemassa sellainen kokonaisluku x, että*

$$x \equiv a_i \pmod{m_i}$$

aina, kun $i = 1, 2, \ldots, k$. Jos luku x on tämän kongruenssiyhtälöryhmän ratkaisu, niin kokonaisluku y on myös ratkaisu, jos ja vain jos

$$x \equiv y \pmod{m_1 m_2 \cdots m_k}.$$

Todistus. Vrt. [4] s. 63. Todistetaan induktiolla luvun k suhteen. Tapaus $k = 2$ on apulauseen 2.1 erikoistapaus.

Olkoon $k \geq 3$. Oletetaan, että lause on tosi, kun ryhmässä on $k-1$ kongruenssia. Nyt on olemassa sellainen kokonaisluku z, että $z \equiv a_i \pmod{m_i}$, jossa $i = 1, 2, \ldots, k-1$. Koska kaikille lukupareille $(m_i, m_j) = 1$, jossa $j = 1, 2, \ldots, k-1$, niin $(m_1 m_2 \cdots m_{k-1}, m_k) = 1$. Tapauksen $k = 2$ mukaan on olemassa sellainen kokonaisluku x, että $x \equiv z \pmod{m_1 m_2 \cdots m_{k-1}}$ ja $x \equiv a_k \pmod{m_k}$. Siis

$$x \equiv z \equiv a_i \pmod{m_i},$$

kun $i = 1, 2, \ldots, k-1$.

Jos y on jokin toinen ratkaisu kongruenssiyhtälöjoukolle, jossa on k kongruenssiyhtälöä, niin $x - y$ on jaollinen luvulla m_i, kun $i = 1, 2, \ldots, k$. Koska $m_1, m_2, \ldots, m_k$ ovat pareittain keskenään jaottomia alkulukuja, on luku $x-y$ jaollinen luvulla $m_1 m_2 \cdots m_k$. □

Etsitään nyt ratkaisu edellä esitettyyn ongelmaan.

Esimerkki 2.7 Ratkaistaan kongruenssiryhmä

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

Koska modulot ovat keskenään jaottomia, on kongruenssiryhmällä kiinalaisen jäännöslauseen mukaan ratkaisu. Ensimmäisen kongruenssin perusteella tiedetään, että $x = 3k + 1$, jossa $k \in \mathbf{Z}$. Sijoittamalla tämä toiseen kongruenssiin saadaan $k \equiv 2 \pmod{5}$. Merkitään tätä $k = 5l + 2$, jossa $l \in \mathbf{Z}$. Sijoittamalla tämä ensimmäiseen kongruenssiin saadaan kahden ensimmäisen kongruenssin ratkaisuksi $x = 15l + 7$. Toisin sanoen $x \equiv 7 \pmod{15}$. Sijoittamalla saatu tulos kolmanteen kongruenssiin saadaan vastaavalla tavalla kolmen kongruenssin ratkaisuksi $x \equiv 52 \pmod{105}$. Tämä on myös koko konruenssiryhmän ratkaisu.

Kongruenssiyhtälöt voivat olla myös korkeampaa astetta. Polynomikongruenssiyhtälöt ovat muotoa $f(x) \equiv 0 \pmod{m}$, jossa $f(x)$ on kokonaislukukertoiminen, asteeltaan yhtä suurempi polynomi. Jos modulo m voidaan jakaa

alkulukutekijöihin, niin kongruenssi $f(x) \equiv 0 \pmod{m}$ voidaan ratkaista ratkaisemalla kongruenssiryhmä

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

Kun kaikki k kongruenssia modulo $p_i^{a_i}$ on ratkaistu, voidaan kiinalaista jäännöslausetta käyttämällä ratkaista kongruenssi modulo m, kuten seuraavassa esimerkissä.

Esimerkki 2.8 Ratkaistaan kongruenssi

$$2x^2 + 3x - 2 \equiv 0 \pmod{20}.$$

Koska $20 = 2^2 \cdot 5$, voidaan kongruenssi jakaa kahteen osaan: ensimmäinen modulo 4 ja toinen modulo 5. Näin ollen saadaan

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

ja

$$2x^2 + 3x - 2 \equiv 0 \pmod{5}.$$

Ensimmäisessä kongruenssissa käydään läpi muuttujan x arvot luvusta 0 lukuun 3. Tällöin saadaan ratkaisuksi $x \equiv 2 \pmod{4}$. Vastaavasti jälkimmäisessä kongruenssissa käydään läpi arvot luvusta 0 lukuun 4, jolloin ratkaisuksi saadaan $x \equiv 3 \pmod{5}$. Nyt kiinalaista jäännöslausetta käyttämällä saadaan kongruenssiparin ratkaisuksi

$$x \equiv 18 \pmod{20},$$

joka on myös polynomikongruenssin ratkaisu.

2.4 Fermat'n pieni lause

Lukuteorian tärkeimpiä lauseita niin teorian kuin käytännönkin kannalta on Fermat'n pieni lause. Siihen liittyy läheisesti myös Wilsonin lause.

Lause 2.5 (Fermat'n pieni lause) *Olkoon p alkuluku. Jos kokonaisluku a ei ole jaollinen alkuluvulla p, niin*

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

Todistus. Vrt. [2] s. 19. Tarkastellaan lukuja $0, a, 2a, \ldots, (p-1)a$. Mitkään kaksi näistä eivät ole kongruentteja modulo p. Jos näin olisi, olisi olemassa sellaiset luvut $i, j \in 0, 1, 2, \ldots, (p-1)$, että $ia \equiv ja \pmod{p}$. Tällöin $p|(i-j)a$, ja koska $p \nmid a$, niin $p|(i-j)$. Koska $i, j < p$, niin $i = j$. Toisin sanoen kokonaislukujoukko $0, a, 2a, \ldots, (p-1)a$ on uudelleenjärjestely kokonaislukujoukosta $0, 1, 2, \ldots, (p-1)$ modulo p. Nyt ensimmäisen joukon tulo on kongruentti toisen joukon tulon kanssa modulo p, eli

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

Nyt $p|((p-1)!(a^{p-1}-1))$. Koska $p \nmid (p-1)!$, niin $p|(a^{p-1}-1)$. Siis

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

□

Esimerkki 2.9 Etsitään luvun 4^{123} pienin positiivinen jäännös modulo 7. Fermat'n pienen lauseen mukaan tiedetään, että $4^6 \equiv 1 \pmod{7}$, koska $7 \nmid 4$. Nyt

$$4^{123} = (4^6)^{20} \cdot 4^3 \equiv 1^{20} \cdot 4^3 \equiv 64 \equiv 1 \pmod{7}.$$

Siis luvun 4^{123} pienin positiivinen jäännös modulo 7 on 1.

Fermat'n pienellä lauseella on myös laajennus.

Lause 2.6 *Olkoon p alkuluku ja olkoon a positiivinen kokonaisluku. Tällöin*

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

Todistus Vrt. [5] s. 200. Jos $p \nmid a$, niin Fermat'n pienen lauseen mukaan $a^{p-1} \equiv 1 \pmod{p}$. Kun nyt kerrotaan kongruenssin molemmat puolet luvulla a saadaan $a^p \equiv a \pmod{p}$. Oletetaan nyt, että $p|a$. Tällöin $p|a^p$, joten $a^p \equiv a \equiv 0 \pmod{p}$. □

Lause 2.7 (Wilsonin lause) *Olkoon p alkuluku. Tällöin*

$$(p-1)! \equiv -1 \pmod{p}.$$

Todistus. Vrt. [8] s. 53. Kaikilla luvun $(p-1)!$ tekijöillä $1, 2, \ldots, p-1$ on käänteisluku mod p, eli jokaiselle kokonaisluvulle $a \in \{1, 2, \ldots, p-1\}$ on olemassa yksikäsitteinen kokonaisluku $a^{-1} \in \{1, 2, \ldots, p-1\}$, että $aa^{-1} \equiv 1 \pmod{p}$. Siis jokainen luku a voidaan poistaa käänteisluvullaan lukuunottamatta lukuja, jotka ovat itsensä vastalukuja. Tällaisia lukuja ovat vain

$$1 \equiv -1 \pmod{p}$$

ja

$$p - 1 \equiv -1 \pmod{p},$$

sillä jos $x^2 \equiv 1 \pmod{p}$, niin

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

Toisin sanoen luku p jakaa luvun $(x-1)(x+1)$. Siis luku p jakaa joko luvun $(x-1)$ tai luvun $(x+1)$. Siis $x \equiv 1 \pmod{p}$ tai $x \equiv -1 \pmod{p}$. Näin ollen

$$(p-1)! \equiv -1 \pmod{p}.$$

□

Esimerkki 2.10 Wilsonin lauseen mukaan

$$6! = 720 \equiv -1 \pmod{7}$$

ja

$$12! = 479001600 \equiv -1 \pmod{13}.$$

2.5 Valealkuluvuista

Fermat'n pienen lauseen laajennuksen mukaan, jos n on alkuluku ja b on kokonaisluku, niin $b^n \equiv b \pmod{n}$. Näin ollen, jos on olemassa sellainen kokonaisluku b, että $b^n \not\equiv b \pmod{n}$, niin n ei ole alkuluku.

Esimerkki 2.11 Luku 33 ei ole alkuluku, sillä

$$2^{33} = 2^{30} \cdot 2^3 = (2^5)^6 \cdot 2^3 = 32^6 \cdot 2^3 \equiv 2^3 \equiv 8 \not\equiv 2 \pmod{33}.$$

Fermat'n pienen lauseen avulla voidaan siis löytää kokonaislukuja, jotka eivät ole alkulukuja. Käänteisesti tämä ei kuitenkaan toimi, kuten seuraava esimerkki osoittaa.

Esimerkki 2.12 Vrt. [5] s. 205. Olkoon $n = 341 = 11 \cdot 31$. Fermat'n pienen lauseen mukaan $2^{10} \equiv 1 \pmod{11}$, joten $2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}$. Koska $2^{340} = (2^5)^{68} \equiv 32^{68} \equiv 1 \pmod{31}$, niin $2^{340} \equiv 1 \pmod{341}$. Kertomalla kongruenssi molemmin puolin luvulla 2 saadaan $2^{341} \equiv 2 \pmod{341}$, vaikka luku 341 ei ole alkuluku.

Edellisen kaltaiset esimerkit johtavat valealkulukujen määritelmään.

