Alkulukutestejä

Vieno Aho

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Syyskuu 2022

Tiivistelmä: Vieno Aho, *Alkulukutestejä* (engl. *Primality testing*), matematiikan pro gradu -tutkielma, 49 s., Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, syyskuu 2022.

Tämän tutkielman aiheena on alkulukutestit, jotka ovat sellaisia menetelmiä ja algoritmeja, joiden avulla voidaan tutkia, onko jokin luku alkuluku vai alkulukujen tulo. Tutkielman alussa käydään läpi joitakin yksinkertaisia määritelmiä ja aputuloksia jaollisuuteen liittyen sekä Eratostheneen seula, jonka avulla voidaan etsiä pienempiä alkulukuja. Toisessa luvussa käydään läpi joitakin kongruenssiin liittyviä tuloksia, joita tarvitaan myöhemminkin tutkielmassa. Toisessa luvussa osoitetaan myös Fermat'n pieni lause ja Wilsonin lause, joiden avulla voidaan tutkia hieman suurempienkin lukujen jaollisuutta.

Tutkielman ensimmäinen päätulos on probabilistinen Solovay-Strassenin alkulukutesti. Se antaa todennäköisen vastauksen, onko tutkittava luku alkuluku. Tätä testiä varten kolmannen luvun alussa osoitetaan erilaisia tuloksia sekä lukuteorian että myös algebran osa-alueilta. Lisäksi luvussa tutustutaan erilaisten pseudoalkulujen käsitteisiin ja osoitetaan niihin liittyviä aputuloksia, ennen kuin voidaan varsinaisesti käsitellä Solovay-Strassenin alkulukutestiä.

Toinen päätulos on deterministinen Miller-Rabinin alkulukutesti. Se antaa varman vastauksen, onko tutkittava luku alkuluku. Tätä testiä varten on neljännen luvun alussa jälleen aputuloksia, joita tarvitaan Miller-Rabinin alkulukutestin käsittelyyn. Tutkielman viidennessä luvussa esitellään vielä alkulukutestien sovelluksena RSA-salausmenetelmä, johon alkulukutestejä voidaan hyödyntää.

Sisällys

Johdanto

Tämän tutkielman aihe on alkulukutestit. Alkulukutesteillä tarkoitetaan sellaisia algoritmeja ja menetelmiä, joiden avulla voidaan selvittää, onko jokin luku alkuluku. Niitä tarvitaan tieto- ja viestintätekniikassa, sillä erityisesti suurilla alkuluvuilla on tärkeä rooli salakirjoitusmenetelmien toiminnassa. Alkulukutestejä on olemassa useita erilaisia ja ne voidaan jakaa karkeasti deterministisiin ja probabilistisiin testeihin. Deterministisiä testejä ovat sellaiset, joiden avulla voidaan sanoa varmasti, onko kyseessä alkuluku vai yhdistetty luku. Tällaisia testejä ovat Miller-Rabinin alkulukutesti sekä Wilsonin lauseeseen perustuva alkulukutesti. Probabilistisen testin avulla voidaan puolestaan selvittää onko kyseinen luku todennäköisesti alkuluku. Se ei siis anna varmaa tietoa tutkittavan luvun jaollisuudesta, mutta on determinististä testiä nopeampi ja siten usein käytännöllisempi työkalu. Solovay-Strassenin alkulukutesti on probabilistinen testi, mutta myös Miller-Rabinin alkulukutestistä esitellään probabilistinen versio.

Neljässä ensimmäisessä luvussa esitellään kussakin jokin menetelmä, jolla voidaan tutkia, onko annettu luku alkuluku vai yhdistetty luku. Luvun alussa on aina kyseiseen alkulukutestiin vaadittavia aputuloksia, joita voidaan hyödyntää myös myöhemmin tutkielman edetessä. Ensimmäisen luvun alussa on esitietoja, joita tarvitaan läpi tutkielman. Luvun lopussa esitellään Eratostheneen seula, jota voidaan hyödyntää pienempien alkulukujen löytämisessä.

Toinen luku sisältää kongruenssin käsitteen sekä siihen liittyviä aputuloksia, joita hyödynnetään myös tutkielman myöhemmissä luvuissa. Luvun lopussa osoitetaan Fermat'n pieni lause sekä Wilsonin lause, joiden avulla voidaan tutkia myös suurten lukujen jaollisuutta. Testit ovat yksinkertaisia, mutta eivät ongelmattomia. Fermat'n testin toteuttavat luvut eivät ole välttämättä alkulukuja ja Wilsonin lauseen avulla puolestaan suurten lukujen tutkiminen on hyvin työlästä.

Kolmannen luvun alkupuolella on runsaasti käsitteitä ja aputuloksia, joita tarvitaan Solovay-Strassenin alkulukutestin olemassaoloon. Ensin määritellään jäännösluokkarenkaat ja Eulerin ϕ-funktio sekä osoitetaan niihin liittyviä tuloksia. Sitten sivutaan algebraa yksikköryhmien ja syklisten ryhmien osalta. Tämän jälkeen tutustutaan vielä erilaisiin pseudoalkulukuihin ja neliönjäännökseen. Luvun lopussa esitellään Solovay-Strassenin alkulukutesti. Tämä testi on tehokas työkalu ja antaa melko hyvän arvion siitä, onko tutkittava luku alkuluku.

Neljännessä luvussa keskitytään Miller-Rabinin alkulukutestiin. Ensin osoitetaan testiin tarvittavia aputuloksia muun muassa indeksiaritmetiikkaa hyödyntäen. Lopuksi esitellään Miller-Rabinin alkulukutestistä sekä deterministinen että myös probabilistinen versio. Lopuksi viidennessä luvussa esitellään RSA-salausmenetelmät, joihin alkulukutestejä hyödynnetään.

Tutkielman päälähde on Kenneth H. Rosenin *Elementary Number Theory And Its Applications* [**3**], jota on hyödynnetty tutkielman kaikissa luvuissa. Kolmessa ensimmäisessä luvussa on käytetty lähteenä myös Gareth A. Jonesin ja J. Mary Jonesin teosta *Elementary Number Theory* [**2**]. Benjamin Finen ja Gerhard Rosenbergerin *Number Theory An Introduction via the Distribution of Primes* [**1**] on lähteenä puolestaan kolmessa viimeisessä luvussa. Eero Ruosteenojan *Lukuteoria 1* -kurssin luentomuistiinpanoja [**4**] on käytetty apuna joidenkin suomenkielisten käsitteiden ja tulosten muotoiluun, mutta sitä ei ole käytetty varsinaisten tulosten lähteenä. Lähdeviittaukset on merkitty tarkemmin jokaisen luvun alkuun. Tuloksia ja määritelmiä havainnollistavat esimerkit olen keksinyt itse, ellei toisin erikseen mainita.

LUKU 1

Eratostheneen seula

Alkuluvut kuuluvat kokonaislukujen $\mathbb{Z}$ ja luonnollisten lukujen $\mathbb{N}$ joukkoihin, sekä niiden osajoukkoihin. Tutkielmassani luonnolliset luvut on määritelty siten, että luku 0 ei kuulu luonnollisten lukujen joukkoon.

Pienistä luvuista on melko helppo nähdä, onko kyseessä alkuluku. Tällöin ei oikeastaan edes tarvita alkulukutestejä. Hyvin suurille luvuille puolestaan jaollisuuden tutkiminen on todella hidasta, jolloin alkulukutestit ovat käytännöllisiä apuvälineitä lukujen tutkimiseen.

Tässä luvussa keskitytään jaollisuuteen liittyviin peruskäsitteisiin ja laskusääntöihin. Näitä käsitteitä ja tuloksia tarvitaan pohjatietoina tutkielman myöhemmissä tuloksissa. Lisäksi luvun lopussa esitellään Eratostheneen seula, joka on yksi työkalu erityisesti pienten alkulukujen etsimiseen. Tämän luvun lähteitä ovat [**3**] ja [**2**].

1.1. Jaollisuus

Määritellään ensin kokonaislukujen jaollisuuden ja tekijän käsitteet, joihin koko alkulukuteoria käytännössä pohjautuu.

MÄÄRITELMÄ 1.1. Olkoon $a, b \in \mathbb{Z}$. Luku a jakaa luvun b, jos $b = k \cdot a$ jollakin $k \in \mathbb{Z}$. Tällöin merkitään $a|b$ ja pätee myös, että b on jaollinen luvulla a. Vastaavasti voidaan todeta, että a on luvun b tekijä ja b on luvun a monikerta.

Jos luku b ei ole jaollinen luvulla a, voidaan käyttää merkintää $a \nmid b$.

Määritelmästä voidaan huomata, että myös luku k on luvun b tekijä, sillä kertolasku on vaihdannainen ja a on kokonaisluku. Osoitetaan sitten lemma, joka liittyy tekijöiden laskusääntöihin. Nämä tulokset seuraavat hyvin suoraviivaisesti edellisestä määritelmästä.

LEMMA 1.2. *Olkoon $a, b, c, n, m \in \mathbb{Z}$.*
1) Jos $a|b$ ja $b|c$, niin $a|c$.
2) Jos $c|a$ ja $c|b$, niin $c|(na + mb)$.

TODISTUS. 1) Koska $a|b$ ja $b|c$, niin on olemassa $i, j \in \mathbb{Z}$ siten, että $b = ai$ ja $c = bj$, jolloin $c = bj = aij = a(ij)$. Näin ollen $a|c$.

2) Koska $c|a$ ja $c|b$, niin on olemassa kokonaisluvut $d, e \in \mathbb{Z}$ siten, että $a = cd$ ja $b = ce$. Tällöin $na + mb = ncd + mce = c(nd + me)$. Näin ollen $c|(na + mb)$. □

Määritellään seuraavaksi suurimman yhteisen tekijän käsite, joka on yksi tärkeimmistä peruskäsitteistä läpi tutkielman. Suurimman yhteisen tekijän olemassaoloa ei erikseen todisteta tässä tutkielmassa ja siksi lukujen suurin yhteinen tekijä annetaan määritelmänä. Lähteestä [**4**] löytyy kyseinen tulos yksityiskohtaisesti todistettuna aputuloksineen.

MÄÄRITELMÄ 1.3. Olkoon $a, b \in \mathbb{Z}$ siten, että $a \neq 0$ tai $b \neq 0$. Suurin lukujen a ja b yhteinen tekijä on suurin kokonaisluku $k \in \mathbb{N}$, jolle pätee $k|a$ ja $k|b$. Tällöin merkitään $\text{syt}(a, b) = k$.

Osoitetaan sitten lemma suurimman yhteisen tekijän laskusääntöihin liittyen. Nämä tulokset seuraavat suoraviivaisesti aikaisemmista määritelmistä. Havainnollistetaan tuloksia esimerkin avulla.

LEMMA 1.4. *Olkoon $a, b, c \in \mathbb{Z}$ siten, että $\text{syt}(a, b) = d$. Tällöin*
1) $\text{syt}(\frac{a}{d}, \frac{b}{d}) = 1$ *ja*
2) $\text{syt}(a + cb, b) = \text{syt}(a, b)$.

TODISTUS. 1) Osoitetaan, että luvuilla $\frac{a}{d} \in \mathbb{Z}$ ja $\frac{b}{d} \in \mathbb{Z}$ ei ole muita yhteisiä positiivisia tekijöitä kuin 1. Olkoon $e \in \mathbb{N}$ siten, että $e|\frac{a}{d}$ ja $e|\frac{b}{d}$. Tällöin on olemassa $i, j \in \mathbb{Z}$ siten, että $\frac{a}{d} = ei$ ja $\frac{b}{d} = ej$, joten $a = dei$ ja $b = dej$. Siis luku de on lukujen a ja b tekijä. Koska $\text{syt}(a, b) = d$, täytyy olla $e = 1$. Näin ollen $\text{syt}(\frac{a}{d}, \frac{b}{d}) = 1$.

2) Osoitetaan, että lukujen a ja b yhteiset tekijät ovat täsmälleen samat kuin lukujen $a + cb$ ja b yhteiset tekijät. Olkoon $e \in \mathbb{Z}$ lukujen a ja b yhteinen tekijä. Lemman 1.2 2-kohdan nojalla $e|(a + cb)$, joten luku e on myös lukujen $a + cb$ ja b yhteinen tekijä. Olkoon sitten $f \in \mathbb{Z}$ lukujen $a + cb$ ja b yhteinen tekijä. Lemman 1.2 2-kohdan nojalla f jakaa luvun $(a + cb) - cb = a$, joten luku f on myös lukujen a ja b yhteinen tekijä. Näin ollen $\text{syt}(a + cb, b) = \text{syt}(a, b)$. □

ESIMERKKI 1.5. Koska $\text{syt}(18, 45) = 9$, niin

$$\text{syt}(\frac{18}{9}, \frac{45}{9}) = \text{syt}(2, 5) = 1$$

ja

$$\text{syt}(18 + 2 \cdot 45, 45) = \text{syt}(108, 45) = 9 = \text{syt}(18, 45).$$

Osoitetaan sitten Bezout'n lemmana tunnettu tulos, jonka mukaan lukujen suurimman yhteisen tekijän voi ilmaista näiden lukujen lineaarikombinaationa. Lemman todistuksessa mainittu Eukleideen algoritmi oletetaan esitietoina tunnetuksi, mutta tarvittaessa se löytyy esimerkiksi lähteistä [**2**] ja [**4**].

LEMMA 1.6. *Olkoon $a, b \in \mathbb{Z}$, siten että $a \neq 0$ tai $b \neq 0$. Tällöin on olemassa luvut $n, m \in \mathbb{Z}$ siten, että* $\text{syt}(a, b) = na + mb$.

TODISTUS. Tutkitaan ensin tapausta, kun $a = 0$. Tällöin

$$\text{syt}(a, b) = \text{syt}(0, b) = \text{syt}(0, |b|) = |b|$$

ja $b \cdot (\pm 1) + 0 \cdot 0 = |b|$, missä luvun 1 etumerkki riippuu luvusta b. Jos $b > 0$, voidaan valita etumerkiksi $+$, jolloin $b \cdot 1 = b = |b|$, ja jos $b < 0$, valitaan -1, jolloin $b \cdot (-1) = |b|$.

Vastaavasti, jos $b = 0$, niin $a \cdot (\pm 1) + 0 \cdot 0 = |a|$, missä luvun 1 etumerkki riippuu luvusta a. Jos $a > 0$, niin $a \cdot 1 = a = |a|$, ja jos $a < 0$, niin $a \cdot (-1) = |a|$.

Tutkitaan sitten tapaus, jossa $a \neq 0$ ja $b \neq 0$. Tällöin $|a| > 0$ ja $|b| > 0$. Tällöin Eukleideen algoritmilla löydetään luvut $n, m \in \mathbb{Z}$ siten, että

$$n|a| + m|b| = \text{syt}(|a|, |b|) = \text{syt}(a, b).$$

Koska $a = \pm|a|$ ja $b = \pm|b|$, niin saadaan $(\pm n)a + (\pm m)b = \text{syt}(a, b)$, kun etumerkki valitaan oikein. Näin ollen väite pätee kaikilla $a, b \in \mathbb{Z}$, kun $a \neq 0$ tai $b \neq 0$. □

Osoitetaan vielä edellistä Bezout'n lemmaa hyödyntävä lemma jaollisuuteen liittyen.

LEMMA 1.7. *Olkoon* $n, m, k \in \mathbb{N}$ *siten, että* $\text{syt}(n, m) = 1$. *Tällöin*
1) $n|k$, *jos* $n|mk$ *ja*
2) $nm|k$, *jos* $n|k$ *ja* $m|k$.

TODISTUS. 1) Koska $\text{syt}(n, m) = 1$, niin Lemman 1.6 nojalla on olemassa $a, b \in \mathbb{Z}$ siten, että $na + mb = 1$. Kun yhtälön molemmat puolet kerrotaan luvulla k, saadaan $nka + mkb = k$. Lemman 1.2 2-kohdan nojalla $n|(nka + mkb)$, koska kyseessä on lineaarikombinaatio luvuista n ja mk, jotka molemmat ovat jaollisia luvulla n. Näin ollen $n|k$.

2)Olkoot $k = an$ ja $k = bm$, jollakin $a, b \in \mathbb{Z}$. Lemman 1.6 nojalla on olemassa $x, y \in \mathbb{Z}$ siten että $nx + my = 1$. Tällöin

$$k = k(nx + my) = knx + kmy = bmnx + anmy = nm(bx + ay).$$

Koska $bx + ay \in \mathbb{Z}$, niin $nm|k$. □

Todistetaan tulos, jonka seurauksena saadaan yhteys suurimman yhteisen tekijän ja lineaarisen kahden muuttujan yhtälön kokonaislukuratkaisujen löytymisen välille.

LAUSE 1.8. *Olkoon* $a, b \in \mathbb{Z}$ *siten, että* $a \neq 0$ *tai* $b \neq 0$. *Tällöin*

$$\{ax + by : x, y \in \mathbb{Z}\} = \{k \cdot \text{syt}(a, b) : k \in \mathbb{Z}\}.$$

TODISTUS. Merkitään $A := \{ax + by : x, y \in \mathbb{Z}\}$ ja $B := \{k \cdot \text{syt}(a, b) : k \in \mathbb{Z}\}$. Osoitetaan ensin, että $A \subset B$. Olkoon $c \in A$. Tällöin $c = ax_0 + by_0$ jollakin $x_0, y_0 \in \mathbb{Z}$. Koska $\text{syt}(a, b)|a$ ja $\text{syt}(a, b)|b$, on olemassa luvut $z, w \in \mathbb{Z}$ siten, että $a = z \cdot \text{syt}(a, b)$ ja $b = w \cdot \text{syt}(a, b)$. Tällöin

$$c = ax_0 + by_0 = (zx_0 + wy_0)\,\text{syt}(a, b),$$

missä $zx_0 + wy_0 \in \mathbb{Z}$, joten $c \in B$. Siis $A \subset B$.