Määritelmä 2.3 *Olkoon b positiivinen kokonaisluku. Jos luku n ei ole alkuluku ja*

$$b^n \equiv b \pmod{n},$$

*kutsutaan lukua n tällöin b-*kantaiseksi valealkuluvuksi*.*

Huomautus 2.4 Jos $(b, n) = 1$, niin kongruenssi $b^n \equiv b \pmod{n}$ on yhtäpitävä kongruenssin $b^{n-1} \equiv 1 \pmod{n}$ kanssa.

Esimerkki 2.13 Edellisessä esimerkissä ollut luku 341 on 2-kantainen valealkuluku. Vastaavasti luku 471 on 2-kantainen valealkuluku, sillä $2^{470} \equiv 1 \pmod{471}$, mutta $471 = 157 \cdot 3$ ja luku 143 on 3-kantainen valealkuluku, sillä $3^{143} \equiv 1 \pmod{143}$, mutta $143 = 11 \cdot 13$.

Valealkuluvut ovat huomattavasti harvinaisempia kuin alkuluvut. Lukua 10^{10} pienempiä alkulukuja on 455 052 512, mutta tätä pienempiä 2-kantaisia valealkulukuja on vain 14 884 (lähde [5] s. 206). Tästä huolimatta valealkulukuja on ääretön määrä millä tahansa kantaluvulla. Tätä ei kuitenkaan tässä tutkielmassa todisteta.

Määritelmä 2.4 *Olkoon n positiivinen kokonaisluku, joka ei ole alkuluku. Jos $b^{n-1} \equiv 1 \pmod{n}$ kaikilla kokonaisluvuilla b, joille $(b, n) = 1$, kutsutaan lukua n tällöin* Carmichaelin luvuksi*.*

Esimerkki 2.14 Tarkastellaan lukua $1105 = 5 \cdot 13 \cdot 17$. Jos $(b, 1105) = 1$, niin $(b, 5) = (b, 13) = (b, 17) = 1$. Tällöin Fermat'n pienen lauseen mukaan $b^4 \equiv 1 \pmod{5}$, $b^{12} \equiv 1 \pmod{13}$ ja $b^{16} \equiv 1 \pmod{17}$. Nyt $b^{1104} \equiv (b^4)^{276} \equiv 1 \pmod{5}$, $b^{1104} \equiv (b^{12})^{92} \equiv 1 \pmod{13}$ ja $b^{1104} \equiv (b^{16})^{69} \equiv 1 \pmod{17}$. Siis $b^{1104} \equiv 1 \pmod{1105}$ aina, kun $(b, 1105) = 1$. Siis luku 1105 on Carmichaelin luku.

Pienimmät Carmichaelin luvut ovat 561, 1105, 1729, 2465, 2821, 6601 ja 8911 (lähde [10]). Myös Carmichaelin lukuja on ääretön määrä, mutta tämä todistus sivuutetaan.

3 Primitiiviset juuret

3.1 Eulerin lause

Eulerin lause on yhdessä Fermat'n pienen lauseen kanssa yksi lukuteorian tärkeimmistä lauseista. Ennen kuin sitä voidaan käsitellä, pitää kuitenkin käydä läpi joitakin pohjustavia määritelmiä ja lauseita.

Määritelmä 3.1 *Olkoon n positiivinen kokonaisluku.* Eulerin φ - funktio $\varphi(m)$ *on sellaisten positiivisten kokonaislukujen määrä, jotka eivät ylitä lukua m ja ovat keskenään jaottomia luvun m kanssa.*

Esimerkki 3.1 Seuraavassa taulukossa ovat Eulerin φ - funktion arvot luvun m arvoille 1 - 10.

m	1	2	3	4	5	6	7	8	9	10
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4

Huomautus 3.1 $\varphi(m)$ on parillinen aina, kun $m \geq 3$ (Ks. [5] s. 225), ja jos m on alkuluku, niin $\varphi(m) = m - 1$ (Ks. [5] s. 223).

Määritelmä 3.2 Supistettu jäännössysteemi modulo m *on $\varphi(m)$ alkiota sisältävä joukko sellaisia kokonaislukuja, että jokainen joukon luku on keskenään jaoton luvun m kanssa eivätkä mitkään kaksi joukon lukua ole kongruentteja modulo m.*

Esimerkki 3.2 Kokonaislukujoukko 1, 2, 4, 5, 7 ja 8 on supistettu jäännössysteemi modulo 9.

Lause 3.1 *Olkoon $r_1, r_2, \ldots, r_{\varphi(m)}$ supistettu jäännössysteemi modulo m. Olkoon a sellainen positiivinen kokonaisluku, että $(a, m) = 1$. Tällöin joukko $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ on supistettu jäännössysteemi modulo m.*

Todistus. Vrt. [5] s. 216. Todistetaan ensin, että kokonaisluku ar_j on keskenään jaoton luvun m kanssa. Oletetaan, että luku ar_j ei ole keskenään jaoton luvun m kanssa. Tällöin on olemassa sellainen alkuluku p, että $(ar_j, m)|p$. Siis joko $p|a$ tai $p|r_j$. Tällöin joko $p|a$ ja $p|m$ tai $p|r_j$ ja $p|m$. Kuitenkaan sekä $p|r_j$ että $p|m$ eivät voi olla samaan aikaan voimassa, koska r_j kuuluu supistettuun jäännössysteemiin modulo m. Myöskään $p|a$ ja $p|m$ eivät voi olla

samaan aikaan voimassa, sillä $(a, m) = 1$. Siis luvut ar_j ja m ovat keskenään jaottomia aina, kun $j = 1, 2, \ldots, \varphi(m)$.

Todistetaan nyt, etteivät mitkään kaksi muotoa ar_j olevaa lukua ole kongruentteja modulo m. Oletetaan, että $ar_j \equiv ar_k \pmod{m}$, missä luvut j ja k ovat sellaisia toisistaan eriäviä positiivisia kokonaislukuja, että $1 \leq j \leq \varphi(m)$ ja $1 \leq k \leq \varphi(m)$. Koska $(a, m) = 1$, niin $r_j \equiv r_k \pmod{m}$. Tämä on mahdotonta, sillä luvut r_j ja r_k kuuluvat alkuperäiseen supistettuun jäännössysteemiin modulo n, joten $r_j \not\equiv r_k \pmod{m}$. □

Eulerin φ - funktio on multiplikatiivinen, kuten seuraava lause osoittaa.

Lause 3.2 *Olkoon m ja n sellaisia kokonaislukuja, että* $(m,n) = 1$. *Tällöin* $\varphi(mn) = \varphi(m)\varphi(n)$.

Todistus. Ks. [9] s. 164.

Esimerkki 3.3 Kokonaislukujoukko 1, 2, 4, 5, 7 ja 8 on supistettu jäännössysteemi modulo 9. Koska $(4, 9) = 1$, niin lauseen 3.1 mukaan joukko $4 \cdot 1 = 1$, $4 \cdot 2 = 8$, $4 \cdot 4 = 16$, $4 \cdot 5 = 20$, $4 \cdot 7 = 28$ ja $4 \cdot 8 = 32$ on myös supistettu jäännössysteemi modulo 9.

Lause 3.3 (Eulerin lause) *Olkoon m positiivinen kokonaisluku ja olkoon a sellainen kokonaisluku, että* $(a, m) = 1$. *Tällöin*

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

Todistus. Vrt. [4] s. 67. Olkoon $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ supistettu jäännössysteemi modulo m. Koska $(a, m) = 1$, niin $(ar_i, m) = 1$, kun $i = 1, 2, \ldots, \varphi(m)$. Nyt jokaista lukua $i \in \{1, 2, \ldots, \varphi(m)\}$ kohti on olemassa sellainen $\sigma(i) \in \{1, 2, \ldots, \varphi(m)\}$, että

$$ar_i \equiv r_{\sigma(i)} \pmod{m}.$$

Edelleen, $ar_i \equiv ar_j \pmod{m}$, jos ja vain jos $i = j$, ja siis σ on permutaatio joukosta $\{1, 2, \ldots, \varphi(m)\}$ ja $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ on myös supistettu jäännössysteemi modulo m. Nyt siis

$$\begin{aligned} a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} &\equiv (ar_1)(ar_2)\cdots(ar_{\varphi(m)}) \pmod{m} \\ &\equiv r_{\sigma(1)} r_{\sigma(2)} \cdots r_{\sigma(\varphi(m))} \pmod{m} \\ &\equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}. \end{aligned}$$

Kun tämä jaetaan luvulla $r_1 r_2 \cdots r_{\varphi(m)}$, saadaan

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

□

Huomautus 3.2 Fermat'n pieni lause on Eulerin lauseen luonnollinen seuraus. Mikäli Eulerin lause on jo todistettu, kun ryhdytään käsittelemään Fermat'n pientä lausetta, sen todistus on huomattavasti helpompi, kuin tapa jolla se on tässä tutkielmassa todistettu, ks. [4] s. 68.

Esimerkki 3.4 Eulerin lauseen mukaan

$$5^{\varphi(16)} = 5^8 = 390625 \equiv 1 \pmod{16},$$

sillä $(5, 16) = 1$.

Eulerin lausetta voidaan käyttää käänteislukujen etsimiseen modulo m, sillä jos luvut a ja m ovat keskenään jaottomia, niin

$$a \cdot a^{\varphi(m)-1} = a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Tällöin $a^{\varphi(m)-1}$ on luvun a käänteisluku modulo m.

Esimerkki 3.5 Koska

$$2^{\varphi(7)-1} = 2^{6-1} = 2^5 = 32 \equiv 4 \pmod{7},$$

niin luku 4 on luvun 2 käänteisluku modulo 7.

Edellistä esimerkkiä voidaan käyttää lineaarikongruenssiyhtälöiden ratkaisemiseen. Kun ratkaistaan kongruenssiyhtälöä $ax \equiv b \pmod{m}$, jossa $(a, m) = 1$, voidaan kertoa yhtälön molemmat puolet käänteisluvulla $a^{\varphi(m)-1}$. Tällöin saadaan

$$a^{\varphi(m)-1}ax \equiv a^{\varphi(m)-1}b \pmod{m}.$$

Näin ollen ratkaisuksi saadaan sellaiset luvut x, että

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

Esimerkki 3.6 Etsitään ratkaisu lineaarikongruenssiin $5x \equiv 9 \pmod{12}$. Koska $(5, 12) = 1$, voidaan käyttää Eulerin lausetta. Koska $\varphi(12) = 4$, niin

$$x \equiv 5^{4-1} \cdot 9 \equiv 5^3 \cdot 9 \equiv 5 \cdot 9 \equiv 9 \pmod{12}.$$

3.2 Kokonaisluvun kertaluku

Eulerin lauseen mukaan, jos positiiviset kokonaisluvut a ja m ovat keskenään jaottomia, niin $a^{\varphi(m)} \equiv 1 \pmod{m}$. Näin ollen on olemassa ainakin yksi sellainen positiivinen kokonaisluku x, että kongruenssi $a^x \equiv 1 \pmod{m}$ toteutuu. Hyvinjärjestysperiaatteen mukaan on olemassa pienin positiivinen kokonaisluku x, joka toteuttaa kyseisen kongruenssin. Tämä johtaa kertaluvun määritelmään.

Määritelmä 3.3 *Olkoot a ja m keskenään jaottomia positiivisia kokonaislukuja. Tällöin pienintä positiivista kokonaislukua x, joka toteuttaa kongruenssin*

$$a^x \equiv 1 \pmod{m},$$

kutsutaan kokonaisluvun a kertaluvuksi *modulo m. Tällöin merkitään* $\mathrm{ord}_m a = x$.

Esimerkki 3.7 Etsitään luvun 3 kertaluku modulo 8. Tämä on olemassa, sillä $(3, 8) = 1$. Lasketaan luvun 3 potenssien pienimmät positiiviset jäännökset modulo 8. Nyt

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

Siis $\mathrm{ord}_8 3 = 2$.
Vastaavasti $\mathrm{ord}_8 5 = 2$, $\mathrm{ord}_9 2 = 6$ ja $\mathrm{ord}_7 3 = 6$.

Lause 3.4 *Olkoon a kokonaisluku ja olkoon m positiivinen kokonaisluku siten, että $(a, m) = 1$. Tällöin positiivinen kokonaisluku x on kongruenssin*

$$a^x \equiv 1 \pmod{m}$$

ratkaisu, jos ja vain jos $\mathrm{ord}_m a | x$.

Todistus. Vrt. [5] s. 308. Jos $\mathrm{ord}_m a | x$, niin $x = k \cdot \mathrm{ord}_n a$, jossa k on positiivinen kokonaisluku. Siis

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

Käänteisesti, jos $a^x \equiv 1 \pmod{m}$, niin saadaan

$$x = q \cdot \mathrm{ord}_m a + r,\ 0 \leq r \leq \mathrm{ord}_m a.$$

Edelleen

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

Koska $a^x \equiv 1 \pmod{m}$, niin $a^r \equiv 1 \pmod{m}$ ja koska $0 \leq r < \mathrm{ord}_m a$, niin $r = 0$, sillä määritelmän mukaan $y = \mathrm{ord}_m a$ on pienin sellainen positiivinen kokonaisluku, että $a^y \equiv 1 \pmod{m}$. Koska $r = 0$, niin $x = q \cdot \mathrm{ord}_m a$. Siis $\mathrm{ord}_m a | x$. □

Seuraus 3.1 Vrt. [5] s. 309. *Eulerin lauseesta ja lauseesta* 3.4 *seuraa, että kun a ja m ovat keskenään jaottomia kokonaislukuja ja* $m > 0$*, niin*

$$\mathrm{ord}_m a | \varphi(m).$$

Esimerkki 3.8 Etsitään kongruenssille $3^x \equiv 1 \pmod{8}$ jokin ratkaisu. Edellisen esimerkin mukaan $\mathrm{ord}_8 3 = 2$. Koska $2|4$, niin lauseen 3.4 mukaan luku 4 on ratkaisu kongruessiin $3^x \equiv 1 \pmod{8}$. Samoin, koska $2|6$ ja $2|18$, ovat luvut 6 ja 18 ratkaisuja kyseiseen kongruenssiin.

Esimerkki 3.9 Seurauksen 3.1 avulla kokonaisluvun kertaluvun löytäminen on helpompaa. Etsitään kertaluku luvulle 3 modulo 10. Tiedetään, että $\varphi(10) = 4$. Koska ainoat luvun 4 positiiviset tekijät ovat 1, 2 ja 4, ovat ne myös ainoat mahdolliset arvot kertaluvulle $\mathrm{ord}_{10} 3$. Nyt $3^1 \equiv 3 \pmod{10}$, $3^2 \equiv 9 \pmod{10}$ ja $3^4 \equiv 81 \equiv 1 \pmod{10}$. Siis $\mathrm{ord}_{10} 3 = 4$.

Lause 3.5 *Olkoon t positiivinen kokonaisluku ja olkoon* $\mathrm{ord}_m a = k$*. Tällöin*

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

Todistus. Vrt. [9] s. 199. Merkitään $(t,k) = d$, $t = bd$, $k = cd$ ja $(b,c) = 1$. Nyt

$$(a^t)^c = (a^{bd})^c = (a^{cd})^b = (a^k)^b \equiv 1 \pmod{m}.$$

Lauseen 3.4 mukaan $\mathrm{ord}_m(a^t) | c$. Nyt

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

Nyt lauseen 3.4 mukaan $k | t \cdot \mathrm{ord}_m(a^t)$. Siis $cd|(bd)\mathrm{ord}_m(a^t)$ ja edelleen $c | b \cdot \mathrm{ord}_m(a^t)$. Koska b ja c ovat keskenään jaottomia lukuja, niin luku c jakaa luvun $\mathrm{ord}_m(a^t)$. Siis $c = \mathrm{ord}_m(a^t)$. Tästä seuraa, että

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

□

Esimerkki 3.10 Esimerkin 3.7 mukaan tiedetään, että $\mathrm{ord}_9 2 = 6$. Lauseen 3.5 mukaan,

$$\mathrm{ord}_9(2)^8 = \frac{6}{(8,6)} = \frac{6}{2} = 3.$$

Lause 3.6 *Olkoot a ja m keskenään jaottomia kokonaislukuja siten, että $m > 0$. Tällöin*

$$a^i \equiv a^j \pmod{m},$$

jossa $i, j \geq 0$, jos ja vain jos

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

Todistus. Vrt. [5] s. 310. Oletetaan, että $i \equiv j \pmod{\mathrm{ord}_m a}$ ja $0 \leq j \leq i$. Nyt $i = j + k \cdot \mathrm{ord}_m a$, jossa k on positiivinen kokonaisluku. Näin ollen

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

koska $a^{\mathrm{ord}_m a} \equiv 1 \pmod{m}$.

Käänteisesti, oletetaan, että $a^i \equiv a^j \pmod{m}$, jossa $i \geq j$. Koska $(a, m) = 1$, niin $(a^j, m) = 1$. Näin ollen kongruenssista

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

seuraa, että

$$a^{i-j} \equiv 1 \pmod{m},$$

kun jaetaan puolittain luvulla a^j. Lauseen 3.4 mukaan kertaluku $\mathrm{ord}_m a$ jakaa luvun $i - j$, eli

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

□

Esimerkki 3.11 Tarkastellaan lukuja 5 ja 12. Selvästi $(5, 12) = 1$ ja $\mathrm{ord}_{12} 5 = 2$. Lauseen 3.5 mukaan $5^3 \equiv 5^7 \pmod{12}$ ja $5^{124} \equiv 5^{34} \pmod{12}$, sillä $3 \equiv 7 \pmod{2}$ ja $124 \equiv 34 \pmod{2}$.

3.3 Primitiiviset juuret

Määritelmä 3.4 *Olkoon q kokonaisluku ja olkoon m positiivinen kokonaisluku. Jos*

$$\mathrm{ord}_m q = \varphi(m),$$

niin lukua q kutsutaan tällöin primitiiviseksi juureksi *modulo m.*

Esimerkki 3.12 Esimerkin 3.7 mukaan $\mathrm{ord}_7 3 = 6 = \varphi(7)$. Siis luku 3 on primitiivinen juuri modulo 7. Vastaavasti luku 2 on primitiivinen juuri modulo 9.

Huomautus 3.3 Kaikilla kokonaisluvuilla ei ole primitiivisiä juuria. Esimerkiksi ei ole olemassa primitiivisiä juuria modulo 8. Seuraava lause osoittaa, millaisilla luvuilla primitiivinen juuri on olemassa.

Lause 3.7 *Olkoot m ja k positiivisia kokonaislukuja ja olkoon p pariton alkuluku. Luvulla m on primitiivinen juuri, jos ja vain jos $m = 2$, $m = 4$, $m = p^k$ tai $m = 2p^k$.*

Todistus. Todistetaan ensin tapaukset $m = 2$ ja $m = 4$. Vrt. [4] s. 94. Selvästi 1 on primitiivinen juuri modulo 2 ja 3 on primitiivinen juuri modulo 4. Todistetaan, että kun $k \geq 3$, ei ole olemassa primitiivistä juurta modulo 2^k. Koska $\varphi(2^k) = 2^{k-1}$, riittää osoittaa, että

$$a^{2^{k-2}} \equiv 1 \pmod{2^k},$$

jossa luku a on pariton ja $k \geq 3$. Todistetaan induktiolla luvun k suhteen. Tapauksessa $k = 3$,

$$a^{2^{3-2}} = a^2 \equiv 1 \pmod{2^3},$$

sillä

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}.$$

Siis ei ole olemassa primitiivisiä juuria modulo 8. Olkoon nyt $k \geq 3$ ja oletetaan, että $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. Tällöin $2^k | (a^{2^{k-2}} - 1)$. Koska luku a on pariton, niin luku $a^{2^{k-2}} + 1$ on parillinen. Tästä seuraa, että luku

$$a^{2^{k-1}} - 1 = (a^{2^{k-2}} - 1)(a^{2^{k-2}} + 1)$$

on jaollinen luvulla 2^{k+1}. Näin ollen

$$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}},$$

ja tällöin induktioperiaatteen mukaan tapaukset $m = 2$ ja $m = 4$ on todistettu.