Osoitetaan sitten, että $B \subset A$. Lemman 1.6 nojalla on olemassa luvut $m, n \in \mathbb{Z}$ siten, että $\text{syt}(a, b) = na + mb$. Tällöin, jos $k \in \mathbb{Z}$, niin

$$k \cdot \text{syt}(a, b) = k(na + mb) = akn + bkm,$$

missä $kn, km \in \mathbb{Z}$. Siis $B \subset A$. Näin ollen $A = B$. □

SEURAUS 1.9. *Olkoot* $a, b, c \in \mathbb{Z}$ *annettuja lukuja siten, että* $a \neq 0$ *tai* $b \neq 0$. *Tällöin yhtälöllä* $ax + by = c$ *on kokonaislukuratkaisuja, jos ja vain jos* $\text{syt}(a, b)|c$.

Määritellään Diofantoksen yhtälö sekä todistetaan tulos, joka kertoo, miten yhtälön kaikki ratkaisut löydetään, kun jokin ratkaisuista tiedetään.

MÄÄRITELMÄ 1.10. Vähintään kahden muuttujan kokonaislukukertoimista polynomiyhtälöä, jolle etsitään kokonaislukujaratkaisuja, kutsutaan Diofantoksen yhtälöksi. Yhtälöä

$$ax + by = c,$$

missä $a, b, c \in \mathbb{Z}$ voidaan kutsua myös tarkemmin lineaariseksi kahden muuttujan Diofantoksen yhtälöksi. Siis Diofantoksen yhtälöllä on olemassa ratkaisu, jos ja vain jos luvut $x, y \in \mathbb{Z}$ toteuttavat yhtälön.

LAUSE 1.11. *Olkoot luvut $a, b, c \in \mathbb{Z}$ siten, että $a \neq 0$ tai $b \neq 0$. Olkoon Diofantoksen yhtälöllä*

$$ax + by = c$$

eräs kokonaislukuratkaisu x_0, y_0. Tällöin kokonaislukupari x', y' on Diofantoksen yhtälön ratkaisu, jos ja vain jos

$$\begin{cases} x' = x_0 + k\dfrac{b}{d} \\ y' = y_0 - k\dfrac{a}{d}, \end{cases}$$

missä $d = \mathrm{syt}(a, b)$ ja $k \in \mathbb{Z}$.

TODISTUS. Oletetaan ensin, että kokonaislukupari x', y' toteuttaa yhtälöparin jollakin $k \in \mathbb{Z}$. Koska lukupari x_0, y_0 on Diofantoksen yhtälön eräs kokonaislukuratkaisu, saadaan

$$\begin{aligned} ax' + by' &= a\left(x_0 + k\frac{b}{d}\right) + b\left(y_0 - k\frac{a}{d}\right) \\ &= ax_0 + by_0 + \left(k\frac{ab}{d} - k\frac{ba}{d}\right) \\ &= ax_0 + by_0 = c. \end{aligned}$$

Näin ollen, jos lukupari x', y' toteuttaa yhtälöparin, on se myös eräs Diofantoksen yhtälön ratkaisu.

Oletetaan sitten, että kokonaislukupari x', y' on eräs Diofantoksen yhtälön ratkaisu. Tällöin

$$a(x_0 - x') + b(y_0 - y') = ax_0 + by_0 - (ax' + by') = c - c = 0,$$

sillä parit x_0, y_0 ja x', y' ovat kokonaislukuratkaisuja. Edellisestä yhtälöstä saadaan

$$\frac{b}{d}(y_0 - y') = -\frac{a}{d}(x_0 - x').$$

Siis $\frac{b}{d} | -\frac{a}{d}(x_0 - x')$. Tällöin Lemmojen 1.4 ja 1.7 nojalla pätee $\frac{b}{d} | -(x_0 - x')$. Näin ollen on olemassa sellainen $k \in \mathbb{Z}$, jolle pätee $-(x_0 - x') = k\frac{b}{d}$, joten

$$x' = x_0 + k\frac{b}{d}.$$

Sijoittamalla saatu x' yhtälöön $\frac{b}{d}(y_0 - y') = -\frac{a}{d}(x_0 - x')$, saadaan edelleen

$$y' = y_0 - k\frac{a}{d}.$$

□

1.2. Alkutekijät

Määritellään alkuluvut, joiden löytäminen erilaisten testien avulla on koko tutkielman aihe ja päätavoite. Näin ollen määritelmä ja siihen liittyvät tulokset ovat merkittävässä roolissa läpi tutkielman. Havainnollistetaan määritelmää vielä yksinkertaisella esimerkillä.

MÄÄRITELMÄ 1.12. Olkoon $q \geq 2$ luonnollinen luku. Jos sen ainoat positiiviset tekijät ovat luvut 1 ja q itse, niin kyseessä on alkuluku. Jos positiivisia tekijöitä on muitakin, niin silloin kyseessä on yhdistetty luku.

Esimerkki 1.13. Luku 11 on alkuluku, sillä sen ainoat tekijät ovat 1 ja 11 itse. Luku 21 on puolestaan yhdistetty luku, sillä sen tekijöitä ovat luvut $1, 3, 7$ ja 21.

Huomautus 1.14. Luku 1 ei ole alkulukujen määritelmän nojalla alkuluku, mutta se ei ole myöskään yhdistetty luku.

Osoitetaan sitten alkulukuihin liittyviä jaollisuussääntöjä sisältävä tulos.

Lemma 1.15. *Olkoon q alkuluku.*
1) Olkoon $a \in \mathbb{Z}$. Jos $q \nmid a$, niin $\mathrm{syt}(a, q) = 1$.
2) Jos $q|ab$, missä $a, b \in \mathbb{Z}$, niin $q|a$ tai $q|b$.
3) Jos $q|a_1 \cdots a_n$, missä $a_i \in \mathbb{Z}$ kaikilla $i \in \{1, \ldots, n\}$, niin $q|a_i$ jollakin $i \in \{1, \ldots, n\}$.

Todistus. 1) Koska $\mathrm{syt}(a, q) > 0$ ja $\mathrm{syt}(a, q)|q$, niin alkulukujen määritelmän nojalla $\mathrm{syt}(a, q) = 1$ tai $\mathrm{syt}(a, q) = q$. Jos $\mathrm{syt}(a, q) = q$, niin $q|a$, koska $\mathrm{syt}(a, q)|a$. Siis täytyy olla $\mathrm{syt}(a, q) = 1$.

2) Jos $q \nmid a$, niin 1-kohdan nojalla $\mathrm{syt}(a, q) = 1$. Tällöin Lemman 1.6 nojalla $1 = na + mq$, missä $n, m \in \mathbb{Z}$, joten $b = nab + mqb$. Koska $q|ab$, niin $q|nab$. Koska selvästi $q|mqb$, niin Lemman 1.2 2-kohdan nojalla $q|b$. Vastaavasti, jos $q \nmid b$, niin $q|a$.

3) Osoitetaan väite induktiolla.

Alkuaskel: $n = 1$ Jos $q|a_1$, niin väite on selvästi tosi.

Induktio-oletus: $n = k$ Jos $q|a_1 \cdots a_k$, niin $q|a_i$ jollakin $i \in \{1, \ldots, k\}$.

Induktioaskel: $n = k + 1$ Merkitään $a := a_1 \cdots a_k$ ja $b := a_{k+1}$. Jos $q|a_1 \cdots a_{k+1}$, niin $q|ab$, jolloin 2-kohdan nojalla $q|a$ tai $q|b$. Jos $q|b = a_{k+1}$, niin väite pätee. Jos taas $q|a = a_1 \cdots a_k$, niin induktio-oletuksen nojalla $q|a_i$ jollakin $i \in \{1, \ldots, k\}$. □

Osoitetaan seuraavaksi Aritmetiikan peruslause, johon Eratostheneen seulakin perustuu. Havainnollistetaan tulosta esimerkin avulla.

Lause 1.16. *Olkoon $n \geq 2$ luonnollinen luku. Tällöin se voidaan esittää alkulukujen tulona, joka on tekijöiden järjestystä lukuunottamatta yksikäsitteinen. Tätä tuloa kutsutaan alkutekijäesitykseksi.*

Todistus. Todistetaan ensin alkutekijäesityksen olemassaolo induktiolla.

Alkuaskel: $n = 2$ Luku $2 = 2^1$ on alkuluku, joten väite pätee.

Induktio-oletus: $n = k$ Luvut $2, 3, \ldots, k$ ovat alkulukujen tuloja.

Induktioaskel: $n = k + 1$ Jos luku $k + 1 = (k + 1)^1$ on alkuluku, niin väite pätee. Oletetaan sitten, että $k+1$ on yhdistetty luku. Tällöin se voidaan kirjoittaa muodossa $k + 1 = ab$, missä $2 \leq a, b \leq k$. Koska induktio-oletuksen nojalla luvuilla a ja b on alkutekijäesitys, voidaan luku $k + 1$ esittää näiden alkutekijäesitysten tulona.

Osoitetaan sitten yksikäsitteisyys. Olkoon luvun n alkutekijäesitykset

$$n = p_1^{h_1} \cdots p_r^{h_r} = q_1^{k_1} \cdots q_m^{k_m},$$

missä $p_1 \ldots p_r$ ja $q_1 \ldots q_m$ ovat kaksi erilaista alkulukujen joukkoa ja kaikki eksponentit $h_i \in \mathbb{N}$ ja $k_j \in \mathbb{N}$. Koska $p_1|n$, niin $p_1|q_1^{k_1} \cdots q_m^{k_m}$, jolloin Lemman 1.15 3-kohdan nojalla $p_1|q_j$ jollakin $j \in \{1, \ldots, m\}$. Uudelleenjärjestämällä alkutekijät toisesta esityksestä voidaan olettaa, että $j = 1$, jolloin $p_1|q_1$. Koska q_1 on alkuluku, saadaan $p_1 = q_1$, jolloin supistamalla alkuluku molemmista alkutekijäesityksistä, saadaan edelleen

$$\frac{n}{q_1} = p_1^{h_1 - 1} \cdots p_r^{h_r} = q_1^{k_1 - 1} \cdots q_m^{k_m}.$$

Jatkamalla vastaavasti etsien keskenään samat alkuluvut molemmista esityksistä ja supistamalla ne molemmista yhtälöistä, alkuluvut loppuvat ainakin toisesta alkutekijäesityksestä. Jos toisen alkutekijäesityksen alkuluvut loppuvat ensin, saadaan yhtälöstä alkulukujen p_i tai q_j tuloksi luku 1, mikä on mahdotonta, sillä $p_i, q_j > 1$. Siispä alkuluvut loppuvat alkutekijäesityksistä yhtä aikaa, joten vasemmalta puolelta on täytynyt supistaa h_i kertaa jokainen p_i ja oikealta yhtä monta (k_j) kertaa luku q_j. Näin ollen tarvittaessa tekijät uudelleenjärjestämällä saadaan $m = r$, jokainen $p_i = q_j$ ja jokainen $h_i = k_j$, mikä todistaa yksikäsitteisyyden. □

Esimerkki 1.17. Luku 22680 voidaan hajottaa alkutekijäesitykseksi ja saadaan

$$22680 = 2^3 \cdot 3^4 \cdot 5 \cdot 7 = 7 \cdot 3^4 \cdot 5 \cdot 2^3.$$

Osoitetaan vielä viimeinen Eratostheneen seulaan liittyvä lause. Tämän tuloksen avulla algoritmin käyttö tehostuu, kun algoritmia ei tarvitse toistaa ihan kaikille tutkittavaa lukua pienemmille alkuluvuille.

Lause 1.18. *Olkoon $n \geq 2$ luonnollinen luku. Tällöin luku n on yhdistetty luku, jos ja vain jos on olemassa sellainen alkuluku $q \leq \sqrt{n}$, joka on luvun n tekijä.*

Todistus. Olkoon n on yhdistetty luku, jolloin se voidaan kirjoittaa muotoon $n = ab$, siten, että $a, b \in \mathbb{N}$ ja $a \leq b < n$. Tällöin täytyy olla $a \leq \sqrt{n}$, sillä muuten $ab > \sqrt{n} \cdot \sqrt{n} = n$. Nyt Lauseen 1.16 nojalla luvulla a täytyy olla alkulukutekijä q, joka on Lemman 1.2 1-kohdan nojalla myös luvun n tekijä ja selvästi $q \leq \sqrt{n}$.

Olkoon alkuluku $q \leq \sqrt{n}$ luvun $n \in \mathbb{N}$ tekijä. Koska $q > 1$, niin määritelmän nojalla n on yhdistetty luku. □

Aikaisempien tulosten avulla saadaan algoritmi, jolla voidaan etsiä kaikki tutkittavaa lukua x pienemmät alkuluvut. Tätä algoritmia kutsutaan Eratostheneen seulaksi. Lauseen 1.18 nojalla, riittää käydä Eratostheneen seulasta läpi kaikki alkuluvut q, joille pätee $q \leq \sqrt{x}$. Havainnollistetaan tätä lopuksi esimerkin avulla.

Kaikki lukua $x > 0$ pienemmät alkuluvut löydettään seuraavalla algoritmilla:

1° Listataan kaikki luonnolliset luvut n, joille pätee $1 < n < x$.

2° Poistetaan luvun 2, eli ensimmäisen alkuluvun kaikki monikerrat, jotka ovat suurempia, kuin luku 2 itse.

3° Poistetaan luvun 3, eli toisen alkuluvun kaikki monikerrat, jotka ovat suurempia, kuin luku 3 itse.

4° Poistetaan luvun 5, eli kolmannen alkuluvun kaikki monikerrat, jotka ovat suurempia, kuin luku 5 itse.

5° Jatketaan poistamalla kaikkien seuraavienkin alkulukujen monikerrat, jotka ovat suurempia, kuin alkuluku itse.

Lopulta jäljellä olevat luvut ovat kaikki lukua x pienemmät alkuluvut.

Esimerkki 1.19. Taulukossa ympyröitynä lukua $x = 101$ pienemmät alkuluvut. Koska lukua $\sqrt{101}$ pienemmät alkuluvut ovat $2, 3, 5$ ja 7, riittää, kun poistaa kaikki näiden alkulukujen monikerrat. Tällöin jäljelle jää vain alkulukuja.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

LUKU 2

Fermat'n alkulukutesti

Tässä luvussa esitellään kaksi ensimmäistä suurillekin luvuille sopivaa alkulukutestiä. Ensimmäisessä alaluvussa määritellään kongruenssin ja jäännösluokkien käsitteet sekä niihin liittyviä tuloksia. Toinen alaluku puolestaan käsittelee Fermat'n pientä lausetta ja Wilsonin lausetta sekä niiden käyttämistä alkulukutestauksessa. Tämän luvun päälähde on [**3**]. Ensimmäisestä alaluvusta Kiinalainen jäännöslause 2.14 ja Lause 2.16 sekä toisesta alaluvusta Wilsonin lause 2.20 ovat kuitenkin lähteestä [**2**].

2.1. Kongruenssi

Määritellään aluksi kongruenssin käsite. Sekin on yksi peruskäsitteistä, joita tarvitaan jatkuvasti tutkielman edetessä. Havainnollistetaan määritelmää yksinkertaisen esimerkin avulla.

MÄÄRITELMÄ 2.1. Olkoot $a, b \in \mathbb{Z}$ ja $n \in \mathbb{N}$. Luku a on kongruentti luvun b kanssa modulo n, jos $n|(a-b)$. Tällöin merkitään

$$a \equiv b \mod (n).$$

Jos $n \nmid (a-b)$, niin merkitään $a \not\equiv b \mod (n)$.

ESIMERKKI 2.2. Luvuille 6 ja 21 pätee $21 \equiv 6 \mod (5)$, sillä $21 - 6 = 15 = 3 \cdot 5$.

Todistetaan kaksi lausetta ja seuraus, jotka perustuvat kongruenssin määritelmään sekä suurimpaan yhteiseen tekijään. Näiden tulosten avulla saadaan Fermat'n pieni lause todistettua. Havainnollistetaan molempia lauseita esimerkeillä.

LAUSE 2.3. *Olkoot $a, b, c \in \mathbb{Z}$ ja $n \in \mathbb{N}$ siten, että $a \equiv b \mod (n)$. Tällöin*
1) $a + c \equiv b + c \mod (n)$ ja
2) $ac \equiv bc \mod (n)$.

TODISTUS. 1) Koska $a \equiv b \mod (n)$, niin kongruenssin määritelmän nojalla $n|(a-b)$. Koska edelleen $a - b = a - b + c - c = (a + c) - (b + c)$, niin $a + c \equiv b + c \mod (n)$.
2) Huomataan, että $ac - bc = c(a - b)$. Koska $n|(a-b)$, niin $n|c(a-b)$. Näin ollen $ac \equiv bc \mod (n)$. □

ESIMERKKI 2.4. Koska $21 \equiv 6 \mod (5)$, niin $21 + 8 = 29 \equiv 4 \equiv 14 = 6 + 8 \mod (5)$ ja $21 \cdot 8 = 168 \equiv 3 \equiv 48 = 6 \cdot 8 \mod (5)$.

LAUSE 2.5. *Olkoot $a, b, c \in \mathbb{Z}$ ja $n \in \mathbb{N}$. Jos $\text{syt}(c, n) = d$ ja $ac \equiv bc \mod (n)$, niin $a \equiv b \mod (\frac{n}{d})$.*

TODISTUS. Koska $ac \equiv bc \mod (n)$, niin $n|(ac-bc) = c(a-b)$. Täten on olemassa luku $k \in \mathbb{Z}$ siten, että $c(a-b) = kn$. Kun jaetaan yhtälön molemmat puolet luvulla d, saadaan $\frac{c}{d}(a-b) = k(\frac{n}{d})$, missä $\frac{n}{d}, \frac{c}{d} \in \mathbb{Z}$. Koska Lemman 1.4 nojalla $\text{syt}(\frac{n}{d}, \frac{c}{d}) = 1$, niin saadaan edelleen $\frac{n}{d}|(a-b)$. Näin ollen $a \equiv b \mod (\frac{n}{d})$. □

ESIMERKKI 2.6. Koska $\text{syt}(4, 10) = 2$ ja $12 \equiv 32 \mod (10)$, niin $3 \equiv 8 \mod (5)$.

SEURAUS 2.7. *Olkoot $a, b, c \in \mathbb{Z}$ ja $n \in \mathbb{N}$. Jos $\text{syt}(c, n) = 1$ ja $ac \equiv bc \mod (n)$, niin $a \equiv b \mod (n)$.*

Osoitetaan sitten, että kongruenssi on ekvivalenssirelaatio kokonaislukujen joukossa, mikä seuraa suoraviivaisesti kongruessin määritelmästä. Tätä tulosta hyödynnetään kuitenkin vasta seuraavassa luvussa.