Todistetaan nyt tapaukset $m = p^k$ ja $m = 2p^k$, vrt. [4] s. 91. Olkoot a ja m sellaisia kokonaislukuja, että $(a, m) = 1$ ja $m \geq 3$. Oletetaan, että $m = m_1 m_2$, jossa $(m_1, m_2) = 1$ ja $m_1,\ m_2 \geq 3$. Tällöin $(a, m_1) = (a, m_2) = 1$. Koska $m \geq 3$, $\varphi(m)$ on parillinen. Olkoon

$$n = \frac{\varphi(m)}{2} = \frac{\varphi(m_1)\varphi(m_2)}{2}.$$

Eulerin lauseen mukaan

$$a^{\varphi(m_1)} \equiv 1 \pmod{m_1},$$

josta seuraa, että

$$a^n = (a^{\varphi(m_1)})^{\varphi(m_2)/2} \equiv 1 \pmod{m_1}.$$

Vastaavasti

$$a^n = (a^{\varphi(m_2)})^{\varphi(m_1)/2} \equiv 1 \pmod{m_2}.$$

Koska $(m_1, m_2) = 1$ ja $m = m_1 m_2$, niin

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

Näin ollen luvun a kertaluku modulo m on pienempi kuin $\varphi(m)$. Tästä johtuu, että jos luku m voidaan jakaa tekijöihinsä, ei tällöin ole olemassa primitiivistä juurta modulo m. Erityisesti, jos luku m voidaan jakaa kahdella toisistaan eriävällä parittomalla alkuluvulla, ei luvulla m tällöin ole primitiivistä juurta. Vastaavasti, jos luku $m = 2^l p^k$, jossa $l \geq 2$, niin luvulla m ei ole primitiivistä juurta. Käänteisesti, ks. [4] s. 92. Näin ollen primitiivisiä juuria on ainoastaan luvuilla m $(\neq 2^l)$, jotka ovat muotoa p^k tai $2p^k$. □

Lause 3.8 *Jos luku q on primitiivinen juuri modulo m, niin luvut*

$$q, q^2, \ldots, q^{\varphi(m)}$$

muodostavat supistetun jäännössysteemin modulo m.

Todistus. Vrt. [9] s. 201. Koska q on primitiivinen juuri modulo m, niin $\mathrm{ord}_m q = \varphi(m)$ ja $(q, m) = 1$. Näin ollen $(q^i, m) = 1$, jossa $i = 1, 2, \ldots, \varphi(m)$. Lukujoukossa $q, q^2, \ldots, q^{\varphi(m)}$ on yhteensä $\varphi(m)$ kappaletta keskenään inkongruenttia positiivista kokonaislukua. Jos $q^i \equiv q^j \pmod{m}$, jossa $1 \leq i < j \leq \varphi(m)$, niin lauseen 3.5 mukaan $i \equiv j \pmod{\varphi(m)}$. Näin ollen $\varphi(m)$ jakaa luvun $j - i$, joka on mahdotonta sillä $0 < j - i < \varphi(m)$. Siis $q^i \not\equiv q^j \pmod{\varphi(m)}$, jossa $1 \leq i < j \leq \varphi(m)$. Nyt luvut $q, q^2, \ldots, q^{\varphi(m)}$ muodostavat supistetun jäännössysteemin modulo m. □

Esimerkki 3.13 Edellisen esimerkin mukaan luku 3 on primitiivinen juuri modulo 7. Nyt lauseen 3.8 mukaan luvut

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

muodostavat supistetun jäännössysteemin modulo 7.

Lause 3.9 *Olkoon r primitiivinen juuri modulo m. Tällöin r^t on primitiivinen juuri modulo m, jos ja vain jos $(t, \varphi(m)) = 1$.*

Todistus. Vrt. [5] s. 312. Lauseen 3.5 mukaan tiedetään, että

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

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

Tämä johtaa suoraan seuraavaan lauseeseen.

Lause 3.10 *Olkoon m sellainen luku, että on olemassa vähintään yksi primitiivinen juuri modulo m. Tällöin primitiivisten juurten kokonaismäärä modulo m on $\varphi(\varphi(m))$.*

Todistus. Vrt. [5] s. 312. Olkoon r primitiivinen juuri modulo m. Lauseen 3.7 mukaan luvut $r, r^2, \ldots, r^{\varphi(m)}$ muodostavat supistetun jäännössysteemin modulo m. Lauseen 3.9 mukaan tiedetään, että r^t on primitiivinen juuri modulo m, jos ja vain jos $(t, \varphi(m)) = 1$. Koska on olemassa tasan $\varphi(\varphi(m))$ kappaletta tällaisia kokonaislukuja t, on primitiivisiä juuria modulo m on tasan $\varphi(\varphi(m))$ kappaletta. □

Esimerkki 3.14 Olkoon $m = 9$. Esimerkin 3.12 mukaan luku 2 on primitiivinen juuri modulo 9. Koska on olemassa primitiivinen juuri modulo 9, niin lauseen 3.10 mukaan on olemassa $\varphi(\varphi(9)) = 2$ primitiivistä juurta modulo 9. Koska 2 on primitiivinen juuri modulo 9, lauseen 3.9 mukaan $2^5 = 32 \equiv 5 \pmod 9$ on primitiivinen juuri modulo 9. Siis luvut 2 ja 5 muodostavat täydellisen inkongruenttien primitiivisten juurten joukon modulo 9.

Primitiiviset juuret auttavat myös tutkimaan sitä, onko kongruenssiyhtälöllä ratkaisu.

Lause 3.11 *Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että $(a, p) = 1$. Tällöin kongruenssiyhtälöllä*

$$x^m \equiv a \pmod p$$

on ratkaisu, jos ja vain jos

$$a^{\frac{(p-1)}{d}} \equiv 1 \pmod p,$$

jossa $d = (m, p-1)$.

Todistus. Vrt. [9] s. 204. Oletetaan, että $a^{\frac{(p-1)}{d}} \equiv 1 \pmod p$ ja olkoon q primitiivinen juuri modulo p, joka on olemassa lauseen 3.7 mukaan. Nyt on olemassa sellainen kokonaisluku s, että $a = q^s$. Siis

$$q^{\frac{s(p-1)}{d}} \equiv a^{\frac{(p-1)}{d}} \equiv 1 \pmod p.$$

Koska q on primitiivinen juuri modulo p, $\mathrm{ord}_p q = p - 1$. Siis $s/d = k$ on kokonaisluku ja $a \equiv q^{kd} \pmod p$. Koska $d = (m, p-1)$, niin on olemassa sellaiset kokonaisluvut u ja v, että $d = um + v(p-1)$. Näin ollen

$$a = q^{kd} = q^{kum+kv(p-1)} = q^{kum} q^{(p-1)kv} = q^{(ku)m} \cdot 1 = q^{(ku)m}.$$

Siis q^{ku} on ratkaisu kongruenssiyhtälölle $x^m \equiv a \pmod p$.

Oletetaan nyt, että kongruenssilla $x^m \equiv a \pmod p$ on ratkaisu y. Fermat'n pienen lauseen mukaan

$$a^{\frac{p-1}{d}} \equiv y^{\frac{m(p-1)}{d}} \equiv (y^{p-1})^{\frac{m}{d}} \equiv 1 \pmod p,$$

jossa $d = (m, p-1)$. □

Esimerkki 3.15 Kongruenssiyhtälöllä $x^6 \equiv 7 \pmod{31}$ ei ole ratkaisua, sillä

$$7^{\frac{31-1}{(31-1,6)}} = 7^{\frac{30}{6}} = 7^5 \equiv 5 \pmod{31}.$$

Kongruenssiyhtälöllä $x^8 \equiv 16 \pmod{17}$ on ratkaisu, sillä

$$16^{\frac{17-1}{(17-1,8)}} = 16^{\frac{16}{8}} = 16^2 \equiv 1 \pmod{17}.$$

Valealkuluvut osoittivat, että Fermat'n pienellä lauseella ei voida todistaa sitä, onko jokin luku alkuluku. Primitiivisten juurten avulla Fermat'n pientä lausetta voidaan kuitenkin soveltaa alkulukujen löytämiseen, kuten seuraava lause osoittaa.

Lause 3.12 (Lucasin käännös Fermat'n pienestä lauseesta) *Olkoon m positiivinen kokonaisluku. Jos on olemassa sellainen kokonaisluku x, että*

$$x^{m-1} \equiv 1 \pmod{m}$$

ja

$$x^{\frac{m-1}{q}} \not\equiv 1 \pmod{m}$$

kaikilla luvuilla q jotka ovat luvun $m-1$ alkulukutekijöitä, niin m on alkuluku.

Todistus. Vrt. [5] s. 340. Koska $x^{m-1} \equiv 1 \pmod{m}$, niin lauseen 3.4 mukaan $\mathrm{ord}_m x | (m-1)$. Osoitetaan, että $\mathrm{ord}_m x = m-1$. Oletetaan, että $\mathrm{ord}_m x \neq m-1$. Koska $\mathrm{ord}_m x | (m-1)$, niin on olemassa sellainen kokonaisluku k, että $m-1 = k \cdot \mathrm{ord}_m x$ ja koska $\mathrm{ord}_m x \neq m-1$, niin $k > 1$. Olkoon q luvun k alkulukutekijä. Tällöin

$$x^{\frac{m-1}{q}} = x^{\frac{k}{\mathrm{ord}_m x \cdot q}} = (x^{\mathrm{ord}_m x})^{\frac{k}{q}} \equiv 1 \pmod{m}.$$

Tämä on ristiriidassa oletuksen kanssa, joten $\mathrm{ord}_m x = m-1$. Koska $\mathrm{ord}_m x \leq \varphi(m)$ ja $\varphi(m) \leq m-1$, niin $\varphi(m) = m-1$. Huomautuksen 3.1 mukaan luku m on alkuluku. □

Esimerkki 3.16 Tutkitaan, onko luku 71 alkuluku. Luvun 70 alkulukutekijät ovat 2, 5 ja 7. Fermat'n pienen lauseen mukaan $11^{70} \equiv 1 \pmod{71}$. Nyt $11^{35} \equiv 70 \pmod{71}$, $11^{14} \equiv 54 \pmod{71}$ ja $11^{10} \equiv 32 \pmod{71}$. Siis 71 on alkuluku.

4 Neliönjäännökset

4.1 Neliönjäännökset ja Eulerin kriteeri

Määritelmä 4.1 *Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että $p \nmid a$. Tällöin a on* neliönjäännös modulo p*, jos kongruenssilla*

$$x^2 \equiv a \pmod{p}$$

on ratkaisu. Jos kyseisellä kongruenssilla ei ole ratkaisua, kutsutaan lukua a neliönepäjäännökseksi modulo p.

Esimerkki 4.1 Tutkitaan alkulukua 7. Nyt

$$\begin{aligned} 1^2 &\equiv 1 \pmod{7}, \\ 2^2 &\equiv 4 \pmod{7}, \\ 3^2 &\equiv 9 \equiv 2 \pmod{7}, \\ 4^2 &\equiv 16 \equiv 2 \pmod{7}, \\ 5^2 &\equiv (-2)^2 \equiv 4 \pmod{7}, \\ 6^2 &\equiv (-1)^2 \equiv 1 \pmod{7}. \end{aligned}$$

Siis luvut 1, 2 ja 4 ovat neliönjäännöksiä modulo 7 ja luvut 3, 5 ja 6 ovat neliönepäjäännöksiä modulo 7.