LAUSE 2.8. *Kongruenssi on ekvivalenssirelaatio kokonaislukujen joukossa. Olkoot luvut $n \in \mathbb{N}$ ja $a, b, c \in \mathbb{Z}$. Tällöin pätee*

1) $a \equiv a \mod (n)$,

2) $b \equiv a \mod (n)$, jos $a \equiv b \mod (n)$ ja

3) $a \equiv c \mod (n)$, jos $a \equiv b \mod (n)$ ja $b \equiv c \mod (n)$.

TODISTUS. 1) Koska $n|0$, niin $n|(a-a)$, joten väite pätee.

2) Koska $a - b = -(b-a)$, niin $n|(b-a)$ aina, kun $n|(a-b)$.

3) Jos $n|(a-b)$ ja $n|(b-c)$, niin $n|(a-c)$, sillä $a-c = a-b+b-c = (a-b)+(b-c)$. □

Määritellään kongruenssiluokat ja havainnollistetaan niitä yksinkertaisen esimerkin avulla. Tutkielman edetessä käytetään vaihtelevasti termejä kongruenssiluokka ja jäännösluokka. Nämä ovat kuitenkin toistensa synonyymejä, joten käytetystä termistä riippumatta määritelmä on sama.

MÄÄRITELMÄ 2.9. Olkoot $a \in \mathbb{Z}$ ja $n \in \mathbb{N}$. Luvun a kongruenssiluokka modulo n on joukko

$$[a]_n = \{b \in \mathbb{Z} : a \equiv b \mod (n)\}.$$

Notaatiosta voidaan jättää alaindeksi merkitsemättä, jos se oletetaan asiayhteydestä selväksi.

ESIMERKKI 2.10. Luvun 1 kongruenssiluokka modulo 2 on parittomien lukujen joukko

$$[1]_2 = \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \dots\}.$$

Todistetaan sitten lause, joka kertoo, kuinka monta ratkaisua lineaarisella kongruenssiyhtälöllä on. Lause antaa myös kaavan, miten kaikki ratkaisut löydetään, jos yksi ratkaisuista tiedetään. Havainnollistetaan tulosta jälleen esimerkin avulla.

LAUSE 2.11. *Olkoot $n \in \mathbb{N}$ ja $a, b \in \mathbb{Z}$. Merkitään $\text{syt}(a, n) = c$.*

1) Lineaarisella kongruenssiyhtälöllä $ax \equiv b \mod (n)$ ei ole kokonaislukuratkaisua, jos $c \nmid b$.

2) Jos $c|b$, lineaarisella kongruenssiyhtälöllä $ax \equiv b \mod (n)$ on c ratkaisua kongruenssiluokkina modulo n. Ratkaisut saadaan kaavalla $x \equiv x_0 + \frac{n}{c}i \mod (n)$, missä $i = 0, 1, \dots, c-1$ ja luku x_0 on eräs kongruenssiyhtälön ratkaisu.

TODISTUS. Etsitään sellainen luku $x \in \mathbb{Z}$, jolle pätee yhtälö $ax + ny = b$, jollakin $y \in \mathbb{Z}$.

1) Seurauksen 1.9 nojalla tällaista lukua $x \in \mathbb{Z}$ ei ole olemassa, jos $c \nmid b$.

2) Jos $c|b$, niin Lauseen 1.8 perusteella on olemassa sellaiset luvut $d_0, e_0 \in \mathbb{Z}$, joille pätee $ad_0 + ne_0 = c$, joten $a \cdot \frac{b}{c}d_0 + n \cdot \frac{b}{c}e_0 = b$. Koska lukujen a ja n kertoimet ovat kokonaislukuja, niin yhtälön $ax \equiv b \mod (n)$ eräs ratkaisu on $x_0 = \frac{b}{c}d_0$. Koska jakoyhtälön mukaan on olemassa luvut $p, i \in \mathbb{Z}$ siten, että $m = pc + i$ ja $0 \leq i \leq c-1$, niin Lauseen 1.11 Diofantoksen yhtälön ratkaisuista sekä jakoyhtälöstä seuraa

$$x = x_0 + m\frac{n}{c} = x_0 + (pc + i)\frac{n}{c} \equiv x_0 + i\frac{n}{c} \mod (n),$$

missä $i = 0, 1, \ldots, c-1$. □

Esimerkki 2.12. Kongruenssiyhtälöllä $4x \equiv 5 \mod (6)$ ei ole kokonaislukuratkaisuja, koska $\text{syt}(4, 6) = 2$ ja $2 \nmid 5$. Sen sijaan kongruenssiyhtälöllä $6x \equiv 42 \mod (9)$ on 3 kokonaislukuratkaisua kongruenssiluokkina modulo 9, koska $\text{syt}(6, 9) = 3$ ja $3|42$. Luku 1 on eräs kongruenssiyhtälön ratkaisuista, jolloin loput ratkaisut löydetään kaavalla $x = 1 + \frac{9}{3}i = 1 + 3i$, missä $i = 1, 2$. Kongruenssiyhtälön kaikki ratkaisut ovat siis kongruenssiluokat $[1]_9$, $[4]_9$ ja $[7]_9$.

Seuraus 2.13. *Olkoot $n \in \mathbb{N}$ ja $a \in \mathbb{Z}$ siten, että $\text{syt}(n, a) = 1$. Tällöin lineaarisella kongruenssilla $ax \equiv b \mod (n)$ on olemassa kongruenssiluokkana yksikäsitteinen ratkaisu kaikilla $b \in \mathbb{Z}$.*

Todistetaan Kiinalainen jäännöslause, joka on hyvin tärkeä aputulos tässä tutkielmassa. Tätä lausetta tarvitaan molempien tutkielman päätulosten todistamisessa. Havainnollistetaan tulosta vielä yksinkertaisen esimerkin avulla.

Lause 2.14. *Olkoot $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ ja $n_1, n_2, \ldots, n_k \in \mathbb{N}$, joille pätee $\text{syt}(n_i, n_j) = 1$ kaikilla $i, j \in \{1, \ldots, k\}$, kun $i \neq j$. Tällöin kongruenssiyhtälöryhmällä*

$$\begin{cases} x \equiv a_1 \mod (n_1) \\ x \equiv a_2 \mod (n_2) \\ \quad \vdots \\ x \equiv a_k \mod (n_k) \end{cases}$$

on ratkaisu, joka on yksikäsitteinen kongruenssiluokkana modulo $n_1 \cdot n_2 \cdots n_k$.

Todistus. Olkoot $n = n_1 \cdot n_2 \cdots n_k$ ja $b_i = \frac{n}{n_i}$, missä $i = 1, \ldots, k$. Koska $\text{syt}(n_i, n_j) = 1$ kaikilla $i, j \in \{1, \ldots, k\}$, kun $i \neq j$, niin $\text{syt}(b_i, n_i) = 1$ kaikilla $i \in \{1, \ldots, k\}$. Tällöin Seurauksen 2.13 nojalla yhtälöllä

$$b_i x \equiv 1 \mod (n_i)$$

on ratkaisu, joka on yksikäsitteinen kongruenssiluokkana modulo n_i. Merkitään tätä ratkaisua kongruenssiluokkana $[c_i]_{n_i}$. Osoitetaan sitten, että luku

$$x_0 = a_1 b_1 c_1 + a_2 b_2 c_2 + \cdots + a_k b_k c_k$$

on yhtälöryhmän ratkaisu. Jos $i \neq j$, niin $n_i | b_j$, joten $a_j b_j c_j \equiv 0 \mod (n_i)$. Siis $x_0 \equiv a_i b_i c_i \mod (n_i)$. Koska $b_i c_i \equiv 1 \mod (n_i)$, niin edelleen $x_0 \equiv a_i \mod (n_i)$. Näin ollen luku x_0 on kaikkien yhtälöryhmän kongruenssiyhtälöiden ratkaisu, joten kongruenssiluokka $[x_0]_n$ on yhtälöryhmän ratkaisu.

Osoitetaan seuraavaksi, että ratkaisu on yksikäsitteinen. Olkoon luku $x \in \mathbb{N}$ yhtälöryhmän ratkaisu, jolloin $x \equiv a_i \mod (n_i)$ ja $x_0 \equiv a_i \mod (n_i)$. Edelleen Lauseen 2.8 nojalla $x_0 \equiv x \mod (n_i)$, joten $n_i|(x - x_0)$ kaikilla $i \in \{1, \ldots, k\}$. Koska $\text{syt}(n_i, n_j) = 1$, niin Lemman 1.7 2-kohdan nojalla $n|(x - x_0)$. Siis $x \equiv x_0 \mod (n)$. Näin ollen ratkaisu $[x_0]_n$ on yksikäsitteinen. □

Esimerkki 2.15. Kongruenssiyhtälöryhmällä

$$\begin{cases} x \equiv 7 \mod (3) \\ x \equiv 2 \mod (4) \\ x \equiv 8 \mod (5) \end{cases}$$

on yksikäsitteinen ratkaisu kongruenssiluokkana modulo 60.

Tämä ratkaisu on kongruenssiluokka $[58]_{60}$.

Todistetaan vielä tulos, joka kertoo kokonaislukukertoimisen polynomin nollakohtien määrän sovellettuna kongruenssiluokille. Tätä tulosta tarvitaan Wilsonin lauseen 2.20 todistuksessa.

Lause 2.16. *Olkoot q alkuluku ja funktio $f(x) = a_k x^k + \cdots + a_1 x + a_0$ kokonaislukukertoiminen polynomi, missä $a_i \not\equiv 0 \mod (q)$ jollakin $i \in \{0, 1, \ldots, k\}$. Tällöin kongruenssiyhtälö $f(x) \equiv 0 \mod (q)$ pätee korkeintaan k kongruenssiluokalle $[x]_q$.*

Todistus. Osoitetaan väite induktiolla.

Alkuaskel: Jos $k = 0$, niin $f(x) = a_0$ siten, että $q \nmid a_0$. Tällöin ei ole olemassa ratkaisua yhtälölle $f(x) \equiv 0 \mod (q)$.

Induktio-oletus: Oletetaan sitten, että $k \geq 1$ ja kaikilla polynomeilla

$$g(x) = b_{k-1} x^{k-1} + \cdots + b_1 x + b_0,$$

joille pätee $b_i \not\equiv 0 \mod (q)$ jollakin $i \in \{0, 1, \ldots, k-1\}$, on enintään $k - 1$ juurta $[x]_q$.

Induktioaskel: Jos kongruenssiyhtälöllä $f(x) \equiv 0 \mod (q)$ ei ole ratkaisuja, todistus on valmis. Oletetaan siis, että $[a]_q$ on ratkaisu. Täten $f(a) \equiv 0 \mod (q)$, joten $q|f(a)$. Tällöin

$$f(x) - f(a) = \sum_{i=0}^{k} a_i x^i - \sum_{i=0}^{k} a_i a^i = \sum_{i=0}^{k} a_i (x^i - a^i) = \sum_{i=1}^{k} a_i (x^i - a^i).$$

Kaikilla $i = 1, \ldots, k$ voidaan merkitä

$$x^i - a^i = (x - a)\left(x^{i-1} + a x^{i-2} + \cdots + a^{i-2} x + a^{i-1}\right),$$

jolloin ottamalla $x - a$ yhteiseksi tekijäksi saadaan

$$f(x) - f(a) = (x - a) g(x)$$

jollakin enintään $k - 1$ asteisella kokonaislukukertoimisella polynomilla $g(x)$.Tällöin q ei voi jakaa kaikkia polynomin $g(x)$ kertoimia; jos näin olisi, kaikki funktion

$$f(x) = f(a) + (x - a) g(x)$$

kertoimet täytyisivät, vastoin oletuksia, olla jaollisia luvulla q, sillä $q|f(a)$. Näin ollen induktio-oletuksen nojalla saadaan, että enintään $k-1$ kongruenssiluokalle $[x]_q$ pätee $g(x) \equiv 0 \mod (q)$. Lasketaan sitten kongruenssiluokat $[x]_q$, joille pätee $f(x) \equiv 0$

mod (q). Jos mille tahansa kongruenssiluokalle $[x]_q = [b]_q$ pätee $f(b) \equiv 0 \mod (q)$, niin $q|f(a)$ ja $q|f(b)$, joten myös $f(b) - f(a) = (b-a)g(b)$ on jaollinen luvulla q. Koska q on alkuluku, niin Lemman 1.15 2)-kohdan nojalla $q|b-a$ tai $q|g(b)$, joten joko $[b]_q = [a]_q$ tai $g(b) \equiv 0 \mod (q)$. On olemassa enintään $k-1$ kongruenssiluokkaa $[b]_q$, jolle pätee $g(b) \equiv 0 \mod (q)$ ja täten enintään $1+(k-1) = k$ kongruenssiluokkaa, jolle pätee $f(b) \equiv 0 \mod (q)$. □

2.2. Fermat'n pieni lause

Todistetaan Fermat'n pieni lause, jonka avulla saadaan tutkielman ensimmäinen suurillekin luvuille sopiva alkulukutesti. Testi on puutteellinen, mutta sillä voidaan usein todeta, että tutkittava luku on varmasti yhdistetty luku. Testin lisäksi lause toimii aputuloksena myös joillekin myöhempien lukujen tuloksille.

LAUSE 2.17. *Olkoot $a \in \mathbb{Z}$ ja q alkuluku siten, että $q \nmid a$. Tällöin*

$$a^{q-1} \equiv 1 \mod (q).$$

TODISTUS. Olkoot luvut $a, 2a, ..., (q-1)a \in \mathbb{Z}$. Yksikään kokonaisluvuista $a, 2a, ..., (q-1)a$ ei ole jaollinen luvulla q, sillä jos $q|ia$, niin Lemman 1.7 1-kohdan nojalla $q|i$, kun $q \nmid a$. Tämä on kuitenkin mahdotonta, koska $1 \leq i \leq q-1$. Lisäksi mitkään kaksi lukua joukosta $a, 2a, ..., (q-1)a$ eivät ole kongruentteja keskenään modulo q. Tämän osoittamiseksi oletetaan, että $ia \equiv ja \mod (q)$, jollakin $i, j \in \mathbb{N}$, joille pätee $i, j \leq q-1$. Koska $\text{syt}(a, q) = 1$, Seurauksen 2.7 nojalla $i \equiv j \mod (q)$, mikä on mahdotonta, sillä $1 \leq i, j \leq q-1$.

Koska luvut $a, 2a, ..., (q-1)a$ ovat $q-1$ kokonaisluvun joukko, joista yksikään ei ole kongruentti luvun 0 kanssa modulo q eivätkä mitkään luvut ole kongruentteja toistensa kanssa modulo q, niin pienimmät positiiviset jäännökset ovat $1, 2, ..., (q-1)$. Tällöin lukujen $a, 2a, ..., (q-1)a$ tulo on kongruentti lukujen $1, 2, ..., (q-1)$ tulon kanssa modulo q. Näin ollen

$$a \cdot 2a \cdots (q-1)a \equiv 1 \cdot 2 \cdots (q-1) \mod (q).$$

Edelleen saadaan

$$a^{q-1}(q-1)! \equiv (q-1)! \mod (q).$$

Koska $\text{syt}(q, (q-1)!) = 1$ Seurauksen 2.7 nojalla voidaan sieventää molemmilta puolilta luku $(q-1)!$ ja saadaan

$$a^{q-1} \equiv 1 \mod (q).$$

□

Fermat'n pienen lauseen avulla voidaan tutkia lukua $p \in \mathbb{N}$. Jos p on alkuluku, niin $a^p \equiv a \mod (p)$, millä tahansa $a \in \mathbb{Z}$. Jos taas $a^p \not\equiv a \mod (p)$, jollakin $a \in \mathbb{Z}$, niin p on yhdistetty luku.

ESIMERKKI 2.18. Koska 19 on alkuluku ja $19 \nmid 34$, niin $34^{18} \equiv 1 \mod (19)$. Sen sijaan, koska $249 \nmid 5$ ja $5^{248} \equiv 40 \not\equiv 1 \mod (249)$, niin luku 249 on yhdistetty luku.

HUOMAUTUS 2.19. Vaikka $a^p \equiv a \mod (p)$, niin p voi olla kuitenkin yhdistetty luku. Tällaisia lukuja kutsutaan pseudoalkulukuiksi ja niihin tutustutaan tarkemmin luvussa 3.

Fermat'n alkulukutestillä voidaan osoittaa, että jokin luku on yhdistetty luku. Valitaan siis jokin $a \in \mathbb{Z}$ siten, että $1 \leq a \leq p-1$. Lasketaan sitten luvun a^{p-1} jakojäännös modulo p. Jos jakojäännös ei ole 1, niin Fermat'n pienen lauseen nojalla luku p on yhdistetty luku. Fermat'n testin avulla ei voida kuitenkaan etsiä yhdistetyn luvun p tekijöitä eikä vahvistaa, että luku p olisi alkuluku.

Todistetaan sitten Wilsonin lause, joka seuraa Fermat'n pienestä lauseesta. Wilsonin lauseen avulla saadaan deterministinen alkulukutesti, joka kertoo varmasti, onko tutkittava luku alkuluku vai yhdistetty.

LAUSE 2.20. *Luku $q \in \mathbb{N}$ on alkuluku, jos ja vain jos $(q-1)! \equiv -1 \mod (q)$.*

TODISTUS. Oletetaan ensin, että q on alkuluku. Jos $q = 2$, niin $(q-1)! = 1 \equiv -1 \mod (q)$, jolloin väite pätee. Voidaan siis olettaa, että q on pariton. Määritellään kokonaislukukertoiminen polynomi

$$f(x) = (1-x)(2-x)\cdots(q-1-x) + 1 - x^{q-1}.$$

Polynomin f asteluvulle d pätee $d < q-1$, sillä lausekkeen sulut avaamalla huomataan, että ne kaksi termiä, jotka sisältävät x^{q-1}, kumoavat toisensa. Jos $a = 1, 2, \ldots, q-1$, niin Fermat'n pienen lauseen 2.17 nojalla

$$\begin{aligned} f(a) &= (1-a)(2-a)\cdots(q-1-a) + 1 - a^{q-1} \\ &= +1 - a^{q-1} \equiv 0 \mod (q). \end{aligned}$$

Siis polynomilla $f(x)$ on enemmän kuin d juurta modulo q, joten Lauseesta 2.16 seuraa, että kaikki sen kertoimet ovat jaollisia luvulla q. Erityisesti q jakaa vakiotermin $(q-1)! + 1$, joten $(q-1)! \equiv -1 \mod (q)$.