Huomautus 4.1 Jos $p|a$, niin $a \equiv 0 \equiv 0^2 \pmod{p}$ ja a on neliönjäännös modulo p.

Huomautus 4.2 Jos $a \equiv b \pmod{p}$, niin a ja b ovat molemmat joko neliönjäännöksiä tai neliönepäjäännöksiä modulo p. Näin ollen neliönjäännöksiä tutkittaessa riittää, että tarkastellaan ainoastaan lukuja $1, 2, \ldots, p-1$.

Apulause 4.1 *Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että $p \nmid a$. Tällöin kongruenssiyhtälöllä*

$$x^2 \equiv a \pmod{p}$$

on joko tasan kaksi ratkaisua tai ei ratkaisuja ollenkaan.

Todistus. Ks. [5] s. 376.

Lause 4.1 *Olkoon p pariton alkuluku. Tällöin on olemassa tasan $\frac{p-1}{2}$ neliönjäännöstä modulo p ja tasan $\frac{p-1}{2}$ neliönepäjäännöstä modulo p välillä $1, 2, \ldots, p-1$.*

Todistus. Vrt. [5] s. 377. Tutkitaan lukujen $1, 2, \ldots, p-1$ neliöiden pienimpiä positiivisia jäännöksiä modulo p. Koska kyseessä on yhteensä $p-1$ neliötä ja koska kongruenssilla $x^2 \equiv a \pmod{p}$ on joko kaksi tai ei yhtään ratkaisua, täytyy tällöin olla tasan $\frac{p-1}{2}$ neliönjäännöstä modulo p välillä $1, 2, \ldots, p-1$. Jäljelle jääneet $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ lukua p pienempää positiivista kokonaislukua ovat neliönepäjäännöksiä modulo p. □

Määritelmä 4.2 Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että $p \not| a$. Tällöin

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

Tätä kutsutaan *Legendren symboliksi.*

Esimerkki 4.2 Esimerkin 4.1 mukaan

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$$

ja

$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Huomautus 4.3 Voidaan myös sanoa, että jos $p|a$, niin

$$\left(\frac{a}{p}\right) = 0.$$

Tämä ei kuitenkaan ole millään tavalla kiinnostavaa tietoa, joten yleensä sitä ei käytetä.

Lause 4.2 (Eulerin kriteeri) *Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että $(a, p) = 1$. Tällöin*

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

Todistus. Vrt. [9] s. 189. Olkoon r sellainen kokonaisluku, että $1 \leq r \leq p-1$. Koska kongruenssilla $rx \equiv a \pmod{p}$ on vain yksi ratkaisu, niin on olemassa täsmälleen yksi sellainen kokonaisluku s, että $rs \equiv a \pmod{p}$. Jos a on neliönepäjäännös modulo p, eli $\left(\frac{a}{p}\right) = -1$, niin $r \not\equiv s \pmod{p}$. Tällöin luvut $1, 2, \ldots, p-1$ voidaan ryhmitellä pareiksi $r_i s_i$ siten, että $r_i s_i \equiv a \pmod{p}$, jossa $i = 1, 2, \ldots, \frac{p-1}{2}$. Nyt Wilsonin lauseen mukaan

$$-1 \equiv (p-1)! \equiv \prod_{i=1}^{\frac{p-1}{2}} r_i s_i \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Jos luku a on neliönjäännös modulo p, eli $\left(\frac{a}{p}\right) = 1$, niin on olemassa sellainen kokonaisluku b, että $b^2 \equiv a \pmod{p}$. Nyt Fermat'n pienen lauseen mukaan

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}.$$

Näin ollen molemmissa tapauksissa saadaan

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

□

Esimerkki 4.3 Tutkitaan, onko luku 7 neliönjäännös modulo 13. Eulerin kriteerin mukaan

$$7^{\frac{13-1}{2}} = 7^6 \equiv -1 \pmod{13}.$$

Siis 7 on neliönepäjäännös modulo 13.

Lause 4.3 *Olkoon p pariton alkuluku ja olkoot a ja b sellaisia kokonaislukuja, että $p \nmid a$ ja $p \nmid b$. Tällöin ovat voimassa seuraavat ominaisuudet.*

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

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

(iii) $\left(\frac{a^2}{p}\right) = 1$

(iv) $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$

Todistus. (i) Vrt. [5] s. 379. Jos $a \equiv b \pmod{p}$, niin kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisu, jos ja vain jos kongruenssilla $x^2 \equiv b \pmod{p}$ on ratkaisu. Siis $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) Vrt. [9] s. 190. Eulerin kriteerin mukaan

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

Koska Legendren symboli saa vain arvoja 1 ja -1, niin

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

(iii) Koska Legendren symboli saa vain arvoja 1 ja -1, niin ominaisuuden (ii) mukaan

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

(iv) Lähde [7]. Eulerin kriteerin mukaan

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

Koska $\left(\frac{-1}{p}\right)$ ja $(-1)^{\frac{p-1}{2}}$ saavat vain arvoja 1 tai -1 ja $1 \not\equiv -1 \pmod{p}$, niin

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

□

Esimerkki 4.4 Tutkitaan, onko kongruenssilla $x^2 \equiv 3 \pmod{11}$ ratkaisu. Koska $3 \equiv 8 \pmod{11}$, saadaan lauseen 4.3 ominaisuuden (ii) perusteella

$$\left(\frac{3}{11}\right) = \left(\frac{8}{11}\right)$$

ja edelleen

$$\left(\frac{8}{11}\right) \equiv \left(\frac{2^2}{11}\right)\left(\frac{2}{11}\right) \equiv \left(\frac{2}{11}\right)2^{\frac{11-1}{2}} \equiv 2^5 \equiv 32 \equiv -1 \pmod{11}.$$

Siis kongruenssi $x^2 \equiv 3 \pmod{11}$ ei ole ratkeava.

4.2 Neliönjäännösten resiprookkilaki

Lause 4.4 (Gaussin lemma) *Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että $(a, p) = 1$. Tällöin*

$$\left(\frac{a}{p}\right) = (-1)^s,$$

jossa luku s on sellaisten kokonaislukujen määrä joukossa

$$\{a, 2a, \ldots, \frac{p-1}{2}a\}, \tag{1}$$

joiden jakojäännös on suurempi kuin $\frac{p}{2}$.

Todistus. Vrt. [3] s. 140. Joukon (1) luvut ovat inkongruentteja modulo p, sillä kongruenssilla

$$ha \equiv ka \pmod{p}$$

on ratkaisu ainoastaan, kun $h \equiv k \pmod{p}$. Olkoot luvut $m_1, m_2, \ldots, m_s$ joukon (1) pienimmät positiiviset lukua $\frac{p}{2}$ suuremmat jakojäännökset modulo p ja olkoot luvut $n_1, n_2, \ldots, n_t$ joukon (1) pienimmät positiiviset lukua $\frac{p}{2}$ pienemmät jakojäännökset modulo p. Tällöin $s + t = \frac{1}{2}(p-1)$. Luvut $p - m_1, p - m_2, \ldots, p - m_s$ ovat kaikki välillä $[0, \frac{1}{2}p]$. Yksikään näistä luvuista ei ole kongruentti toisen tällaisen luvun kanssa modulo p, sillä jos

$$p - m_i \equiv n_j \pmod{p},$$

$$m_i \equiv ba \pmod{p}$$

ja

$$n_j \equiv ca \pmod{p},$$

jossa $i \in \{1, 2, \ldots, s\}$, $j \in \{1, 2, \ldots, t\}$ ja $b, c \in \{1, 2, \ldots, \frac{1}{2}(p-1)\}$, niin

$$b + c \equiv 0 \pmod{p}.$$

Tämä on mahdotonta, sillä selvästi $0 < b + c < p$. Siis luvut

$$n_1, n_2, \ldots, n_t, p - m_1, p - m_2, \ldots, p - m_s \tag{2}$$

ovat kaikki pienempiä tai yhtäsuuria kuin luku $\frac{1}{2}(p-1)$ ja niitä on yhteensä $\frac{1}{2}(p-1)$ kappaletta. Nyt kertomalla kaikki luvut (2) yhteen, saadaan

$$n_1 \cdot n_2 \cdot \cdots \cdot n_t \cdot (p - m_1) \cdot (p - m_2) \cdot \cdots (p - m_s)$$

$$\equiv \left(\frac{p-1}{2}\right)! \equiv (-1)^s \cdot \left(\frac{p-1}{2}\right)! \cdot a^{\frac{1}{2}(p-1)} \pmod{p}.$$

Nyt Eulerin kriteerin mukaan

$$\left(\frac{a}{p}\right) = (-1)^s.$$

□

Esimerkki 4.5 Olkoon $a = 7$ ja $p = 17$. Nyt $\frac{p-1}{2} = 8$.

i	1	2	3	4	5	6	7	8
$a \cdot i$	7	14	21	28	35	42	49	56
jäännös, kun $\frac{ai}{17}$	7	14	4	11	1	8	15	5

Kuten oheinen taulukko osoittaa, lukua $\frac{17}{2}$ pienempiä jakojäännöksiä on yhteensa 5 kappaletta. Siis Gaussin lemman mukaan

$$\left(\frac{7}{17}\right) = (-1)^5 = -1.$$

Siis luku 7 on neliönepäjäännös modulo 17.