Oletetaan sitten, että $(q-1)! \equiv -1 \mod (q)$. Tällöin $(q-1)! \equiv -1 \mod (p)$ mille tahansa luvun q takijälle p. Jos $p < q$, niin $p|(q-1)!$, joten $(q-1)! \equiv 0 \mod (p)$. Siis $-1 \equiv 0 \mod (p)$, mistä seuraa, että $p = 1$, joten voidaan päätellä, että q on alkuluku. □

Wilsonin lauseen avulla voidaan tutkia lukua $p \in \mathbb{N}$. Jos $(p-1)! \equiv -1 \mod (p)$, niin p on alkuluku. Vastaavasti p on yhdistetty luku jos $(p-1)! \not\equiv -1 \mod (p)$.

ESIMERKKI 2.21. Koska 53 on alkuluku, niin $(52)! \equiv 52 \equiv -1 \mod (53)$. Vastaavasti koska $(122)! \equiv 11 \not\equiv -1 \mod (123)$, niin luku 123 on yhdistetty luku.

Jos Fermat'n testin heikkous on sen epätarkkuus, on tämän testin vahvuutena tuloksen varmuus. Heikkoutena puolestaan on testin hitaus. Kertoman laskeminen muuttuu nopeasti erittäin työlääksi siirryttäessä yhä suurempiin lukuihin, eikä lopulta parhaatkaan laskentaohjelmistot pysty laskemaan kongruenssiyhtälöä kohtuullisessa ajassa.

LUKU 3

Solovay-Strassenin alkulukutesti

Tämän luvun tarkoituksena on tutustua Solovay-Strassenin alkulukutestiin. Ensin määritellään jäännösluokkarenkaat ja Eulerin ϕ-funktio sekä osoitetaan Eulerin lause ja muita tuloksia, jotka liittyvät edellä mainittuihin käsitteisiin. Toinen alaluku keskittyy algebran osa-alueeseen käsitellen yksikköryhmiä sekä ryhmien syklisyyttä. Kolmannessa puolestaan määritellään pseudoalkuluvut. Tutustutaan sitten neliönjäännökseen ja siitä seuraaviin käsitteisiin. Neljässä ensimmäisessä alaluvussa kerätään siis aputuloksia, joita tarvitaan Solovay-Strassenin lauseen todistamiseksi. Viimeisessä alaluvussa osoitetaan tulos, jonka avulla voidaan muodostaa Solovay-Strassenin alkulukutesti. Tämän luvun lähdeviitteet on merkitty yksityiskohtaisemmin jokaisen alaluvun alkuun.

3.1. Eulerin ϕ-funktio

Tässä alaluvussa määritellään jäännösluokkarenkaat ja osoitetaan siihen tuloksia. Lisäksi määritellään Eulerin ϕ-funktio. Lopuksi todistetaan Fermat'n pienen lauseen yleistys Eulerin lause sekä Eulerin ϕ-funktion laskusäännöt. Tämän alaluvun päälähde on [**2**], jonka lisäksi lähdettä [**3**] on käytetty lähinnä Eulerin lauseessa ja sen aputuloksena käytetyssä Lemmassa 3.8.

Määritellään ensin jäännösluokkarengas. Tämä vaatii kuitenkin hyvin määritellyt laskutoimitukset, jotka osoitetaan siis hyvin määritellyiksi vasta itse jäännösluokkarenkaan määritelmän jälkeen.

MÄÄRITELMÄ 3.1. Olkoon $n \in \mathbb{N}$ annettu siten, että $n > 1$. Tällöin kaikkien jäännösluokkien joukkoa merkitään symbolilla $\mathbb{Z}_n$. Siis

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

Hyvin määritellyillä yhteen- ja kertolaskulla varustettua joukkoa $\mathbb{Z}_n$ kutsutaan jäännösluokkarenkaaksi (modulo n).

Täytyy kuitenkin osoittaa, että yhteen- ja kertolaskut ovat hyvin määriteltyjä, eivätkä määritelmät riipu edustajien valinnasta. Tämä voidaan osoittaa seuraavien lemman ja lauseen avulla. Havainnollistetaan lausetta vielä yksinkertaisella esimerkillä.

LEMMA 3.2. *Olkoot $a, b \in \mathbb{Z}$ ja $n \in \mathbb{N}$. Tällöin $a \equiv b \mod (n)$, jos ja vain jos $[a] = [b]$.*

TODISTUS. Oletetaan ensin, että $a \equiv b \mod (n)$. Olkoon $c \in [a]$, jolloin $c \equiv a \mod (n)$. Tällöin Lauseen 2.8 3)-kohdan nojalla $c \equiv b \mod (n)$, joten $c \in [b]$. Siis $[a] \subset [b]$. Lukujen a ja b rooleja vaihtamalla saadaan vastaavasti $[b] \subset [a]$. Näin ollen $[a] = [b]$.

Oletetaan sitten, että $[a] = [b]$. Lauseen 2.8 1)-kohdan nojalla $a \equiv a \mod (n)$, joten $a \in [a]$. Tällöin myös $a \in [b]$, joten $a \equiv b \mod (n)$ jäännösluokan määritelmän nojalla. □

LAUSE 3.3. *Olkoot* $[a] = [c]$ *ja* $[b] = [d]$ *joukossa* $\mathbb{Z}_n$. *Tällöin*

$$[a + b] = [c + d] \quad ja$$
$$[ab] = [cd].$$

TODISTUS. Koska $[a] = [c]$ ja $[b] = [d]$, niin Lemman 3.2 nojalla $a \equiv c \mod (n)$ ja $b \equiv d \mod (n)$. Tällöin Lauseen 2.3 nojalla $a + b \equiv c + d \mod (n)$ ja $ab \equiv cd \mod (n)$. Edelleen Lemman 3.2 nojalla $[a + b] = [c + d]$ ja $[ab] = [cd]$. □

ESIMERKKI 3.4. Koska $[4]_5 = [19]_5$ ja $[8]_5 = [3]_5$, niin

$$[4 + 8]_5 = [12]_5 = [2]_5 = [22]_5 = [19 + 3]_5 \quad \text{ja}$$
$$[4 \cdot 8]_5 = [32]_5 = [2]_5 = [57]_5 = [19 \cdot 3]_5.$$

Osoitetaan sitten aputulos jäännösluokkarenkaaseen ja sen laskutoimituksiin liittyen.

LEMMA 3.5. *Olkoot* A *jäännösluokkarengas modulo* n, $k \in \mathbb{Z}$ *ja* $m \in \mathbb{N}$ *siten, että* $\text{syt}(m, n) = 1$. *Tällöin joukko* $Am + k = \{[am + k]_n : [a]_n \in A\}$ *on myös jäännösluokkarengas modulo* n.

TODISTUS. Jos $a_i m + k \equiv a_j m + k \mod (n)$, missä a_i ja a_j ovat alkioiden $[a_i]_n, [a_j]_n \in A$ edustajia, niin Lauseen 2.3 nojalla $a_i m \equiv a_j m \mod (n)$ ja edelleen Seurauksen 2.7 nojalla $a_i \equiv a_j \mod (n)$. Siis $i = j$, sillä jos olisi $i \neq j$, niin $a_i \not\equiv a_j \mod (n)$. Koska joukossa $Am + k$ on n erillistä jäännösluokkaa, on se jäännösluokkarengas modulo n. □

Määritellään Eulerin ϕ-funktio, jota tarvitaan myöhemmin tutkielman edetessä. Havainnollistetaan määritelmää sen jälkeen esimerkin avulla.

MÄÄRITELMÄ 3.6. Olkoon $n \in \mathbb{N}$. Tällöin funktio $\phi(n)$ kuvaa lukumäärää niistä luonnollisista luvuista $a \in \mathbb{N}$, jolle pätee $a \leq n$ ja $\text{syt}(a, n) = 1$.

ESIMERKKI 3.7. Jos $n = 10$, niin $\phi(n) = 4$, sillä

$$\text{syt}(1, 10) = \text{syt}(3, 10) = \text{syt}(7, 10) = \text{syt}(9, 10) = 1,$$

mutta

$$\text{syt}(2, 10) = \text{syt}(4, 10) = \text{syt}(6, 10) = \text{syt}(8, 10) = 2$$

ja

$$\text{syt}(5, 10) = 5.$$

Osoitetaan vielä aputulos, jota tarvitaan Eulerin lauseen todistuksessa. Havainnollistetaan lemmaa jälleen esimerkillä.

LEMMA 3.8. *Olkoon* $a, n \in \mathbb{N}$ *siten, että* $\text{syt}(a, n) = 1$. *Jos joukko*

$$R = \{[r_1]_n, [r_2]_n, \ldots, [r_{\phi(n)}]_n\}$$

sisältää kaikki sellaiset kongruenssiluokat, joille pätee $\text{syt}(n, r_i) = 1$ *kaikilla* $i = 1, 2, \ldots, \phi(n)$ *ja* $aR = \{a[r] : [r] \in R\}$, *niin* $R = aR$.

TODISTUS. Oletetaan ensin, että $\text{syt}(n, ar_j) > 1$. Tällöin on olemassa alkuluku q siten, että $q|\ \text{syt}(n, ar_j)$. Siis joko $q|a$ tai $q|r_j$. Täten joko $q|a$ ja $q|n$ tai $q|r_j$ ja $q|n$, mikä on ristiriita, sillä $\text{syt}(a, n) = 1$ ja $\text{syt}(r_j, n) = 1$. Näin ollen $\text{syt}(n, ar_j) = 1$ kaikilla $j = 1, 2, \ldots, \phi(n)$.

Osoitetaan sitten epäsuoralla todistuksella, että $ar_i \not\equiv ar_j \mod (n)$ aina, kun $i \neq j$. Oletetaan, että $ar_i \equiv ar_j \mod (n)$, missä indekseille $i, j \in \mathbb{N}$ pätee $i \neq j$, $1 \leq i \leq \phi(n)$ ja $1 \leq j \leq \phi(n)$. Koska $\text{syt}(a, n) = 1$, niin Seurauksen 2.7 nojalla $r_i \equiv r_j \mod (n)$, mikä on ristiriita, sillä $[r_i]_n, [r_j]_n \in R$, joten $r_i \not\equiv r_j \mod (n)$. Näin ollen väite pätee. □

ESIMERKKI 3.9. Joukot $\{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}, \}$ ja $\{[3{\cdot}1]_{10}, [3{\cdot}3]_{10}, [3{\cdot}7]_{10}, [3{\cdot}9]_{10}, \}$ ovat järjestystä vaille samat, sillä $[21]_{10} = [1]_{10}$ ja $[27]_{10} = [7]_{10}$.

Todistetaan Eulerin lause, joka on nimensä mukaisesti Leonhard Eulerin kehittämä. Tulos perustuu Fermat'n pieneen lauseeseen ja on sen yleistys. Eulerin lause pätee siis alkuluvuilla, mutta myös yhdistetyillä luvuilla. Havainnollistetaan tätäkin tulosta yksinkertaisen esimerkin avulla.

LAUSE 3.10. *Olkoon $a, n \in \mathbb{N}$ siten, että $\text{syt}(a, n) = 1$. Tällöin*

$$a^{\phi(n)} \equiv 1 \mod (n).$$

TODISTUS. Olkoon joukko $A = \{[a_1]_n, \ldots, [a_{\phi(n)}]_n\}$ sisältäen kongruenssiluokat, joille pätee $\text{syt}(n, a_i) = 1$ kaikilla $i = 1, 2, \ldots, \phi(n)$ ja $aA = \{a[a_i] : [a_i] \in A\}$, jolloin Lemman 3.8 nojalla $A = aA$. Näin ollen molemmista joukoista löytyvät samat alkiot modulo n, jolloin pätee

$$(aa_1)(aa_2)\cdots(aa_{\phi(n)}) \equiv (a_1)(a_2)\cdots(a_{\phi(n)}) \mod (n).$$

Koska kaikilla a_i, $i = 1, 2, \ldots, \phi(n)$ pätee $\text{syt}(a_i, n) = 1$, voidaan yhtälön molemmilta puolilta supistaa jokainen a_i. Tällöin $a^{\phi(n)} \equiv 1 \mod (n)$. □

ESIMERKKI 3.11. Koska $\phi(10) = 4$ ja $\text{syt}(9, 10) = 1$, niin $9^4 = 6561 \equiv 1 \mod (10)$.

Jos luku $n \in \mathbb{N}$ on pieni yhdistetty luku, Eulerin ϕ-funktio on helppo määrittää. Tällöin voidaan tutkia erikseen jokaisen lukua n pienemmän alkuluvun suurin yhteinen tekijä luvun n kanssa. Jos taas n on alkuluku voidaan käyttää Fermat'n pientä lausetta. Jos n on kuitenkin suuri yhdistetty luku, Eulerin ϕ-funktion määrittely ilman tehokkaita laskukaavoja on hyvin työlästä. Todistetaan siis Eulerin ϕ-funktioiden laskusääntöihin liittyvät kaksi lausetta sekä kaksi seurausta. Havainnollistetaan kutakin tulosta esimerkeillä.

LAUSE 3.12. *Olkoot q alkuluku ja $n \in \mathbb{N}$. Tällöin*

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

TODISTUS. Jos $a \in \mathbb{Z}$ siten, että $1 \leq a \leq q$, niin joko $a = q$ tai $\text{syt}(a, q) = 1$. Tällöin kaikki luvut $m \in \mathbb{N}$, joille pätee $m \leq q^n$ ja $\text{syt}(m, q^n) \neq 1$, ovat luvun q monikertoja. Tällaisia lukuja ovat siis luvut $q, 2q, \ldots, q^{n-1}q$ ja niitä on täten q^{n-1} kappaletta. Kaikkien muiden luonnollisten lukujen, jotka ovat korkeintaan q^n, suurin yhteinen tekijä luvun q^n kanssa on 1. Näin ollen $\phi(q^n) = q^n - q^{n-1} = q^{n-1}(q-1)$. □

Esimerkki 3.13. Kun q on alkuluku, $\phi(q^2) = q(q-1)$.
Vastaavasti, koska $14641 = 11^4$, niin

$$\phi(14641) = \phi(11^4) = 11^{4-1}(11-1) = 11^3 \cdot 10 = 13310.$$

Lause 3.14. *Olkoon $m, n \in \mathbb{N}$ siten, että* $\text{syt}(m,n) = 1$. *Tällöin*

$$\phi(mn) = \phi(m)\phi(n).$$

Todistus. Jos $m = 1$ tai $n = 1$, niin tulos on triviaali, sillä $\phi(1) = 1$. Oletetaan siis, että $m, n > 1$. Järjestetään mn luonnollista lukua $1, 2, \ldots, nm$ taulukkoon, jossa on n riviä ja m saraketta.

1	2	...	m
m+1	m+2	...	2m
⋮	⋮		⋮
(n-1)m+1	(n-1)m+2	...	nm

Nämä luvut $i \in \mathbb{N}$ muodostavat jäännösluokkarenkaan modulo mn, joista $\phi(mn)$ alkiolle pätee $\text{syt}(i,n) = \text{syt}(i,m) = 1$. Jokaisen sarakkeen kaikki jäsenet ovat keskenään kongruentteja modulo m ja nämä m saraketta vastaavat kongruenttiluokkia modulo m. Siis täsmälleen $\phi(m)$ saraketta sisältää alkioita, joille pätee $\text{syt}(i,m) = 1$ ja näiden sarakkeiden kaikki alkiot ovat sellaisia.

Nyt jokainen sarake, jonka alkioille pätee $\text{syt}(i,m) = 1$, muodostavat joukon $\{k, m+k, 2m+k, \ldots, (n-1)m+k\}$, jollakin $k \in \mathbb{Z}$. Koska $syt(m,n) = 1$ ja tämä joukko on muotoa $Am + k$, missä $A = \{[0], [1], [2], \ldots, [n-1]\}$, niin Lemman 3.5 nojalla se on jäännösluokkarengas modulo n. Jokainen näistä sarakkeista sisältää täten $\phi(n)$ alkioita, joille pätee $\text{syt}(i,n) = 1$. Siis näistä $\phi(m)$ sarakkeesta saadaan yhteensä $\phi(m)\phi(n)$ alkioita, joille pätee $\text{syt}(i,mn) = 1$. Näin ollen väite pätee. □

Esimerkki 3.15. Koska $45 = 5 \cdot 9$ ja $\text{syt}(5,9) = 1$, niin

$$\phi(45) = \phi(5)\phi(9) = 4 \cdot 6 = 24.$$

Seuraus 3.16. *Olkoot $n \in \mathbb{N}$ siten, että sen alkutekijäesitys on $n = q_1^{a_1} q_2^{a_2} \cdots q_k^{a_k}$. Tällöin*

$$\phi(n) = n\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\cdots\left(1 - \frac{1}{q_k}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{q_i}\right).$$

Todistus. Lauseiden 3.12 ja 3.14 nojalla

$$\begin{aligned}
\phi(n) &= \phi(q_1^{a_1})\phi(q_2^{a_2})\cdots\phi(q_k^{a_k}) \\
&= q_1^{a_1}\left(1 - \frac{1}{q_1}\right) q_2^{a_2}\left(1 - \frac{1}{q_2}\right)\cdots q_k^{a_k}\left(1 - \frac{1}{q_k}\right) \\
&= q_1^{a_1} q_2^{a_2}\cdots q_k^{a_k}\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\cdots\left(1 - \frac{1}{q_k}\right) \\
&= n\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\cdots\left(1 - \frac{1}{q_k}\right) \\
&= n\prod_{i=1}^{k}\left(1 - \frac{1}{q_i}\right).
\end{aligned}$$

□

Esimerkki 3.17. Koska luvun 1100 alkutekijäesitys on $1100 = 2^2 \cdot 5^2 \cdot 11$, niin

$$\phi(1100) = \phi(2^2)\phi(5^2)\phi(11) = 2 \cdot 20 \cdot 10 = 400.$$

Seuraus 3.18. *Olkoon $n \in \mathbb{N}$ siten, että $n > 2$. Tällöin $\phi(n)$ on parillinen.*

Todistus. Jos on olemassa pariton alkuluku q siten, että $q^k | n$, jollakin $k \in \mathbb{N}$, niin $2|\phi(n)$ sillä $\phi(q^k)|\phi(n)$, $\phi(q^k) = q^{k-1}(q-1)$ ja $2|(q-1)$. Jos taas $2^k|n$ jollakin $k > 1$, niin $\phi(2^k)|\phi(n)$. Koska $\phi(2^k) = 2^{k-1}$, joka on selvästi parillinen, niin $\phi(n)$ on parillinen. □

Esimerkki 3.19. Luvulle 20 pätee $\phi(20) = \phi(2^2)\phi(5) = 2 \cdot 4$.

3.2. Yksikköryhmät

Tässä alaluvussa keskitytään yksikköryhmien käsitteeseen sekä niiden syklisyyden tutkimiseen. Tämän alaluvun päälähde on [**2**], jonka lisäksi kertaluvun määritelmä on lähteestä [**3**]. Lähdettä [**1**] on käytetty Lemmassa 3.22 sekä osittain ryhmän määritelmässä ja Lauseessa 3.26.

Määritellään ensin yksikkö ja havainnollistetaan sitä jälleen esimerkillä. Todistetaan sen jälkeen aputulos, joka kertoo, onko joukon alkio yksikkö.

Määritelmä 3.20. Kongruenssiluokan $[a]_n \in \mathbb{Z}_n$ käänteisalkio kertolaskun suhteen on alkio $[b]_n \in \mathbb{Z}_n$, jolle pätee $[a]_n[b]_n = [1]_n$. Kongruenssiluokkaa $[a]_n$ kutsutaan jäännösluokkarenkaan $\mathbb{Z}_n$ yksiköksi, jos sillä on olemassa käänteisalkio joukossa $\mathbb{Z}_n$.

Esimerkki 3.21. Kongruenssiluokat $[4]_9$ ja $[7]_9$ ovat toistensa käänteisalkioita joukossa $\mathbb{Z}_9$, sillä $[4]_9[7]_9 = [1]_9$. Siis $[4]_9$ ja $[7]_9$ joukon $\mathbb{Z}_9$ yksiköitä.

Lemma 3.22. *Alkio $[a]_n \in \mathbb{Z}_n$ on yksikkö, jos ja vain jos* $\text{syt}(a, n) = 1$.

Todistus. Oletetaan ensin, että $\text{syt}(a, n) = 1$. Tällöin on olemassa luvut $x, y \in \mathbb{Z}$ siten, että $ax + ny = 1$, jolloin $ax \equiv 1 \mod (n)$, mikä tarkoittaa edelleen, että $[a]_n[x]_n = [1]_n$ joukossa $\mathbb{Z}_n$. Näin ollen $[a]_n$ on yksikkö.

Vastaavasti, oletetaan, että $[a]_n$ on yksikkö renkaassa $\mathbb{Z}_n$. Tällöin on olemassa $[x]_n \in \mathbb{Z}_n$ siten, että $[a]_n[x]_n = [1]_n$. Siis kongruenssien avulla ilmaistuna $ax \equiv 1 \mod (n)$, jolloin $n|(ax-1)$. Edelleen $ax - 1 = ny$ jollakin $y \in \mathbb{Z}$, joten $ax - ny = 1$. Näin ollen $\text{syt}(a, n) = 1$. □

Määritellään seuraavaksi kertaluku. Kertaluku on olennainen käsite erityisesti ryhmien syklisyyden tutkimisessa.

Määritelmä 3.23. Olkoon $a, n \in \mathbb{N}$ siten, että $\text{syt}(a, n) = 1$. Tällöin pienintä lukua $d \in \mathbb{N}$, jolle pätee $a^d \equiv 1 \mod (n)$, kutsutaan luvun a kertaluvuksi modulo n. Kertaluvusta käytetään usein merkintää $|a|$.

Esimerkki 3.24. Luvun 3 kertaluku modulo 10 on $|3| = 4$, sillä $3^4 = 81 \equiv 1 \mod (10)$.

Määritellään sitten ryhmät, jonka jälkeen osoitetaan, että multiplikatiivinen yksiköiden joukko on yksikköryhmä.

MÄÄRITELMÄ 3.25. Ryhmä on epätyhjä joukko G varustettuna laskutoimituksella $*$, joka toteuttaa seuraavat ehdot:

1) $(a * b) * c = a * (b * c)$ kaikilla $a, b, c \in G$,

2) on olemassa $e \in G$ siten, että $e * a = a * e$ kaikilla $a \in G$ ja

3) jokaisella $a \in G$ on olemassa alkio $d \in G$ siten, että $a * d = d * a = e$.

Alkiota e kutsutaan ryhmän G neutraalialkioksi ja alkiota d kutsutaan alkion a käänteisalkioksi. Lisäksi ryhmä G on vaihdannainen, jos

4) $a * b = b * a$ kaikilla $a, b \in G$.

Jos ryhmässä G on äärellinen määrä alkioita, niin ryhmän kertaluku |G| on alkioiden lukumäärä.

LAUSE 3.26. *Yksikköjen joukko*

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

varustettuna jäännösluokkarenkaan $\mathbb{Z}_n$ kertolaskulla on vaihdannainen ryhmä.

TODISTUS. Osoitetaan, että multiplikatiivinen joukko U_n toteuttaa vaihdannaisen ryhmän määritelmän ehdot.

1) Koska $([a]_n[b]_n)[c]_n = [a]_n[b]_n[c]_n = [a]_n([b]_n[c]_n)$ kaikilla $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$ ja $U_n \subset \mathbb{Z}_n$, niin $([a]_n[b]_n)[c]_n = [a]_n([b]_n[c]_n)$ kaikilla $[a]_n, [b]_n, [c]_n \in U_n$.

2) Joukon U_n neutraalialkio on $[1]_n$ sillä $[1]_n[a]_n = [a]_n = [a]_n[1]_n$ kaikilla $[a]_n \in \mathbb{Z}_n$ ja siten myös kaikilla $[a]_n \in U_n$.

3) Koska U_n on kaikkien renkaan $\mathbb{Z}_n$ yksiköiden joukko, niin kaikilla joukon U_n alkioilla on käänteisalkio yksikön määritelmän nojalla.

4) Koska $[a]_n[b]_n = [b]_n[a]_n$ kaikilla $[a]_n, [b]_n \in \mathbb{Z}_n$, niin $[a]_n[b]_n = [b]_n[a]_n$ kaikilla $[a]_n, [b]_n \in U_n$. □

Koska ryhmässä U_n on äärellinen määrä alkioita, niin $|U_n| = \phi(n)$. Tämä seuraa suoraan ryhmien määritelmästä. Määritellään sitten ryhmien syklisyys, virittäjä ja primitiivijuuri. Havainnollistetaan näitäkin käsitteitä esimerkeillä.

MÄÄRITELMÄ 3.27. Ryhmä G on syklinen, jos on olemassa alkio $a \in G$, siten että jokainen $g \in G$ on muotoa $a^i = g$ jollakin $i \in \mathbb{Z}$. Tällöin alkiota a kutsutaan ryhmän G virittäjäksi ja voidaan merkitä $\langle a \rangle$. Jos virittäjän kertaluku $|a| = n$ on äärellinen, niin $|G| = n$.

ESIMERKKI 3.28. Ryhmä $U_{10} = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$ on syklinen, sillä $[3]^1_{10} = [3]_{10}$, $[3]^2_{10} = [9]_{10}$,$[3]^3_{10} = [7]_{10}$ ja $[3]^4_{10} = [1]_{10}$.

Tällöin $[3]_{10}$ on ryhmän U_{10} virittäjä ja $|[3]_{10}| = 4 = |U_{10}|$.

MÄÄRITELMÄ 3.29. Jos U_n on syklinen, niin mitä tahansa ryhmän U_n virittäjää g kutsutaan primitiivijuureksi modulo n. Tämä tarkoittaa, että alkion g kertaluku on yhtä suuri, kuin ryhmän U_n kertaluku $\phi(n)$, joten alkion g potenssien avulla saadaan kaikki ryhmän U_n alkiot.

ESIMERKKI 3.30. Edellisen esimerkin perusteella lukua 3 voidaan myös kutsua primitiivijuureksi modulo 10.

Todistetaan seuraavaksi lause ja lemma, jotka liittyvät alkioiden kertalukuihin. Havainnollistetaan lausetta esimerkin avulla.

LAUSE 3.31. *Olkoon $d, n \in \mathbb{N}$. Tällöin*

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

TODISTUS. Olkoot $S = \{1, 2, \ldots, n\}$ ja $S_d = \{a \in S : \text{syt}(a, n) = \frac{n}{d}\}$, kaikilla $d \in \mathbb{N}$, joille pätee $d|n$. Nämä joukot S_d jakavat joukon S erillisiksi osajoukoiksi, sillä, kun $a \in S$, niin $\text{syt}(a, n) = \frac{n}{d}$, missä $\frac{n}{d}$ on yksikäsitteinen. Siis $\sum_{d|n} |S_d| = |S| = n$, joten riittää osoittaa, että $|S_d| = \phi(d)$ kaikilla d.

Nyt $a \in S_d$, jos ja vain jos $a \in \mathbb{Z}$ siten että $1 \leq a \leq n$ ja $\text{syt}(a, n) = \frac{n}{d}$. Jos määritellään $a' = \frac{ad}{n}$ kaikille $a \in \mathbb{Z}$, niin $a' \in \mathbb{Z}$, sillä $\text{syt}(a, n) = \frac{n}{d}$ jakaa luvun a. Tällöin $a \in S_d$, jos ja vain jos $a = \frac{n}{d}a'$, missä $a' \in \mathbb{Z}$ siten että $1 \leq a' \leq d$ ja $\text{syt}(a', d) = 1$. Siis $|S_d|$ on sellaisten kokonaislukujen a' lukumäärä, joille pätee $1 \leq a' \leq n$ ja $\text{syt}(a', d) = 1$. Tämä on funktion $\phi(d)$ määritelmä, joten $|S_d| = \phi(d)$. Näin ollen väite pätee. □

ESIMERKKI 3.32. Kun $d \in \mathbb{N}$, niin

$$\sum_{d|12} \phi(d) = \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

LEMMA 3.33. *Olkoot q alkuluku ja $a \in \mathbb{N}$ siten, että $[a] \in U_q$. Tällöin $|a|\big|(q-1)$.*

TODISTUS. Koska $[a] \in U_q$, niin $\text{syt}(a, q) = 1$. Fermat'n pienen lauseen nojalla $a^{q-1} \equiv 1 \mod (q)$, joten voidaan merkitä

$$a^{q-1} = a^{k|a|+r} = \left(a^{|a|}\right)^k a^r \equiv a^r \mod (q),$$

missä $k \in \mathbb{N}$ ja $0 \leq r < |a|$. Koska $a^{q-1} \equiv 1 \mod (q)$, niin $a^r \equiv 1 \mod (q)$. Kertaluvun määritelmän perusteella täytyy siis olla $r = 0$, joten $q - 1 = k|a|$. Näin ollen $|a|\big|(q-1)$. □

Todistetaan vielä lause, jonka seurauksena saadaan ensimmäinen tulos, joka kertoo yksikköryhmien syklisyydestä. Havainnollistetaan lausetta jälleen esimerkin avulla.

LAUSE 3.34. *Olkoot q alkuluku ja $d \in \mathbb{N}$. Ryhmällä U_q on $\phi(d)$ kertaluvun d alkiota jokaisella $d|q-1$.*

TODISTUS. Määritellään $\Omega_d = \{a \in U_q : |a| = d\}$ ja $\omega(d) = |\Omega_d|$ kaikille $d \in \mathbb{N}$, joille pätee $d|q-1$. Siis $\omega(d)$ on kertaluvun d alkioiden lukumäärä ryhmässä U_q ja tarkoituksena on osoittaa, että $\omega(d) = \phi(d)$ kaikilla d. Lemmasta 3.33 seuraa, että ryhmän U_q jokaisen alkion kertaluku jakaa luvun $q - 1$. Siis joukot Ω_d muodostavat ryhmän U_q osituksen, ja täten

$$\sum_{d|q-1} \omega(d) = q - 1.$$

Jos asetetaan $n = q - 1$, niin Lauseen 3.31 nojalla saadaan

$$\sum_{d|q-1} \phi(d) = q - 1,$$

joten

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

Jos voidaan osoittaa, että $\omega(d) \leq \phi(d)$ kaikilla $d|q-1$, pätee myös $\phi(d) - \omega(d) \geq 0$. Koska lisäksi näiden summa on 0, täytyy päteä edelleen $\phi(d) - \omega(d) = 0$. Tällöin $\omega(d) = \phi(d)$, kuten haluttiin osoittaa.

Epäyhtälö $\omega(d) \leq \phi(d)$ pätee selvästi, jos Ω_d on tyhjä joukko. Oletetaan siis, että joukko Ω_d sisältää alkion a. Joukon Ω_d määritelmän mukaan potenssit a^i, missä $i = 1, 2, \dots d$, ovat kaikki erillisiä ja niille pätee $(a^i)^d = 1$. Siis ne ovat polynomin $f(x) = x^d - 1$ d erillistä juurta joukossa $\mathbb{Z}_q$. Lauseen 2.16 nojalla funktiolla f on enintään astelukunsa d verran juuria joukossa $\mathbb{Z}_q$, joten $a^i = a, a^2, \dots a^d$ ovat kaikkien polynomin $f(x)$ juurten joukko. Osoitetaan sitten, että Ω_d koostuu näistä juurista a^i, joille pätee $\text{syt}(i, d) = 1$. Jos $b \in \Omega_d$, niin b on polynomin $f(x)$ juuri, joten $b = a^i$ jollakin $i = 1, 2, \dots, d$. Merkitään sitten $j = \text{syt}(i, d)$, jolloin

$$b^{\frac{d}{j}} = a^{\frac{id}{j}} = (a^d)^{\frac{i}{j}} = 1^{\frac{i}{j}} = 1$$

joukossa U_q. Koska d on kuitenkin alkion b kertaluku, ei ole sellaista potenssia $k \in \mathbb{Z}$, jolle pätee $k < d$ ja $b^k = 1$, joten $j = 1$. Täten kaikki alkiot b ovat muotoa a^i, missä $1 \leq i \leq d$ ja $\text{syt}(i, d) = 1$. Tällaisia lukuja i on yhteensä $\phi(d)$ kappaletta, joten alkioiden b määrälle pätee $\omega(d) \leq \phi(d)$. Näin ollen väite pätee. □

Esimerkki 3.35. Ryhmällä U_7 on $\phi(2) = 1$ kertaluvun 2 alkio, $\phi(3) = 2$ kertaluvun 3 alkiota ja $\phi(6) = 2$ kertaluvun 6 alkiota. Kertaluvut ovat $|[1]_7| = 1$, $|[2]_7| = 3$, $|[3]_7| = 6$, $|[4]_7| = 3$, $|[5]_7| = 6$ ja $|[6]_7| = 2$.

Seuraus 3.36. *Jos q on alkuluku, niin ryhmä U_q on syklinen.*

Todistus. Olkoon $n = q-1$, jolloin Lauseen 3.34 nojalla ryhmällä U_q on $\phi(q-1)$ kertaluvun $q-1$ alkiota. Koska $\phi(q-1) \geq 1$, tällaisia alkioita on ryhmässä vähintään yksi. Nyt ryhmän U_q jonkin alkion kertaluku on $\phi(q) = q-1$, joten tällainen alkio on ryhmän U_q virittäjä. Näin ollen tämä ryhmä on syklinen. □

Osoitetaan seuraavaksi kaksi lausetta ja lemma, joista saadaan ehtoja yksikköryhmien syklisyydelle. Ensimmäisen tuloksen todistuksessa mainittu binomikaava oletetaan esitietoina tunnetuksi, mutta se esitellään laskusääntöineen lähteessä [**3**].

Lause 3.37. *Olkoon q pariton alkuluku. Tällöin U_{q^k} on syklinen kaikilla $k \geq 1$.*

Todistus. Jos $k = 1$, tulos pätee Seurauksen 3.36 nojalla. Voidaan siis olettaa, että $k \geq 2$. Seurauksen 3.36 nojalla voidaan myös valita primitiivijuuri modulo q. Tällöin $g^{q-1} \equiv 1 \mod (q)$, mutta $g^i \not\equiv 1 \mod (q)$ kaikilla $1 \leq i < q-1$. Osoitetaan seuraavaksi, että joko g tai $g+q$ on primitiivijuuri modulo q^2. Koska $\text{syt}(g, q) = 1$, niin $\text{syt}(g, q^2) = 1$, joten lukua g voidaan pitää ryhmän U_{q^2} alkiona. Jos $|g| = d$ joukossa U_{q^2}, niin Eulerin lauseen 3.10 nojalla d jakaa luvun $\phi(q^2) = q(q-1)$. Kertaluvun d määritelmän nojalla saadaan $g^d \equiv 1 \mod (q^2)$, joten $g^d \equiv 1 \mod (q)$. Koska alkion g kertaluku on kuitenkin $q-1$ modulo q, niin $q-1|d$. Koska q on alkuluku, niin joko $d = q(q-1)$ tai $d = q-1$. Jos $d = q(q-1)$, niin g on primitiivijuuri modulo q^2. Oletetaan sitten, että $d = q-1$ ja olkoon $h = g+q$. Koska $h \equiv g \mod (q)$, niin h on primitiivijuuri modulo q. Siis kuten hiukan aikaisemminkin saadaan $|h| = q(q-1)$ tai $|h| = q-1$ ryhmässä U_{q^2}. Koska $g^{q-1} \equiv 1 \mod (q^2)$, niin binomikaavaa käyttämällä saadaan

$$h^{q-1} = (g+q)^{q-1} = g^{q-1} + (q-1)g^{q-2}q + \cdots \equiv 1 - qg^{q-2} \mod (q^2),$$

missä luvulla q^2 jaolliset termit jätettiin merkitsemättä. Koska $\text{syt}(g,q) = 1$, niin $qg^{q-2} \not\equiv 0 \mod (q^2)$ ja täten $h^{q-1} \not\equiv 1 \mod (q^2)$. Näin ollen alkiolla h ei ole kertalukua $q-1$ ryhmässä U_{q^2}, joten täytyy olla $|h| = q(q-1)$. Siis h on primitiivijuuri modulo q^2.