Lause 4.5 *Olkoon p pariton alkuluku. Tällöin*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & , jos\ p \equiv \pm 1 \pmod 8, \\ -1 & , jos\ p \equiv \pm 3 \pmod 8). \end{cases}$$

Todistus. Vrt. [9] s. 192. Olkoon s joukon $\{2, 4, \ldots, 2\frac{p-1}{2}\}$ sellaisten alkioiden lukumäärä, jotka ovat suurempia, kuin luku $\frac{p}{2}$. Muotoa $2k$ oleva luku on pienempi kuin $\frac{p}{2}$ aina, kun $k \leq \frac{p}{4}$. Siis,

$$s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

Jos $p = 8k + 1$, niin

$$s = 4k - \lfloor 2k + \frac{1}{4} \rfloor = 4k - 2k \equiv 0 \pmod 2.$$

Jos $p = 8k + 3$, niin

$$s = 4k + 1 - \lfloor 2k + \frac{3}{4} \rfloor = 4k + 1 - 2k \equiv 1 \pmod 2.$$

Jos $p = 8k + 5$, niin

$$s = 4k + 2 - \lfloor 2k + 1 + \frac{1}{4} \rfloor = 2k + 1 \equiv 1 \pmod 2.$$

Jos $p = 8k + 7$, niin

$$s = 4k + 3 - \lfloor 2k + 1 + \frac{3}{4} \rfloor = 2k + 2 \equiv 0 \pmod 2.$$

□

Huomautus 4.4 Koska luku $\frac{p^2-1}{8}$ toteuttaa samat kongruenssit kuin luku s lauseen 4.5 todistuksessa, niin lause 4.5 voidaan myös kirjoittaa muotoon

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Esimerkki 4.6 Lauseen 4.5 mukaan

$$\left(\frac{2}{7}\right) = \left(\frac{2}{17}\right) = 1$$

ja

$$\left(\frac{2}{3}\right) = \left(\frac{2}{5}\right) = \left(\frac{2}{11}\right) = -1.$$

Esimerkki 4.7 Tutkitaan, onko luku 104 neliönjäännös modulo 17. Lauseen 4.3 ominaisuuden (ii) mukaan

$$\left(\frac{104}{17}\right) = \left(\frac{-2}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{2}{17}\right).$$

Koska $\frac{17-1}{2} = 8$, niin lauseen 4.3 ominaisuuden (iv) mukaan $\left(\frac{-1}{17}\right) = 1$. Koska $\frac{17^2-1}{8} = 36$, niin lauseen 4.5 mukaan $\left(\frac{2}{17}\right) = 1$. Siis $\left(\frac{104}{17}\right) = 1$ ja 104 on neliönjäännös modulo 17.

Lause 4.6 (Neliönjäännösten resiprookkilaki) *Olkoot p ja q erisuuria parittomia alkulukuja. Tällöin*

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

Neliönjäännösten resiprookkilain todistamiseen tarvitaan seuraava apulause.

Apulause 4.2 *Olkoot a ja b sellaisia lukua kaksi suurempia parittomia kokonaislukuja, että $(a, b) = 1$. Tällöin*

$$\sum_{i=1}^{\frac{a-1}{2}} \left\lfloor \frac{bi}{a} \right\rfloor + \sum_{j=1}^{\frac{b-1}{2}} \left\lfloor \frac{aj}{b} \right\rfloor = \frac{a-1}{2}\frac{b-1}{2} \ .$$

Todistus. Ks. [3] s. 141.

Todistetaan nyt neliönjäännösten resiprookkilaki käyttämällä apulausetta 4.2.

Todistus. Vrt. [9] s. 193. Tutkitaan kokonaislukuja q_k ja r_k, joissa $kp = pq_k + r_k$ ja $1 \leq r_k \leq p-1$, kun $k = 1, 2, \ldots, \frac{p-1}{2}$. Siis $q_k = \lfloor \frac{kq}{p} \rfloor$ ja r_k on luvun kq pienin jäännös modulo p. Olkoot $a_1, a_2, \ldots, a_r$ luvun r_k lukua $\frac{p}{2}$ pienemmät arvot ja $b_1, b_2, \ldots, b_s$ luvun r_k lukua $\frac{p}{2}$ suuremmat arvot. Nyt $a_1, a_2, \ldots, a_r, p-b_1, p-b_2, \ldots, p-b_s$ ovat luvut $1, 2, \ldots, \frac{p-1}{2}$ jossakin järjestyksessä ja $\left(\frac{q}{p}\right) = (-1)^s$. Olkoon

$$a = \sum_{i=1}^{r} a_j \text{ ja } b = \sum_{j=1}^{s},$$

joten

$$a + b = \sum_{k=1}^{\frac{p-1}{2}} r_k.$$

Näin ollen

$$a + sp - b = \frac{p^2 - 1}{8} \ . \tag{3}$$

Edelleen, olkoon

$$u = \sum_{k=1}^{\frac{p-1}{2}} q_k = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$$

ja ratkaistaan yhtälö $kq = pq_k + r_k$, jossa $1 \leq k \leq \frac{p-1}{2}$. Tällöin saadaan

$$\begin{aligned} pu + a + b &= p\left(\textstyle\sum_{k=1}^{\frac{p-1}{2}} q_k \right) + a + b \\ &= \textstyle\sum_{k=1}^{\frac{p-1}{2}} (pq_k + r_k) \\ &= \textstyle\sum_{k=1}^{\frac{p-1}{2}} kq \\ &= \frac{p^2-1}{8} q. \end{aligned}$$

Vähentämällä yhtälöstä $pu + a + b$ yhtälö (3) saadaan

$$pu + 2b - sp = \left(\frac{p^2 - 1}{8} \right)(q - 1).$$

Koska $p \equiv q \equiv 1 \pmod 2$, niin $u \equiv s \pmod 2$. Näin ollen

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

Toistamalla sama prosessi mutta vaihtamalla lukujen p ja q paikkaa ja käyttämällä luvun u sijasta lukua

$$v = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$$

saadaan

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

Näin ollen

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

Apulauseen 4.2 mukaan saadaan

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

□

Huomautus 4.5 Neliönjäännösten resiprookkilaki voidaan kirjoittaa myös muodossa

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

Esimerkki 4.8 Etsitään arvo Legendren symbolille $\left(\frac{38}{67}\right)$. Lauseen 4.3 ominaisuuden (ii) mukaan

$$\left(\frac{38}{67}\right) = \left(\frac{2}{67}\right)\left(\frac{19}{67}\right).$$

Koska $67 \equiv 3 \pmod 8$, niin lauseen 4.5 mukaan $\left(\frac{2}{67}\right) = -1$. Koska $\frac{19-1}{2}\frac{67-1}{2} = 297$, niin neliönjäännösten resiprookkilain mukaan

$$\left(\frac{2}{67}\right)\left(\frac{19}{67}\right) = (-1)\left(\frac{67}{19}\right)(-1) = \left(\frac{67}{19}\right) = \left(\frac{10}{19}\right).$$

Koska $19 \equiv 3 \pmod 8$ ja $\frac{19-1}{2}\frac{5-1}{2} = 18$, niin lauseiden 4.3 ja 4.5 sekä neliönjäännösten resiprookkilain mukaan

$$\left(\frac{10}{19}\right) = \left(\frac{2}{19}\right)\left(\frac{5}{19}\right) = (-1)\left(\frac{19}{5}\right) = (-1)\left(\frac{4}{5}\right) = (-1)\left(\frac{2^2}{5}\right) = -1.$$

Siis

$$\left(\frac{38}{67}\right) = -1.$$

5 Kryptografia

Lukuteorian tärkein käytännön sovellutus on kryptografia. Kryptografia on oppi salakirjoituksesta, jossa pyritään löytämään turvallisia keinoja lähettää viesti jollekin toiselle niin, ettei kukaan muu kuin vastaanottaja voi sitä lukea. Lukuteorian kannalta kryptografia voidaan jakaa kahteen osa-alueeseen: yhden eli salaisen avaimen ja kahden eli julkisen avaimen järjestelmään.

5.1 Salaisen avaimen kryptografiaa

Käytännössä kaikki ennen 1970-lukua käytössä olleet salausjärjestelmät olivat salaisen avaimen järjestelmiä. Salaisen avaimen järjestelmässä vain vastaanottaja ja lähettäjä tietävät avaimen, ja siinä viesti salataan ja puretaan samalla avaimella. Yksinkertaisimmillaan salaisen avaimen järjestemä on jo Julius Caesarin aikanaan käyttämä kirjaintenvaihtojärjestelmä, jossa esimerkiksi siirretään jokaista salattavan viestin kirjainta viisi kirjainta eteenpäin aakkosissa. Näin sana

KRYPTOGRAFIA

tulisi salattaessa muotoon

PWAUYTLWFKNF.

Toisin sanoen avain on viestiä salattaessa 5 ja purettaessa -5.

Useimmat salaisen avaimen salausjärjestelmät ovat kuitenkin monimutkaisempia. Ne salaavat tiedon määrätyn kokoisissa lohkoissa ja käyvät läpi useita kierroksia jotain yksinkertaista epälineaarista funktiota. Mitä pienemmiksi lohkoiksi tieto salataan, sitä vaikeampi sitä on murtaa. Tällaisia edelleen laajalti käytössä olevia lohkojärjestelmiä on lukuisia. Niiden etuna on nopeus. Suuretkin tiedostot voidaan purkaa tavallisella tietokoneella hetkessä. Ongelmana on se, että molempien osapuolten pitää tietää avain eikä se saa joutua ulkopuolisten käsiin. Lohkosalaimien lisäksi on olemassa virtasalaimia, joissa jokainen viestin merkki korvataan salatulla merkillä. Salaus tapahtuu yleensä satunnaislukugeneraattorilla. Virtasalaimet ovat nopeampia käyttää kuin lohkosalaimet, mutta ne ovat myös helpompia murtaa.

5.2 Julkisen avaimen kryptografiaa

Julkisen avaimen salausjärjestelmä perustuu kahden avaimen käyttöön, joista toista käytetään tiedon salaamiseen ja toista sen purkamiseen. Toinen avaimista on julkinen ja toinen salainen. Vaikka avaimilla on tietty matemaattinen yhteys ja ne ovat toistensa vastakappaleita, ne eivät kerro toisistaan mitään. Kun tieto salataan avaimella, se voidaan purkaa vain sen vastakappaleella. Salaus toimii yksinkertaisesti niin, että lähettäjä salaa tiedon vastaanottajan julkisella avaimella ja vastaanottaja purkaa sen omalla salaisella avaimellaan. Tunnetuin julkisen avaimen salausjärjestelmä on RSA-salausjärjestelmä. Seuraavassa esitellään sen toimintatapa yksityiskohtaisesti ja esitetään siitä käytännön esimerkki.