Lopuksi osoitetaan, että jos h on primitiivijuuri modulo q^2, niin h on primitiivijuuri modulo q^k kaikilla $k \geq 2$. Edellisen vaiheen nojalla voidaan olettaa, että h on primitiivijuuri modulo q^k jollakin $k \geq 2$. Olkoon $|h| = d$ joukossa $U_{q^{k+1}}$. Vastaavilla argumenteilla kuin edellisen vaiheen alussa saadaan, että d jakaa luvun $\phi(q^{k+1}) = q^k(q-1)$ ja on jaollinen luvulla $\phi(q^k) = q^{k-1}(q-1)$, joten $d = q^k(q-1)$ tai $d = q^{k-1}(q-1)$. Näistä ensimmäisessä tapauksessa h on primitiivijuuri modulo q^{k+1}, joten riittää osoittaa $h^{q^{k-1}(q-1)} \not\equiv 1 \mod (q^{k+1})$, jolloin toinen tapaus ei päde.

Koska h on primitiivijuuri modulo q^k, sen kertaluku on $\phi(q^k) = q^{k-1}(q-1)$ joukossa U_{q^k}, joten $h^{q^{k-2}(q-1)} \not\equiv 1 \mod (q^k)$. Kuitenkin $q^{k-2}(q-1) = \phi(q^{k-1})$, jolloin Eulerin lauseen 3.10 nojalla $h^{q^{k-2}(q-1)} \equiv 1 \mod (q^{k-1})$. Tällöin $h^{q^{k-2}(q-1)} = 1 + nq^{k-1}$, jollakin $n \in \mathbb{N}$, jolle pätee $\text{syt}(n,q) = 1$. Binomikaavan avulla saadaan

$$\begin{aligned} h^{q^{k-1}(q-1)} &= \left(1 + nq^{k-1}\right)^q \\ &= 1 + \binom{q}{1} nq^{k-1} + \binom{q}{2} \left(nq^{k-1}\right)^2 + \cdots \\ &= 1 + nq^k + \frac{1}{2} n^2 q^{2k-1}(q-1) + \cdots, \end{aligned}$$

missä jätettiin merkitsemättä termit, jotka ovat jaollisia luvulla $(q^{k-1})^3$, ja siten myös luvulla q^{k+1}, sillä $3(k-1) \geq (k+1)$ kaikilla $k \geq 2$. Täten

$$h^{q^{k-1}(q-1)} \equiv 1 + nq^k + \frac{1}{2} n^2 q^{2k-1}(q-1) \mod \left(q^{k+1}\right).$$

Koska q on pariton, niin termi $\frac{1}{2} n^2 q^{2k-1}(q-1)$ on myös jaollinen luvulla q^{k+1}, sillä $2k - 1 \geq k + 1$ kaikilla $k \geq 2$. Siis

$$h^{q^{k-1}(q-1)} \equiv 1 + nq^k \mod \left(q^{k+1}\right).$$

Koska $q \nmid n$, niin $h^{q^{k-1}(q-1)} \not\equiv 1 \mod (q^{k+1})$. Näin ollen $d = q^k(q-1)$, joten viimeinenkin väite pätee. □

LAUSE 3.38. *Ryhmä U_{2^k} on syklinen, jos ja vain jos $k = 1$ tai $k = 2$.*

TODISTUS. Ryhmät $U_2 = \{1\}$ ja $U_4 = \{1, 3\}$ ovat alkioiden $[1]_2$ ja $[3]_4$ virittämiä syklisiä ryhmiä, joten riittää osoittaa, että U_{2^k} ei ole syklinen, jos $k \geq 3$. Osoitetaan, että ryhmällä U_{2^k} ei ole alkiota, jonka kertaluku olisi $\phi(2^k) = 2^{k-1}$. Tehdään se osoittamalla induktion avulla, että $a^{2^{k-2}} \equiv 1 \mod (2^k)$ kaikilla parittomilla $a \in \mathbb{Z}$.

Alkuaskel: Jos $k = 3$, niin $a^2 = (2b+1)^2 = 4b(b+1) + 1 \equiv 1 \mod (8)$, missä $b \in \mathbb{Z}$. Siis väite pätee, kun $k = 3$.

Induktio-oletus: On olemassa $k \geq 3$ siten, että $a^{2^{k-2}} \equiv 1 \mod (2^k)$ kaikilla parittomilla $a \in \mathbb{Z}$.

Induktioaskel: Koska induktio-oletus pätee jollekin eksponentille $k \geq 3$, niin kaikilla parittomilla a pätee $a^{2^{k-2}} = 1 + 2^k n$, jollakin $n \in \mathbb{Z}$. Tästä saadaan edelleen

neliöimällä

$$\left(a^{2^{k-2}}\right)^2 = a^{2^{(k+1)-2}} = \left(1+2^k n\right)^2 = 1 + 2^{k+1}n + 2^{2k}n^2$$
$$= 1 + 2^{k+1}\left(n + 2^{k-1}n^2\right) \equiv 1 \mod (2^{k+1}).$$

Näin ollen väite pätee kaikille kokonaisluvuille $k \geq 3$, jolloin ryhmät U_{2^k} eivät ole syklisiä. □

LEMMA 3.39. *Jos $n = rs$, missä $r, s \in \mathbb{N}$ siten, että $r, s > 2$ ja $\text{syt}(r, s) = 1$, ryhmä U_n ei ole syklinen.*

TODISTUS. Koska $\text{syt}(r, s) = 1$, niin Lauseen 3.14 nojalla $\phi(n) = \phi(r)\phi(s)$. Koska $r, s > 2$, sekä $\phi(r)$ että $\phi(s)$ ovat parillisia Seurauksen 3.18 nojalla, joten $4|\phi(n)$.Tästä seuraa, että kokonaisluvulle $k = \frac{\phi(n)}{2}$ pätee sekä $\phi(r)|k$ että $\phi(s)|k$. Jos a on yksikkö modulo n, niin a on myös yksikkö modulo r ja modulo s, jolloin Eulerin lauseen 3.10 nojalla $a^{\phi(r)} \equiv 1 \mod (r)$ ja $a^{\phi(s)} \equiv 1 \mod (s)$. Koska $\phi(r)|k$ ja $\phi(s)|k$, niin $a^k \equiv 1 \mod (r)$ ja $a^k \equiv 1 \mod (s)$. Koska $\text{syt}(r, s) = 1$, saadaan, että $a^k \equiv 1 \mod (rs)$, ja edelleen $a^k \equiv 1 \mod (n)$. Näin ollen jokaisen ryhmän U_n alkion kertaluku jakaa luvun k. Siis ei ole olemassa primitiivijuurta modulo n, sillä $k < \phi(n)$. □

Todistetaan vielä tämän alaluvun päätulos, joka antaa täsmällisen ehdon sille, onko yksikköryhmä syklinen ja sisältääkö se siten primitiivijuurta.

LAUSE 3.40. *Ryhmä U_n on syklinen, jos ja vain jos $n = 1, 2, 4, q^k$ tai $2q^k$, missä q on pariton alkuluku ja $k \in \mathbb{N}$.*

TODISTUS. Osoitetaan ensin, että ryhmä U_n on syklinen, jos $n \in \{1, 2, 4, q^k, 2q^k\}$. Ryhmä U_n on selvästi syklinen, kun $n = 1, 2$ ja 4. Kun $n = q^k$, Lauseen 3.37 nojalla U_n on syklinen. Oletetaan sitten, että $n = 2q^k$, jolloin Seurauksen 3.16 nojalla

$$\phi(n) = \phi(2)\phi(q^k) = \phi(q^k).$$

Lauseen 3.37 nojalla on olemassa primitiivijuuri g modulo q^k. Tällöin myös $g + q^k$ on primitiivijuuri modulo q^k ja lisäksi g tai $g + q^k$ on pariton, joten on olemassa pariton primitiivijuuri h modulo q^k. Osoitetaan, että h on primitiivijuuri modulo $2q^k$. Koska sekä $\text{syt}(h, 2) = 1$ että $\text{syt}(h, q^k) = 1$, niin h on yksikkö modulo $2q^k$. Jos $h^i \equiv 1 \mod (2q^k)$, niin erityisesti $h^i \equiv 1 \mod (q^k)$. Koska h on primitiivijuuri modulo q^k, niin $\phi(q^k)|i$. Koska $\phi(q^k) = \phi(2q^k)$, niin $\phi(2q^k)|i$, joten alkion h kertaluku on $\phi(2q^k)$ ryhmässä U_{2q^k} ja h on täten myös ryhmän U_{2q^k} primitiivijuuri.

Osoitetaan sitten, että jos ryhmä U_n on syklinen, niin $n \in \{1, 2, 4, q^k, 2q^k\}$. Jos $n \notin \{1, 2, 4, q^k, 2q^k\}$, niin

1) $n = 2^k$, missä $k \geq 3$,

2) $n = 2^k q^a$, missä $k \geq 2$ ja $a \in \mathbb{N}$ tai

3) n on jaollinen vähintään kahdella parittomalla alkuluvulla.

Lause 3.38 osoittaa, että ensimmäisessä tapauksessa U_n ei ole syklinen. Toisessa tapauksessa voidaan asettaa, $r = 2^k$ ja $s = q^a$ ja kolmannessa tapauksessa puolestaan $r = q^k$, missä $q|n$ ja $s = \frac{n}{r}$. Kahdessa jälkimmäisessä tapauksessa $n = rs$, siten, että $\text{syt}(r, s) = 1$ ja $r, s > 2$, joten Lemman 3.39 nojalla U_n ei ole syklinen. □

3.3. Pseudoalkuluvut

Kuten luvun 2 lopussa todettiin, on olemassa sellaisia yhdistettyjä lukuja, jotka toteuttavat Fermat'n pienen lauseen. Tutustutaan tässä luvussa tarkemmin niihin. Tämän alaluvun lähde on [**1**], lukuun ottamatta Esimerkkejä 3.42 ja 3.44, joissa on käytetty lähdettä [**3**].

Määritellään ensin pseudoalkulukujen käsite ja havainnollistetaan sitä esimerkin avulla.

MÄÄRITELMÄ 3.41. Yhdistettyä lukua $p \in \mathbb{N}$, jolle pätee $\text{syt}(a, p) = 1$, kutsutaan pseudoalkuluvuksi kannan a suhteen, jos $a^p \equiv a \mod (p)$.

ESIMERKKI 3.42. Luku $11 \cdot 31 = 341$ on pseudoalkuluku kannan 2 suhteen, sillä $2^{340} \equiv 1 \mod (341)$. Luku 341 on siis yhdistetty luku joka toteuttaa Fermat'n pienen lauseen 2.17 ehdon kannalle 2.

Määritellään sitten Carmichaelin luvut ja todistetaan sen jälkeen Korseltin kriteeri, jonka avulla luku voidaan todeta Carmichaelin luvuksi. Havainnollistetaan määritelmää jälleen konkreettisella esimerkillä.

MÄÄRITELMÄ 3.43. Yhdistettyjä lukuja $n \in \mathbb{N}$, joille Fermat'n pieni lause toteutuu kaikilla $a \in \mathbb{N}\backslash\{1\}$, joille pätee lisäksi $\text{syt}(a, n) = 1$, kutsutaan Carmichaelin luvuiksi.

ESIMERKKI 3.44. Luku $3 \cdot 11 \cdot 17 = 561$ on Carmichaelin luku, sillä $a^{560} \equiv 1 \mod (561)$ kaikilla $a \in \mathbb{N}\backslash\{1\}$, joille pätee $\text{syt}(a, 561) = 1$. Tämä johtuu siitä, että

$$\text{syt}(a, 3) = \text{syt}(a, 11) = \text{syt}(a, 17) = 1,$$

jolloin Fermat'n pienen lauseen nojalla $a^2 \equiv 1 \mod (3)$, $a^{10} \equiv 1 \mod (11)$ ja $a^{16} \equiv 1 \mod (17)$. Siis $a^{560} \equiv (a^2)^{280} \equiv 1 \mod (3)$, $a^{560} \equiv (a^{10})^{56} \equiv 1 \mod (11)$ ja $a^{560} \equiv (a^{16})^{35} \equiv 1 \mod (17)$. Tällöin Lauseen 2.3 nojalla pätee edelleen $a^{560} \equiv 1 \mod (561)$ kaikilla $a \in \mathbb{N}\backslash\{1\}$, joille $\text{syt}(a, 561) = 1$.

LAUSE 3.45. *Pariton yhdistetty luku $n \in \mathbb{N}$ on Carmichaelin luku, jos ja vain jos luku n ei ole jaollinen minkään alkuluvun neliöllä ja jokaiselle luvun n alkulukutekijälle q pätee $(q-1)|(n-1)$.*

TODISTUS. Osoitetaan ensin, että luku n ei ole Carmichaelin luku, jos n on jaollinen jonkin alkuluvun neliöllä. Koska luvun n tekijä on neliö, on olemassa alkuluku q siten, että $q^2|n$. Lauseen 3.40 nojalla ryhmä U_{q^2} on syklinen, joten on olemassa virittäjä g modulo q^2. Koska Lauseen 3.12 nojalla $\phi(q^2) = q(q-1)$, niin $g^{q(q-1)} \equiv 1 \mod (q^2)$ ja $q(q-1)$ on pienin luvun g potenssi $d \in \mathbb{Z}$, jolle pätee $g^d \equiv 1 \mod (q^2)$. Olkoon sitten $m = q_1 \cdots q_k$, missä luvut $q_1, \ldots, q_k$ ovat luvun n alkulukutekijät luvun q lisäksi. Koska mikään alkuluvun potenssi ei ole Carmichaelin luku, niin tällaiset alkuluvut ovat olemassa. Valitaan luku $a \in \mathbb{Z}$ siten, että se on kongruenssiyhtälöparin

$$\begin{cases} a \equiv g \mod (q^2) \\ a \equiv 1 \mod (m) \end{cases}$$

ratkaisu, joka on olemassa Kiinalaisen jäännöslauseen 2.14 nojalla. Koska $a \equiv g \mod (q^2)$, niin luvulla a on myös kertaluku $q(q-1)$ modulo q^2 ja $a \in U_{q^2}$, jolloin $\text{syt}(a, q^2) = 1$. Koska lisäksi $a \equiv 1 \mod (m)$, niin $\text{syt}(a, m) = 1$, joten $\text{syt}(a, mq^2) =$

$\text{syt}(a,n) = 1$. Oletetaan, että n olisi Carmichaelin luku, jolloin n olisi pseudoalkuluku kannan a suhteen ja $a^{n-1} \equiv 1 \mod (n)$. Tällöin luvun a kertaluvusta seuraa $q(q-1)|n-1$, jolloin $n-1 \equiv 0 \mod (q)$. Toisaalta koska q on luvun n alkutekijä, niin $n-1 \equiv -1 \mod (q)$. Tämä on ristiriita, sillä $-1 \not\equiv 0 \mod (q)$. Näin ollen n ei voi olla pseudoalkuluku kannalle a ja edelleen n ei voi olla Carmichaelin luku.

Oletetaan sitten, että luku n ei ole jaollinen minkään alkuluvun neliöllä, jolloin $n = q_1 \cdots q_k$, missä $k \geq 2$ ja kaikki alkulukutekijät q_i ovat erillisiä. Oletetaan siis, että $(q_i - 1)|(n-1)$ ja $\text{syt}(a,n) = 1$. Tällöin

$$a^{n-1} \equiv a^{(q_i-1)k} \equiv 1^k \equiv 1 \mod (q_i),$$

kaikilla $i = 1, \ldots, k$. Tästä saadaan edelleen

$$a^{n-1} \equiv 1 \mod (n),$$

missä $n = q_1 \cdots q_k$. Näin ollen n on pseudoalkuluku kannalle a ja koska a on mikä tahansa kokonaisluku, jolle pätee $\text{syt}(a,n) = 1$, niin n on Carmichaelin luku.

Vastaavasti oletetaan sitten, että $n = q_1 \cdots q_k$ on Carmichaelin luku. Olkoon q_i eräs luvun n alkulukutekijä ja g ryhmän U_{q_i} virittäjä. Myös tämä ryhmä on syklinen, joten $|g| = q_i - 1$ joukossa U_{q_i}. Olkoon a sitten kongruenssiyhtälöparin

$$\begin{cases} a \equiv g \mod (q_i) \\ a \equiv 1 \mod \left(\dfrac{n}{q_i}\right) \end{cases}$$

ratkaisu, joka on olemassa Kiinalaisen jäännöslauseen 2.14 nojalla. Tällöin $q_i - 1$ on alkion a kertaluku modulo q_i. Edelleen, koska $\text{syt}(a, q_i) = 1$ ja $\text{syt}\left(a, \frac{n}{q_i}\right) = 1$, niin $\text{syt}(a,n) = 1$. Koska n on Carmichaelin luku, on se myös pseudoalkuluku kannalle a. Siis

$$a^{n-1} \equiv 1 \mod (n),$$

joten

$$a^{n-1} \equiv 1 \mod (q_i).$$

Tästä seuraa, että $(q_i - 1)|(n-1)$, sillä $|a| = q_i - 1$ ryhmässä U_{q_i}. Näin ollen väite pätee. □

3.4. Neliönjäännös

Tässä alaluvussa tutustutaan ensin neliönjäännöksen käsitteeseen, johon myös muut myöhemmin tässä luvussa esiintyvät käsitteet perustuvat. Tämän alaluvun lähteitä ovat [**3**] ja [**1**].

Määritellään ensin neliönjäännös. Todistetaan sen jälkeen kaksi tulosta, jotka kertovat olemassaolevien neliönjäännösten määrän. Havainnollistetaan määritelmää ja lausetta jälleen esimerkkien avulla

MÄÄRITELMÄ 3.46. Olkoot $n \in \mathbb{N}$ ja $a \in \mathbb{Z}$ siten, että $\text{syt}(a,n) = 1$. Luku a on luvun n neliönjäännös, jos kongruenssiyhtälöllä $x^2 \equiv a \mod (n)$ on ratkaisu. Jos yhtälöllä ei ole ratkaisua, luku a on luvun n neliönepäjäännös.

ESIMERKKI 3.47. Luku 4 on luvun 7 neliönjäännös, sillä $\text{syt}(4,7) = 1$ ja kongruenssiyhtälö $5^2 = 25 \equiv 4 \mod (7)$ pätee. Vastaavasti, luku 5 on luvun 7 neliönepäjäännös, sillä kongruenssiyhtälöllä $x^2 \equiv 5 \mod (7)$ ei ole ratkaisua.

LEMMA 3.48. *Olkoot q pariton alkuluku ja $a \in \mathbb{Z}$ siten, että $q \nmid a$. Tällöin kongruenssiyhtälöllä $x^2 \equiv a \mod (q)$ joko ei ole yhtään tai on täsmälleen kaksi epäkongruenttia ratkaisua modulo q.*

TODISTUS. Olkoon luku x_0 eräs kongruenssiyhtälön $x^2 \equiv a \mod (q)$ ratkaisu. Osoitetaan, että $-x_0$ on kongruenssiyhtälön toinen ratkaisu ja nämä ratkaisut ovat epäkongruentteja toistensa kanssa modulo q. Koska $(-x_0)^2 = x_0^2 \equiv a \mod (q)$, joten $-x_0$ on ratkaisu. Jos $x_0 \equiv -x_0 \mod (q)$, niin $2x_0 \equiv 0 \mod (q)$. Tämä on kuitenkin mahdotonta, koska q on pariton ja $q \nmid x_0$, sillä $x_0^2 \equiv a \mod (q)$ ja $q \nmid a$. Siis $x_0 \not\equiv -x_0 \mod (q)$.

Oletetaan sitten, että $x = x_0$ ja $x = x_1$ ovat molemmat kongruenssiyhtälön $x^2 \equiv a \mod (q)$ ratkaisuja. Tällöin $x_0^2 \equiv x_1^2 \equiv a \mod (q)$, joten

$$x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1) \equiv 0 \mod (q).$$

Siis $q|(x_0 - x_1)$ tai $q|(x_0 + x_1)$, joten $x_1 \equiv x_0 \mod (q)$ tai $x_1 \equiv -x_0 \mod (q)$. Näin ollen, jos kongruenssiyhtälöllä $x^2 \equiv a \mod (q)$ on olemassa ratkaisu, epäkonruentteja ratkaisuja on täsmälleen kaksi. □

LAUSE 3.49. *Olkoon q pariton alkuluku. Tällöin on olemassa täsmälleen $\frac{q-1}{2}$ neliönjäännöstä luvulle q kokonaislukujen $1, 2, \ldots, q-1$ joukossa. Näin ollen neliönepäjäännöksiä on myös $\frac{q-1}{2}$.*

TODISTUS. Lasketaan pienimmät positiiviset jäännökset modulo q kokonaislukujen $1, 2, \ldots, q-1$ neliöiden joukosta, jotta löydetään kaikki luvun q neliönjäännökset lukujen $1, 2, \ldots, q-1$ joukosta. Koska tarkasteltavia neliöitä on $q-1$ kappaletta ja koska Lemman 3.48 nojalla jokaisella kongruenssiyhtälöllä $x^2 \equiv a \mod (q)$ on joko 2 tai ei yhtään ratkaisua, niin kokonaislukujen $1, 2, \ldots, q-1$ joukossa täytyy olla täsmälleen $\frac{q-1}{2}$ neliönjäännöstä luvulle q. Loput

$$q - 1 - \frac{q-1}{2} = \frac{q-1}{2}$$

lukua ovat neliönepäjäännöksiä luvulle q. □

ESIMERKKI 3.50. Luvulla 7 on $\frac{7-1}{2} = 3$ neliönjäännöstä lukujen $1, 2, \ldots, 6$ joukossa. Nämä neliönjäännökset ovat luvut $1, 2$ ja 4. Neliönepäjäännöksiä ovat puolestaan luvut $3, 5$ ja 6.

Määritellään sitten Legendren symboli. Legendren symbolin avulla on helpompi ilmaista, onko luku neliönjäännös vai neliönepäjäännös. Havainnollistetaan määritelmää taas esimerkillä.

MÄÄRITELMÄ 3.51. Olkoon $p > 2$ alkuluku, jolle pätee $\text{syt}(a, p) = 1$ jollakin $a \in \mathbb{Z}$. Tällöin Legendren symboli $\left(\frac{a}{p}\right)$ määritellään

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

ESIMERKKI 3.52. Legendren symboli $\left(\frac{10}{13}\right) = 1$, sillä $\text{syt}(10, 13) = 1$ ja kongruenssiyhtälö $7^2 = 49 \equiv 10 \mod (13)$ pätee. Vastaavasti

$$\left(\frac{1}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{12}{13}\right) = 1$$

ja

$$\left(\frac{2}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{11}{13}\right) = -1.$$

Määritellään seuraavaksi Jacobin symbolin käsite ja havainnollistetaan sitäkin esimerkin avulla. Jacobin symboli on Legendren symbolien tulo, joten se toimii myös yhdistetyillä luvuilla.

MÄÄRITELMÄ 3.53. Olkoon $n \in \mathbb{N}$ pariton luku alkutekijäesityksellä

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

ja $a \in \mathbb{N}$. Tällöin Jacobin symboli määritellään

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1^{e_1} \cdots p_k^{e_k}}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}.$$

ESIMERKKI 3.54. Koska $7007 = 7^2 \cdot 11 \cdot 13$ ja $\text{syt}(6, 7007) = 1$, niin Jacobin symboli määritellään

$$\begin{aligned}\left(\frac{6}{7007}\right) = \left(\frac{6}{7^2 \cdot 11 \cdot 13}\right) &= \left(\frac{6}{7}\right)^2 \cdot \left(\frac{6}{11}\right) \cdot \left(\frac{6}{13}\right) \\ &= (-1)^2 \cdot (-1) \cdot (-1) = 1.\end{aligned}$$

Määritellään Eulerin pseudoalkuluvut, joihin Solovay-Strassenin alkulukutesti perustuu. Havainnollistetaan määritelmää konkreetisen esimerkin avulla.

MÄÄRITELMÄ 3.55. Olkoon $n \in \mathbb{Z}$ pariton yhdistetty luku. Tällöin n on Eulerin pseudoalkuluku kannalle $a \in \mathbb{N}$, jos

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \mod (n),$$

missä $\left(\frac{a}{n}\right)$ on Jacobin symboli.

ESIMERKKI 3.56. Luku 1105 on Eulerin pseudoalkuluku kannalle 4, sillä $4^{1104} \equiv 1 \mod (1105)$ ja

$$\left(\frac{4}{1105}\right) = \left(\frac{4}{5 \cdot 13 \cdot 17}\right) = \left(\frac{4}{5}\right) \cdot \left(\frac{4}{13}\right) \cdot \left(\frac{4}{17}\right) = 1 \cdot 1 \cdot 1 = 1,$$

joten

$$4^{\frac{1105-1}{2}} \equiv \left(\frac{4}{1105}\right) \mod (1105).$$

Solovay-Strassenin alkulukutesti perustuu siihen, että joidenkin yhdistettyjen lukujen lisäksi Eulerin pseudoalkulukujen kaava pätee jokaisella alkuluvulla kaikille kannoille. Osoitetaan tämä lause, joka tunnetaan myös Eulerin kriteeriona. Havainnollistetaan tätäkin tulosta esimerkin avulla.

LAUSE 3.57. *Olkoot q pariton alkuluku ja $a \in \mathbb{N}$ siten, että $q \nmid a$. Tällöin*

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

TODISTUS. Oletetaan ensin, että $\left(\frac{a}{q}\right) = 1$. Tällöin kongruenssiyhtälöllä $x^2 \equiv a \mod (q)$ on ratkaisu. Merkitään tätä ratkaisua $x = x_0$. Fermat'n pientä lausetta 2.17 käyttämällä saadaan

$$a^{\frac{q-1}{2}} \equiv \left(x_0^2\right)^{\frac{q-1}{2}} = x_0^{q-1} \equiv 1 \mod (q).$$

Siis väite pätee, jos $\left(\frac{a}{q}\right) = 1$.

Tutkitaan sitten tapaus, kun $\left(\frac{a}{q}\right) = -1$. Tällöin kongruenssiyhtälöllä $x^2 \equiv a \mod (q)$ ei ole ratkaisuja. Lauseen 2.11 nojalla jokaiselle luonnolliselle luvulle n, jolle pätee $1 \leq n \leq q-1$, on olemassa yksikäsitteinen luku $m \in \mathbb{N}$, jolle pätee $1 \leq m \leq q-1$ siten, että $nm \equiv a \mod (q)$. Edelleen tiedetään, että $n \neq m$, sillä kongruenssiyhtälöllä $x^2 \equiv a \mod (q)$ ei ole ratkaisuja. Siis luvut $1, 2, \ldots, q-1$ voidaan ryhmitellä $\frac{q-1}{2}$ lukupariksi, joiden tulo on kongruentti luvun a kanssa modulo q. Kun kerrotaan nämä lukuparit keskenään, saadaan

$$(q-1)! \equiv a^{\frac{q-1}{2}} \mod (q),$$

josta voidaan edelleen Wilsonin lauseen 2.20 nojalla todeta, että

$$-1 \equiv a^{\frac{q-1}{2}} \mod (q).$$

Näin ollen $a^{\frac{q-1}{2}} \equiv \left(\frac{a}{q}\right) \mod (q)$. □

ESIMERKKI 3.58. Koska $a^6 \equiv 1 \mod (13)$ ja $\left(\frac{a}{13}\right) = 1$, niin

$$a^{\frac{13-1}{2}} \equiv \left(\frac{a}{13}\right) \mod (13)$$

kaikilla $a = 1, 3, 4, 9, 10, 12$. Toisaalta taas $b^6 \equiv -1 \mod (13)$ ja $\left(\frac{b}{13}\right) = -1$, joten

$$b^{\frac{13-1}{2}} \equiv \left(\frac{a}{13}\right) \mod (13)$$

kaikilla $b = 2, 5, 6, 7, 8, 11$. Luku 13 toteuttaa siis Eulerin pseudoalkulukujen kaavan kaikilla kannoilla. Se ei ole kuitenkaan Eulerin pseudoalkuluku, sillä se ei ole yhdistetty luku.

3.5. Solovay-Strassenin alkulukutesti

Solovay-Strassenin alkulukutesti on probabilistinen testi. Testaamalla riittävän monta kantaa, voidaan todeta hyvin tarkasti, onko kyseessä alkuluku vai yhdistetty luku. Probabilistisenä testinä algoritmi ei anna ihan täsmällistä tulosta, mutta algoritmin vahvuutena puolestaan on sen tehokkuus. Se antaa deterministisiä testejä huomattavasti nopeammin arvion, onko luku erittäin suurella todennäköisyydellä alkuluku. Solovay-Strassenin alkulukutestin algoritmissa ja Lauseen 3.60 alkuosassa on käytetty lähdettä [**1**]. Lemma 3.59 sekä Lauseen 3.60 loppuosa on lähteestä [**3**].

Todistetaan ensin luvun viimeinen aputulos, jota tarvitaan Solovay-Strassenin lauseen todistuksessa.

LEMMA 3.59. *Olkoon $n \in \mathbb{N}$ pariton luku, joka ei ole minkään kokonaisluvun neliö. Tällöin on olemassa $a \in \mathbb{N}$ siten, että $1 < a < n$,* $\operatorname{syt}(a, n) = 1$ *ja* $\left(\frac{a}{n}\right) = -1$ *missä* $\left(\frac{a}{n}\right)$ *on Jacobin symboli.*

TODISTUS. Jos n on alkuluku, niin väite pätee Lauseen 3.49 nojalla. Voidaan siis olettaa, että n on yhdistetty. Koska n ei ole minkään kokonaisluvun neliö, niin voidaan merkitä $n = rs$, missä $r, s \in \mathbb{N}$ siten, että $\text{syt}(r, s) = 1$ ja $r = q^k$ jollakin parittomalla alkuluvulla q ja parittomalla $k \in \mathbb{N}$. Olkoon sitten $t \in \mathbb{N}$ alkuluvun q neliönepäjäännös, joka on olemassa Lauseen 3.49 nojalla. Etsitään sitten luku $a \in \mathbb{Z}$ siten, että $1 < a < n$, $\text{syt}(a, n) = 1$ ja a on kongruenssiyhtälöparin

$$\begin{cases} a \equiv t \mod (r) \\ a \equiv 1 \mod (s) \end{cases}$$

ratkaisu, joka on olemassa Kiinalaisen jäännöslauseen 2.14 nojalla. Tällöin

$$\left(\frac{a}{r}\right) = \left(\frac{a}{q^k}\right) = \left(\frac{a}{q}\right)^k = (-1)^k = -1$$

ja $\left(\frac{a}{s}\right) = 1$, joten

$$\left(\frac{a}{n}\right) = \left(\frac{a}{rs}\right) = \left(\frac{a}{r}\right)\left(\frac{a}{s}\right) = -1 \cdot 1 = -1.$$

□

Todistetaan vielä Solovay-Strassenin lause, joka on tämän luvun, ja samalla koko tutkielman yksi päätuloksista. Solovay-Strassenin alkulukutestin algoritmi seuraa suoraan tästä tuloksesta.

LAUSE 3.60. *Olkoon $n \in \mathbb{N}$ pariton yhdistetty luku. Tällöin n on Eulerin pseudoalkuluku enintään puolelle kannoista $a \in \mathbb{N}$, kun $1 < a < n$ ja* $\text{syt}(a, n) = 1$.

TODISTUS. Olkoon $n \in \mathbb{N}$ pariton yhdistetty luku. Osoitetaan ensin, että tässä tapauksessa, jos n ei ole Eulerin pseudoalkuluku vähintään yhdelle kannalle a, niin se ei ole sellainen vähintään puolelle kannoista a, joille pätee $1 < a < n$ ja $\text{syt}(a, n) = 1$. Osoitetaan sitten, että on olemassa kanta a, jolle n ei ole Eulerin pseudoalkuluku.

Oletetaan, että n ei ole Eulerin pseudoalkuluku kannalle a. Tällöin

$$a^{\frac{n-1}{2}} \not\equiv \pm 1 \mod (n).$$

Jos n ei ole Eulerin pseudoalkuluku yhdellekään kannalle a, on selvää, että se ei ole Eulerin pseudoalkuluku vähintään puolelle mahdollisista kannoista. Oletetaan sitten, että n on Eulerin pseudoalkuluku kannalle a_1, joten

$$a_1^{\frac{n-1}{2}} \equiv \pm 1 \mod (n).$$

Tällöin

$$(aa_1)^{\frac{n-1}{2}} \equiv a^{\frac{n-1}{2}} a_1^{\frac{n-1}{2}} \equiv \pm a^{\frac{n-1}{2}} \not\equiv \pm 1 \mod (n).$$

Siis n ei ole Eulerin pseudoalkuluku kannalle aa_1. Näin ollen jokaiselle kannalle a_i, joille n on Eulerin pseudoalkuluku pätee, että n ei ole Eulerin pseudoalkuluku kannalle aa_i. Edelleen, jos a_i ja a_j ovat erillisiä kantoja modulo n, joille n on Eulerin pseudoalkuluku, niin $aa_i \not\equiv aa_j \mod (n)$. Tästä seuraa, että $aa_1, \ldots, aa_k$ ovat erillisiä kantoja, joille n ei ole Eulerin pseudoalkuluku, jos $a_1, \ldots, a_k$ ovat erillisiä kantoja, joille n on Eulerin pseudoalkuluku. Siis on olemassa vähintään yhtä monta kantaa, joille n ei ole Eulerin pseudoalkuluku, kuin niitä kantoja, joille n on sellainen. Näin ollen, jos on olemassa vähintään yksi kanta a, jolle n ei ole Eulerin pseudoalkuluku, niin n on Eulerin pseudoalkuluku enintään puolelle mahdollisista kannoista.

Osoitetaan sitten, että on olemassa kanta a, jolle n ei ole Eulerin pseudoalkuluku. Oletetaan, että $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \mod (n)$ kaikille $a \in \mathbb{Z}$, joille pätee $1 < a < n$ ja $\text{syt}(a, n) = 1$. Korottamalla kongruenssiyhtälön molemmat puolet toiseen potenssiin saadaan

$$a^{n-1} \equiv \left(\frac{a}{n}\right)^2 \equiv (\pm 1)^2 = 1 \mod (n),$$

kun $\text{syt}(a, n) = 1$, joten n täytyy olla Carmichaelin luku. Tällöin Lauseen 3.45 nojalla $n = q_1 \cdots q_k$, missä luvut $q_1, \ldots, q_k$ ovat keskenään erillisiä parittomia alkulukuja.

Osoitetaan sitten, että

$$a^{\frac{n-1}{2}} \equiv 1 \mod (n),$$

kaikille $a \in \mathbb{Z}$, joille pätee $1 < a < n$ ja $\text{syt}(a, n) = 1$. Olkoon $a \in \mathbb{Z}$ siten, että

$$a^{\frac{n-1}{2}} \equiv -1 \mod (n).$$

Etsitään luku $b \in \mathbb{Z}$ siten, että $1 < b < n$, $\text{syt}(b, n) = 1$ ja b on kongruenssiyhtälöparin

$$\begin{cases} b \equiv a \mod (q_1) \\ b \equiv 1 \mod (q_2 q_3 \cdots q_k) \end{cases}$$

ratkaisu, joka on olemassa Kiinalaisen jäännöslauseen 2.14 nojalla. Tällöin

$$b^{\frac{n-1}{2}} \equiv a^{\frac{n-1}{2}} \equiv -1 \mod (q_1),$$

kun

$$b^{\frac{n-1}{2}} \equiv 1 \mod (q_2 q_3 \cdots q_k).$$

Edellisistä kongruenssiyhtälöistä saaadaan edelleen

$$b^{\frac{n-1}{2}} \not\equiv \pm 1 \mod (n),$$

mikä on ristiriidassa tämän vaiheen ensimmäisen oletuksen kanssa. Siis kaikilla $a \in \mathbb{Z}$, joille pätee $1 < a < n$ ja $\text{syt}(a, n) = 1$ täytyy olla

$$a^{\frac{n-1}{2}} \equiv 1 \mod (n).$$

Näin ollen Eulerin pseudoalkuluvun määritelmästä saadaan, että

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) = 1 \mod (n)$$

kaikilla $a \in \mathbb{Z}$, joille pätee $1 < a < n$ ja $\text{syt}(a, n) = 1$. Kuitenkin Lemman 3.59 nojalla tämä on mahdotonta, joten väite on epätosi. Näin ollen on olemassa vähintään yksi $a \in \mathbb{Z}$, joille pätee $1 < a < n$ ja $\text{syt}(a, n) = 1$ siten, että

$$a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \mod (n).$$

□

Edellisestä lauseesta seuraten voidaan muotoilla testausalgoritmi, jonka tarkkuus riippuu testattujen kantojen määrästä k. Jos testataan paljon kantoja saadaan yhä suurempi todennäköisyys $1 - (\frac{1}{2})^k$ tuloksen totuudenmukaisuudelle, mutta testaaminen hidastuu.