Olkoot A ja B salausjärjestelmän käyttäjät. A valitsee kaksi erisuurta alkulukua p ja q. Nämä kerrotaan keskenään ja saadaa $n = pq$. A valitsee myös avaimen e siten, että se on kokonaisluku väliltä 1 ja $(p-1)(q-1)$ ja se on keskenään jaoton luvun $(p-1)(q-1)$ kanssa. Tällöin lauseen 2.3 mukaan lineaarikongruenssilla

$$ex \equiv 1 \pmod{(p-1)(q-1)}$$

on ratkaisu. Siis on olemassa sellainen positiivinen kokonaisluku d välillä 1 ja $(p-1)(q-1)$, että

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

Tällöin lukua d kutsutaan käyttäjän A salausavaimeksi. Nyt A julkaisee luvut n ja e, mutta ei lukuja d, p ja q. Nyt käyttäjä B haluaa lähettää käyttäjälle A salatun viestin. B pilkkoo viestin siten, että sen jokainen osa on luku, joka on pienempi kuin n. Selvitetään nyt, kuinka käyttäjä B voi lähettää yksittäisen kokonaisluvun a käyttäjälle A siten, että kukaan ulkopuolinen ei pääse sitä lukemaan. B salaa luvun a korottamalla sen potenssiin e supistaen sen modulo n. Siis B lähettää luvun $a^e \pmod{n}$. Kun A vastaanottaa tämän luvun, hän korottaa sen potenssiin d ja supistaa sen modulo n. Toisin sanoen hän muodostaa luvun $(a^e)^d \pmod{n}$. Selvästi

$$de = 1 + c(p-1)(q-1),$$

jossa c on positiivinen kokonaisluku, koska $d, e > 0$. Nyt

$$\begin{array}{lll} \text{jos} & p \not| a, & \text{niin } (a^e)^d = a^{1+c(p-1)(q-1)} = a(a^{(p-1)})^{c(q-1)} \equiv a1^{c(q-1)} \\ & & \equiv a \pmod{p}, \\ \text{jos} & p|a, & \text{niin } (a^e)^d \equiv 0 \equiv a \pmod{p}. \end{array}$$

Näin ollen jokaista kokonaislukua a kohti $(a^e)^d \equiv a \pmod{p}$. Vastaavasti jokaista kokonaislukua a kohti $(a^e)^d \equiv a \pmod{q}$. Koska p ja q ovat erisuuria alkulukuja, niin

$$(a^e)^d \equiv a \pmod{n}.$$

Näin ollen A on purkanut viestin ja saanut luvun a B:ltä.

Oletetaan nyt, että ulkopuolinen käyttäjä C saa haltuunsa lähetetyn luvun $a^e \pmod{n}$. Voidakseen purkaa viestin hänen täytyy tietää luku d. Selvittääkseen luvun d C:n täytyy pystyä ratkaisemaan kongruenssi $de \equiv 1 \pmod{(p-1)(q-1)}$. Toisin sanoen hänen täytyy saada selville luvut p ja q. C tietää luvun n, sillä A on julkaissut kyseisen luvun. Toisin sanoen C:n pitää vain pystyä jakamaan n kahteen alkulukutekijäänsä. Tämä ei ole vaikeaa, jos kyseessä ovat pienet luvut. Tästä syystä RSA-järjestelmässä pitää käyttää erittäin suuria lukuja. Jos luvuissa p ja q on alle 50 numeroa, luku n voidaan jakaa alkulukutekiöihinsä tavallisella kotitietokoneella ja helposti saatavilla olevalla ohjelmistolla muutamassa minuutissa. Nykyään käytössä olevat RSA-luvut ovat vähintään 200-numeroisia lukuja. Jokainen salattu viesti voidaan tietenkin murtaa myös perinteisesti tutkimalla kirjainten yleisyyttä sanoissa ja niitä vastaavia lukuja viestissä. Tämän vaikeuttamiseksi on mahdollista tehdä esimerkiksi kirjainpareja (esimerkiksi $e = 05$, $n = 14 \Rightarrow en = 0514$), jotka ovat huomattavasti vaikeampia murtaa.

Esimerkki 5.1 Vaikka RSA-järjestelmässä tuleekin käyttää valtavan suuria lukuja, on kuitenkin järkevämpää käyttää pienempiä ja helpommin ymmärret täviä lukuja esimerkissä. Olkoon nyt A ja B RSA:n käyttäjät. A julkaisee luvut $n = 391$ ja $e = 13$, jossa $n = pq = 17 \cdot 23$ ja $(13, (17 - 1)(23 - 1)) = 1$. Nyt B haluaa lähettää A:lle viestin

KRYPTOGRAFIA.

Ensin B muuttaa viestin kirjaimet niitä vastaaviksi numeroiksi (eli A = 01, B = 02, ..., Ö = 29). Näin ollen sana kryptografia muuttuu muotoon

11 18 25 16 20 15 07 18 01 05 09 01.

Nyt B salaa kirjaimen K siten, että hän korottaa luvun 11 potenssiin e ja supistaa sen modulo n, eli

$$11^{13} \equiv 109 \pmod{391}.$$

Nyt B lähettää A:lle luvun 109, joka A:n pitää purkaa. Purkuavain d saadaan kongruenssista

$$13d \equiv 1 \pmod{(17-1)(23-1)}.$$

Kun ratkaistaan tämä kongruenssi esimerkin 2.4 tapaan saadaan $d \equiv 325 \pmod{352}$. Siis $d = 325$. Luku 109 saadaan nyt muotoon $109^{325} \pmod{391}$. Salattu viesti saadaan nyt siis kongruenssista $x \equiv 109^{325} \pmod{391}$ ratkaisemalla x. Koska luku 391 ei ole alkuluku, pitää lauseke $109^{325} \pmod{391}$ jakaa kahteen osaan, jotta moduloiksi saadaan alkuluvut. Koska $391 = 17 \cdot 23$, niin Fermat'n pienen lauseen mukaan $109^{325} \equiv 11 \pmod{17}$ ja $109^{325} \equiv 11 \pmod{23}$. Kun ratkaistaan kongruenssipari

$$\begin{aligned} x &\equiv 11 \pmod{17} \\ x &\equiv 11 \pmod{23}, \end{aligned}$$

saadaan $x \equiv 11 \pmod{391}$. Näin on purettu B:n lähettämä viesti ja saatu kirjain K. Vastaavasti käydään läpi muut kirjaimet, jotta saadaan purettua koko viesti.

Julkisen avaimen salausjärjestelmät ovat yleisesti ottaen turvallisempia kuin salaisen avaimen järjestelmät, sillä niissä vain oma purkuavain on salainen, joten avaimen lähetysongelma on vältetty. Näin ollen ne ovat käyttäjäystävällisempiä myös lähettäjälle, sillä kuka tahansa voi saada selville toisen salausavaimen. Julkisen avaimen järjestelmien, kuten RSA:n, suurimpana haittana on niiden hitaus. Niissä joudutaan käyttämään erittäin suuria alkulukuja, joten niiden salaaminen, lähettäminen ja purkaminen voi viedä pitkiäkin aikoja, jos kyseessä on suuri tiedosto. Salaisen avaimen järjestelmät ovat huomattavasti nopeampia, sillä niissä käytetään pienempiä avaimia, ja niiden purkaminen on suoraviivaisempaa. Tästä johtuen salaisen ja julkisen avaimen järjestelmiä käytetään rinta rinnan: Ennen varsinaisen viestin lähettämistä salaisen avaimen järjestelmällä lähetetään käytettävä salasana julkisen avaimen järjestelmällä.

Kuten todettua, sekä julkisen että salaisen avaimen järjestelmässä joudutaan käyttämään huomattavasti suurempia lukuja, kuin esimerkissä 5.1 on

käytetty. Ongelmana on se, kuinka saada käyttöön valtavan suuria alkulukuja. On olemassa monia tietokoneohjelmia, joilla voidaan muodostaa alkulukuja, mutta niitä voidaan luoda myös seuraavalla lauseella.

Lause 5.1 *Olkoot n ja s sellaisia parittomia kokonaislukuja, että $n-1 = sr$, missä $r \in \mathbf{R}$, ja olkoon luvun s jokaista alkulukutekijää q kohti sellainen kokonaisluku a, että*

$$a^{n-1} \equiv 1 \pmod{n}$$

ja

$$(a^{\frac{n-1}{q}} - 1, n) = 1.$$

Tällöin jokainen luvun n alkulukutekijä p toteuttaa kongruenssin

$$p \equiv 1 \pmod{2s}.$$

Todistus. Ks. [11] s. 102.

Seuraus 5.1 *Olkoot lauseen* 5.1 *oletukset voimassa. Nyt jos*

$$r \leq 4s + 2,$$

niin n on alkuluku.

Todistus. Ks. [11] s. 102.

Esimerkki 5.2 Olkoon $s = 89$ ja olkoon $r = 350 \leq 4s + 2$. Nyt luku $n = sr + 1 = 31151$ on alkuluku, sillä se toteuttaa lauseen 5.1 ja sen seurauksen oletukset.

5.3 Digitaaliset allekirjoitukset

Jotta salatun viestin vastaanottaja voi olla varma lähettäjän autenttisuudesta, voi lähettäjä lisätä viestiin digitaalisen allekirjoituksen. Digitaaliset allekirjoitukset perustuvat julkisen avaimen salausjärjestelmään, joten niitä ei voida käyttää salaisen avaimen järjestelmissä.

Jotta viestin vastaanottaja voisi olla varma lähettäjän henkilöllisyydestä, voi hän kertoa vastaanottajalle jotakin, minkä vain hän voi tietää. Jos viesti on lähetetty RSA-järjestelmällä, tämä tieto voi olla lähettäjän oma purkuavain

d, joka liittyy julkistettuihin lukuihin e ja n. Kukaan ei tietenkään halua paljastaa omaa purkuavaintaan kenellekään. On kuitenkin mahdollista osoittaa, että lähettäjä tietää luvun d paljastamatta kuitenkaan, mikä d on. Lähettäjä valitsee jonkin yleisesti tunnetun viestin m ja lähettää viestin

$$m^d \pmod{n}.$$

Nyt on muodostettu salattu viesti, jonka vain luvun d haltija voi luoda. Koska luvut e ja n ovat kaikkien tiedossa, voi vastaanottaja purkaa viestin $m^d \pmod{n}$ korottamalla sen potenssiin e ja supistamalla modulo n, eli

$$(m^d)^e = m^{ed} \equiv m \pmod{n}.$$

Koska vain $m^d \pmod{n}$ voi purkautua tunnetuksi viestiksi m, voi vastaanottaja olla varma, että lähettäjä tuntee luvun d.

Esimerkki 5.3 Olkoot luvut e, n ja d kuten esimerkissä 5.1. Olkoon m jokin yleisesti tunnettu viesti, esimerkiksi luku 15. Nyt lähettäjä haluaa allekirjoittaa viestinsä, joten hän korottaa luvun 15 potenssiin d ja supistaa sen modulo n. Siis

$$15^{325} \pmod{391}.$$

Vastaanottaja saa nyt allekirjoituksena luvun $a = 15^{325} \pmod{391}$. Hän voi nyt purkaa viestin korottamalla sen potenssiin e ja supistamalla modulo n, eli

$$a^{13} \equiv 15 \pmod{391}.$$

Näin vastaanottaja on saanut purettua allekirjoituksen.

5.4 ElGamal-salausjärjestelmä

RSA-salausjärjestelmän turvallisuus perustuu kokonaislukujen tekijöihinjaon vaikeuteen. ElGamal-salausjärjestelmä on vaihtoehtoinen julkisen avaimen salausjärjestelmä. Siinä turvallisuuden lähtökohtana on diskreetit logaritmit modulo suuri alkuluku, joita on vaikea löytää. Diskreetti logaritmi kokonaisluvusta a on eksponentti x kongruenssista

$$r^x \equiv a \pmod{p},$$

jos p on alkuluku ja luku r on primitiivinen juuri modulo p.

ElGamal-salausjärjestelmässä (Vrt. [5] s. 363.) jokainen käyttäjä valitsee alkuluvun p, primitiivisen juuren r modulo p ja sellaisen kokonaisluvun a, että $0 \leq a \leq p-1$. Nyt luku a on salainen avain, jota ei paljasteta muille. Julkaistava avain on (p, r, b), jossa b on sellainen kokonaisluku, että

$$b \equiv r^a \pmod{p},\ 0 \leq a \leq p-1.$$

Seuraavassa esimerkissä havainnollistetaan, kuinka ElGamal-salausjärjestelmässä valitaan avaimet.

Esimerkki 5.4 Valitaan ensin alkuluku p. Olkoon $p = 97$. Seuraavaksi valitaan primitiivinen juuri r modulo p. Olkoon $r = 2$, joka on primitiivinen juuri modulo p, sillä

$$\mathrm{ord}_{97}2 = \varphi(97).$$

Nyt valitaan sellainen kokonaisluku a, että $0 \leq a \leq 96$. Olkoon $a = 12$. Koska

$$b \equiv 2^{12} \equiv 22 \pmod{97},$$

saadaan 22 luvuksi b. Näin ollen on saatu muodostettua julkaistava avain $(p, r, b) = (97, 2, 22)$ ja salainen avain $a = 12$.

Aivan kuten RSA-salausjärjestelmässä myös ElGamal-järjestelmässä joudutaan käyttämään vähintään 200-numeroisia alkulukuja. Selvyyden vuoksi tässä tutkielmassa käytetään kuitenkin huomattavasti pienempiä lukuja.

Kuten RSA-salausjärjestelmässä myös ElGamal-järjestelmässä viestit muutetaan ensin numeeriseen muotoon. Turvallisuuden parantamiseksi viesti jaetaan usein lohkoihin, joissa on parillinen määrä lukuja. Viestin salaamiseksi julkisilla avaimilla (p, r, b) valitaan ensin jokin kokonaisluku $1 \leq k \leq p-2$. Jokaiselle salattavalle luvulle tai lohkolle l muodostetaan luvut y ja d siten, että

$$y \equiv r^k \pmod{p},\ \text{jossa } 0 \leq y \leq p-1$$

ja

$$d \equiv l \cdot b^k \pmod{p},\ \text{jossa } 0 \leq d \leq p-1.$$

Salattavaa viestin lohkoa l vastaava salattu viesti on nyt järjestetty pari (y, d). Selkokielisen viestin lohko l on nyt salattu kertomalla se luvulla b^k, jolloin saadaan luku d. Tämä lähetetään yhdessä luvun y kanssa vastaanottajalle. Tällöin vain lukujen (p, r, b) julkaisija, jolla on siis käytössään luku

a, voi laskea luvut b^k ja y ja näin ollen purkaa salatun viestin. Kun viesti salataan ElGamal-järjestelmällä, salatusta viestistä tulee kaksi kertaa pidempi kuin alkuperäisestä viestistä.

Kuten todettua, ElGamal-järjestelmällä salattu viesti voidaan purkaa vain salaisella avaimella a. Todettakoon, että $\overline{y^a}$ saadaan laskemalla kongruenssi $y^{p-1-a} \pmod{p}$. Purkaminen aloitetaan laskemalla $\overline{y^a}$. Nyt pari $C = (y, d)$ puretaan laskemalla

$$D(C) = (\overline{y^a})^d.$$

Toisin sanoen

$$\begin{aligned} D(C) &\equiv \overline{y^a} \cdot d \pmod{p} \\ &\equiv \overline{r^{ka}} \cdot lb^k \pmod{p} \\ &\equiv (\overline{r^a})^k lb^k \pmod{p} \\ &\equiv \overline{b^k} lb^k \pmod{p} \\ &\equiv \overline{b^k} b^k l \pmod{p} \\ &\equiv l \pmod{p}. \end{aligned}$$

Näin on saatu viesti purettua.

Esimerkki 5.5 Olkoot A ja B ElGamal-salausjärjestelmän käyttäjät. B haluaa lähettää viestin

ELGAMAL

A:lle. Samoin kuin esimerkissä 5.1 B muuttaa viestin numeeriseen muotoon

05 12 07 01 13 01 12

ja lähettää sen yhden kirjaimen lohkoissa A:lle. Olkoot A:n käyttämät avaimet esimerkin 5.4 mukaisia, eli

$$(p, r, b) = (97, 2, 22) \text{ ja } a = 12.$$

Nyt B valitsee sellaisen luvun k, että $1 \leq k \leq 95$. Jokaiselle viestin lohkolle valitaan yleensä eri k turvallisuuden parantamiseksi, mutta tässä esimerkissä riittää, että valitaaan vain yksi, sillä tässä käydään läpi vain yksi lohko, esimerkiksi lohko M = 13. Olkoon $k = 19$. Salataan ensin lohko M siten, että

$$d \equiv 13 \cdot 22^{19} \equiv 5 \pmod{97}$$

ja muodostetaan luku y siten, että

$$y \equiv 2^{19} \equiv 3 \pmod{97}.$$

Nyt B on saanut salattua lohkon K = 11 ja voi lähettää A:lle järjestetyn parin $(y, d) = (3, 5)$.

A voi nyt purkaa viestin laskemalla

$$D((y, d)) \equiv \overline{y^a} \cdot d \pmod{p}.$$

Toisin sanoen

$$\begin{aligned} D((3,5)) &\equiv \overline{5^{12}} \cdot 3 \pmod{97} \\ &\equiv \overline{64} \cdot 3 \pmod{97} \\ &\equiv 69 \cdot 3 \pmod{97} \\ &\equiv 13 \pmod{97} \end{aligned}$$

Nyt viestin lohko on purettu luvuksi 13.

Myös ElGamal-salausjärjestelmällä voidaan luoda digitaalisia allekirjoituksia (Vrt. [5] s. 365). Olkoot (p, r, b) käyttäjän julkaisemat avaimet ja olkoon a salainen avain siten, että $b \equiv r^a \pmod{p}$. Muodostetaan nyt allekirjoitus viestille l. Valitaan nyt sellainen kokonaisluku k, että $(k, p-1) = 1$. Muodostetaan nyt y ja s siten, että

$$y \equiv r^k \pmod{p},\ 0 \leq y \leq p-1$$

ja

$$s \equiv (l - ay)\overline{k} \pmod{p-1},\ 0 \leq s \leq p-2.$$

Nyt allekirjoitus on pari (y, s), joka riippuu luvusta k ja voidaan purkaa vain luvulla a.

Jotta allekirjoitus voidaan purkaa ja jotta se voitaisiin todeta pitäväksi, lasketaan

$$V_1 \equiv y^s b^y \pmod{p},\ 0 \leq V_1 \leq p-1$$

ja

$$V_2 \equiv r^l \pmod{p},\ 0 \leq V_2 \leq p-1.$$

Jos allekirjoitus on aito, niin $V_1 = V_2$. Toisin sanoen

$$\begin{aligned} V_1 &\equiv y^s b^y \pmod{p} \\ &\equiv y^{(l-ay)\overline{k}} b^y \pmod{p} \\ &\equiv (y^{\overline{k}})^{l-ay} b^y \pmod{p} \\ &\equiv r^{(l-ay)} b^y \pmod{p} \\ &\equiv r^l \overline{r^{ay}} b^y \pmod{p} \\ &\equiv r^l \overline{b^y} b^y \pmod{p} \\ &\equiv r^l \pmod{p} \\ &\equiv V_2. \end{aligned}$$

Esimerkki 5.6 Olkoot avaimet (p, r, b) ja a kuten esimerkissä 5.5. Toisin sanoen

$$(p, r, b) = (97, 2, 22) \text{ ja } a = 12.$$

Allekirjoitetaan nyt viesti $l = 13$. Valitaan ensin sellainen kokonaisluku k, että $1 \leq k \leq 96$. Olkoon $k = 7$, jolloin $\overline{7} = 14 \pmod{97}$. Allekirjoitus saadaan nyt muodostamalla luvut

$$y \equiv 2^7 \equiv 31 \pmod{97}$$

ja

$$s \equiv (13 - 12 \cdot 31) \cdot 14 \equiv 18 \pmod{97}.$$

Siis allekirjoitus on nyt pari $(31, 18)$. Nyt voidaan varmistua viestin autenttisuudesta, sillä

$$31^{18} \cdot 22^{31} \equiv 44 \pmod{97}$$

ja

$$2^{13} \equiv 44 \pmod{97}.$$

Viitteet

[1] Paul Erdös, János Surányi. *Topics in the Theory of Numbers*. Springer-Verlag, New York, 2003.

[2] Neal Koblitz. *A Course in Number Theory and Cryptography*. Springer-Verlag, New York, 1987.

[3] Trygve Nagell. *Number Theory*. Chelsea Publishing Company, New York, 1981.

[4] Melvyn B. Nathanson. *Elementary Methods in Number Theory*. Springer-Verlag, New York, 2000.

[5] Kenneth H. Rosen. *Elementary Number Theory and Its Applications*. Addison Wesley Longman, United States, 2000.

[6] Anuj Seth. *Anuj Seth's Home Page*. 2002. http://www.anujseth.com/

[7] D. W. Sharpe. *Topics in Number Theory, lecture notes and handouts*. University of Sheffield, 2000.

[8] John Stillwell. *Elements of Number Theory*. Springer-Verlag, New York, 2003.

[9] James J. Tattersall. *Elementary Number Theory in Nine Chapters*. Cambridge University Press, Cambridge, 1999.

[10] Eric W. Weisstein. *Carmichael Number*. From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com /CarmichaelNumber.html

[11] V. V. Yaschenko. *Cryptography: An Introduction*. American Mathematical Society, 2002.