Periaatteessa testaamalla riittävän monta kantaa, tästäkin alkulukutestistä saisi siis deterministisen testin, mutta se on käytännössä täysin hyödytön työkalu, sillä

kaikkien kantojen testaaminen veisi mahdottoman paljon aikaa. Siksi keskitytään ainoastaan probabilistiseen algoritmiin. Lähteessä [**1**] esitellään algoritmin päätteeksi mainittu arvio todennäköisyydestä sille, että $n \in \mathbb{N}$ on alkuluku.

Solovay-Strassenin alkulukutesti toimii seuraavalla algoritmilla:

Olkoon $n \in \mathbb{Z}$ pariton.

1. Valitaan k satunnaista kokonaislukua $a_1, ...a_k$, siten, että $1 < a_i < n$ kaikilla $i = 1, ..., k$.

2. a) Lasketaan syt(a_i, n) Eukleideen algoritmin avulla. Jos syt$(a_i, n) > 1$, niin n on yhdistetty luku ja testin voi lopettaa.

b) Lasketaan $a_i^{\frac{n-1}{2}} \mod (n)$ ja $(\frac{a_i}{n}) \mod (n)$. Jos $a^{\frac{n-1}{2}} \not\equiv (\frac{a}{n}) \mod (n)$, niin n on yhdistetty luku ja testin voi lopettaa.

3. Toistetaan vaihetta 2 kaikilla $i = 1, ..., k$ tai kunnes huomataan, että n on yhdistetty luku.

4. Todennäköisyys sille, että n on alkuluku, on suurempi kuin $1 - (\frac{1}{2})^k$.

LUKU 4

Miller-Rabinin alkulukutesti

Tämän luvun tarkoituksena on tutustua Miller-Rabinin alkulukutestiin. Ensin osoitetaan kongruenssiin liittyviä aputuloksia, määritellään indeksin käsite sekä osoitetaan indeksiaritmetiikkaan liittyviä aputuloksia. Jälkimmäisessä alaluvussa keskitytään Miller-Rabinin alkulukutestiin liittyviin käsitteisiin ja tuloksiin, joiden avulla muodostetaan Miller-Rabinin alkulukutestin algoritmi. Tämän luvun päälähde on [**3**], jonka lisäksi lähdettä [**1**] on käytetty algoritmin muotoiluun.

Todistetaan ensin kaksi kongruensseihin liittyvää lausetta, joita ei ole aikaisemmin tutkielmassa tarvittu. Näitä tuloksia käytetään kuitenkin apuna indeksiaritmetiikkaan liittyvissä tuloksissa. Havainnollistetaan molempia lauseita esimerkin avulla.

LAUSE 4.1. *Olkoot $n \in \mathbb{N}$ ja $a \in \mathbb{Z}$ siten, että* $\text{syt}(a, n) = 1$. *Tällöin $x \in \mathbb{N}$ on kongruenssiyhtälön $a^x \equiv 1 \mod (n)$ ratkaisu, jos ja vain jos $|a| \big| x$.*

TODISTUS. Jos $|a| \big| x$, niin $x = k|a|$, missä $k \in \mathbb{N}$. Tällöin

$$a^x = a^{k|a|} = \left(a^{|a|}\right)^k \equiv 1 \mod (n).$$

Vastaavasti, jos $a^x \equiv 1 \mod (n)$, voidaan jakoyhtälön avulla kirjoittaa

$$x = q|a| + r,$$

missä $0 \leq r < |a|$. Tästä saadaan edelleen

$$a^x = a^{q|a|+r} = \left(a^{|a|}\right)^q a^r \equiv a^r \mod (n).$$

Koska $a^x \equiv 1 \mod (n)$, niin $a^r \equiv 1 \mod (n)$. Epäyhtälöstä $0 \leq r < |a|$ voidaan päätellä, että $r = 0$, sillä kertaluvun määritelmän mukaan $d = |a|$ on pienin luonnollinen luku siten, että $a^d \equiv 1 \mod (n)$. Koska $r = 0$, niin $x = q|a|$. Näin ollen $|a| \big| x$. □

ESIMERKKI 4.2. Jos $a = 4$ ja $n = 9$, niin $\text{syt}(a, n) = \text{syt}(4, 9) = 1$ ja $|a| = 3$. Tällöin

$$4^{3k} = (4^3)^k \equiv 1^k \equiv 1 \mod (9),$$

mutta

$$4^{3k+1} = (4^3)^k 4 \equiv 1^k 4 \equiv 4 \not\equiv 1 \mod (9)$$

ja

$$4^{3k+2} = (4^3)^k 4^2 \equiv 1^k 4^2 \equiv 16 \equiv 7 \not\equiv 1 \mod (9)$$

kaikilla $k \in \mathbb{Z}$.

LAUSE 4.3. *Olkoot $n \in \mathbb{N}$ ja $a \in \mathbb{Z}$ siten, että* $\text{syt}(a, n) = 1$. *Tällöin $a^i \equiv a^j \mod (n)$, missä $i, j \in \mathbb{N} \cup \{0\}$ jos, ja vain jos $i \equiv j \mod (|a|)$.*

TODISTUS. Oletetaan ensin, että $i \equiv j \mod (|a|)$. Tällöin $i = j + k|a|$ jollakin $k \in \mathbb{N}$. Täten

$$a^i = a^{j+k|a|} = a^j \left(a^{|a|}\right)^k \equiv a^j \mod (n),$$

sillä $a^{|a|} \equiv 1 \mod (n)$.

Oletetaan sitten, että $a^i \equiv a^j \mod (n)$ siten, että $i \geq j$. Koska $\text{syt}(a, n) = 1$, niin $\text{syt}(a^j, n) = 1$. Tällöin Seurauksen 2.7 nojalla kongruenssiyhtälö

$$a^i \equiv a^j a^{i-j} \equiv a^j \mod (n)$$

saadaan supistamalla a^j muotoon

$$a^{i-j} \equiv 1 \mod (n).$$

Lauseen 4.1 nojalla $|a|$ jakaa luvun $i - j$ tai vastaavasti $i \equiv j \mod (|a|)$. □

ESIMERKKI 4.4. Jos $a = 4$ ja $n = 9$, niin $\text{syt}(a, n) = \text{syt}(4, 9) = 1$ ja $|a| = 3$. Tällöin $4^{3k} \equiv 1 \mod (9)$, $4^{3k+1} \equiv 4 \mod (9)$, ja $4^{3k+2} \equiv 7 \mod (9)$ kaikilla $k \in \mathbb{Z}$, joten $4^{3k} \not\equiv 4^{3k+1} \not\equiv 4^{3k+2} \mod (9)$.

4.1. Indeksiaritmetiikkaa

Määritellään indeksin käsite, johon nimensä mukaisesti muut indeksiaritmetiikan tulokset perustuvat. Indeksien avulla voidaan ilmaista eräiden epälineaaristen kongruessiyhtälöiden ratkaisujen olemassaolo sekä keskenään epäkongruenttien ratkaisujen lukumäärä.

MÄÄRITELMÄ 4.5. Olkoon $n \in \mathbb{N}$ siten, että sillä on primitiivijuuri r. Jos $a \in \mathbb{N}$ siten, että $\text{syt}(a, n) = 1$, niin yksikäsitteistä lukua $x \in \mathbb{Z}$, jolle pätee $1 \leq x \leq \phi(n)$ ja $r^x \equiv a \mod (n)$, kutsutaan luvun a indeksiksi kannalle r modulo n. Tällöin voidaan merkitä $a \equiv r^{\text{ind}_r a} \mod (n)$.

Jos x on luvun a indeksi kannalle r modulo n, merkitään $x = \text{ind}_r a$. Tällöin modulo n jätetään merkitsemättä, koska se oletetaan ennalta määrätyksi. Määritelmän perusteella tiedetään myös, että jos $a, b \in \mathbb{Z}$ siten, että $\text{syt}(a, b) = 1$ ja $a \equiv b \mod (n)$, niin $\text{ind}_r a = \text{ind}_r b$.

ESIMERKKI 4.6. Jos $n = 10$ ja $a = 9$, niin $r = 3$ ja $\phi(10) = 4$. Tällöin $\text{ind}_3 9 = 2$, sillä $9 \equiv 3^2 \mod (10)$ ja $1 \leq 2 \leq 4$. Vastaavasti myös $\text{ind}_3 19 = 2$.

Osoitetaan sitten lause, joka sisältää tärkeimmät laskusäännöt indekseillä laskemiseen.

LAUSE 4.7. *Olkoot $n \in \mathbb{N}$ ja $a, b \in \mathbb{Z}$ siten, että r on luvun n primitiivijuuri ja $\text{syt}(a, n) = \text{syt}(b, n) = 1$. Tällöin*

1) $\text{ind}_r 1 \equiv 0 \mod (\phi(n))$,

2) $\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \mod (\phi(n))$ *ja*

3) $\text{ind}_r a^k \equiv k \cdot \text{ind}_r a \mod (\phi(n))$, *jos* $k \in \mathbb{N}$.

TODISTUS. 1) Eulerin lauseen 3.10 nojalla $r^{\phi(n)} \equiv 1 \mod (n)$. Koska r on primitiivijuuri modulo n, mikään pienempi positiivinen luvun r potenssi ei ole kongruentti luvun 1 kanssa modulo n. Näin ollen $\text{ind}_r 1 = \phi(n) \equiv 0 \mod (\phi(n))$.

2) Indeksin määritelmästä saadaan

$$r^{\text{ind}_r(ab)} \equiv ab \mod (n)$$

ja

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

Siis

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

Lausetta 4.3 käyttämällä saadaan

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

3) Huomataan, että määritelmästä saadaan

$$r^{\operatorname{ind}_r a^k} \equiv a^k \mod (n)$$

ja

$$r^{k\cdot \operatorname{ind}_r a} \equiv \left(r^{\operatorname{ind}_r a}\right)^k \equiv a^k \mod (n).$$

Täten

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

Lausetta 4.3 käyttämällä saadaan suoraan haluttu kongruenssiyhtälö

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

□

Osoitetaan sitten lause, joka kertoo täsmälleen, kuinka monta ratkaisua yhden muuttujan kongruenssiyhtälöllä on.

Lause 4.8. *Olkoot $n, k \in \mathbb{N}$ ja $a \in \mathbb{Z}$ siten, että luvulla n on primitiivijuuri ja* $\operatorname{syt}(a, n) = 1$. *Tällöin kongruenssiyhtälöllä $x^k \equiv a \mod (n)$ on ratkaisu, jos ja vain jos*

$$a^{\frac{\phi(n)}{d}} \equiv 1 \mod (n),$$

missä $d = \operatorname{syt}(k, \phi(n))$. Edelleen, jos kongruenssiyhtälöllä $x^k \equiv a \mod (n)$ on olemassa ratkaisu, niin on olemassa täsmälleen d keskenään epäkongruenttia ratkaisua modulo n.

Todistus. Olkoon r primitiivijuuri modulo n. Huomataan, että kongruenssiyhtälö $x^k \equiv a \mod (n)$ pätee, jos ja vain jos

$$k \cdot \operatorname{ind}_r x \equiv \operatorname{ind}_r a \mod (\phi(n)). \tag{4.1}$$

Olkoon sitten $d = \operatorname{syt}(k, \phi(n))$ ja $y = \operatorname{ind}_r x$, jolloin $x \equiv r^y \mod (n)$. Jos $d \nmid \operatorname{ind}_r a$, Lauseen 2.11 perusteella kongruenssiyhtälöllä

$$ky \equiv \operatorname{ind}_r a \mod (\phi(n)) \tag{4.2}$$

ei ole ratkaisuja, joten ei ole olemassa yhtälön (4.1) toteuttavaa lukua $x \in \mathbb{Z}$. Jos $d \mid \operatorname{ind}_r a$, on olemassa täsmälleen d keskenään epäkongruenttia lukua $y \in \mathbb{Z}$ modulo $\phi(n)$ siten, että yhtälö (4.2) pätee. Näin ollen on olemassa myös täsmälleen d keskenään epäkongruenttia lukua $x \in \mathbb{Z}$ modulo n siten, että yhtälö (4.1) pätee. Koska $d \mid \operatorname{ind}_r a$, jos ja vain jos

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

ja edelleen tämä kongruenssiyhtälö pätee, jos ja vain jos

$$a^{\frac{\phi(n)}{d}} \equiv 1 \mod (n),$$

niin väite pätee. □

Osoitetaan seuraavaksi edellisen tuloksen kaltainen aputulos, kun muuttujan potenssi on luonnollinen luku ja jäännösluokkarengas on alkuluvun potenssi. Havainnollistetaan tulosta esimerkin avulla.

LEMMA 4.9. *Olkoot q pariton alkuluku ja $d, e \in \mathbb{N}$. Tällöin kongruessiyhtälöllä*

$$x^d \equiv 1 \mod (q^e)$$

on $\operatorname{syt}(d, q^{e-1}(q-1))$ *keskenään epäkongruenttia ratkaisua modulo q^e.*

TODISTUS. Olkoon r primitiivijuuri modulo q^e. Käyttämällä indeksiä juuren r suhteen, saadaan $x^d \equiv 1 \mod (q^e)$, jos ja vain jos pätee $dy \equiv 0 \mod (\phi(q^e))$, missä $y = \operatorname{ind}_r x$. Lauseen 2.11 nojalla kongruennssiyhtälöllä $dy \equiv 0 \mod (\phi(q^e))$ on olemassa täsmälleen $\operatorname{syt}(d, \phi(q^e))$ keskenään epäkongruenttia ratkaisua. Tästä seuraa edelleen, että kongruenssiyhtälöllä $x^d \equiv 1 \mod (q^e)$ on olemassa täsmälleen

$$\operatorname{syt}(d, \phi(q^e)) = \operatorname{syt}(d, q^{e-1}(q-1))$$

keskenään epäkongruenttia ratkaisua modulo q^e. □

ESIMERKKI 4.10. Jos $q = 3$, $d = 4$ ja $e = 2$, niin yhtälöllä $x^4 \equiv 1 \mod (9)$ on $\operatorname{syt}(4, 3^{2-1}(3-1)) = \operatorname{syt}(4, 6) = 2$ epäkongruenttia ratkaisua, jotka ovat kongruenssiluokat $[1]_9$ ja $[8]_9$.

Todistetaan vielä viimeinen aputulos Miller-Rabinin testiä varten.

LEMMA 4.11. *Olkoon $N = 2^j u$ luonnollinen luku siten, että $j \in \mathbb{N} \cup \{0\}$ ja $u \in \mathbb{N}$ on pariton. Olkoon $q \in \mathbb{N}$ pariton alkuluku siten, että $q - 1 = 2^s t$, missä $s, t \in \mathbb{N}$ ja t on pariton. Tällöin kongruenssiyhtälöllä $x^N \equiv -1 \mod (q)$ on $2^j \operatorname{syt}(t, u)$ keskenään epäkongruenttia ratkaisua, jos $0 \leq j \leq s-1$. Ratkaisuja ei ole olemassa, jos $j \geq s$.*

TODISTUS. Koska $q - 1 \equiv -1 \mod (q)$, niin voidaan yhtälö $x^N \equiv -1 \mod (q)$ kirjoittaa muotoon

$$x^N \equiv 2^s t \mod (q). \tag{4.3}$$

Koska q on alkuluku ja $x^N \not\equiv 0 \mod (q)$, niin $\operatorname{syt}(x, q) = 1$, jolloin Lauseen 4.8 nojalla kongruenssiyhtälöllä (4.3) on ratkaisu, jos ja vain jos

$$(-1)^{\frac{\phi(q)}{d}} \equiv 1 \mod (q), \tag{4.4}$$

missä $d = \operatorname{syt}(N, \phi(q))$. Tällöin ratkaisuja on myös täsmälleen d kappaletta.

Huomataan, että kongruenssiyhtälö (4.4) pätee, jos ja vain jos $\frac{\phi(q)}{d}$ on parillinen. Jos $0 \leq j \leq s-1$, niin $\frac{\phi(q)}{d}$ on parillinen, sillä

$$\frac{\phi(q)}{d} = \frac{\phi(q)}{\operatorname{syt}(N, \phi(q))} = \frac{2^s t}{\operatorname{syt}(2^j u, 2^s t)} = \frac{2^s t}{2^j \operatorname{syt}(u, t)} = \frac{2^{s-j} t}{\operatorname{syt}(u, t)}$$

siten, että $s - j > 0$. Siis kongruenssiyhtälö (4.4) pätee, jolloin edelleen kongruenssiyhtälöllä (4.3) on

$$d = \operatorname{syt}(N, \phi(q)) = \operatorname{syt}(2^j u, 2^s t) = 2^j \operatorname{syt}(u, t)$$

keskenään epäkongruenttia ratkaisua modulo q.

Vastaavasti, jos $s \leq j$, niin

$$\frac{\phi(q)}{d} = \frac{\phi(q)}{\operatorname{syt}(N, \phi(q))} = \frac{2^s t}{\operatorname{syt}(2^j u, 2^s t)} = \frac{2^s t}{2^s \operatorname{syt}(u,t)} = \frac{t}{\operatorname{syt}(u,t)},$$

mikä on pariton, sillä u ja t ovat parittomia. Näin ollen yhtälö (4.4) ei päde, eikä kongruenssiyhtälöllä (4.3) ole ratkaisuja. □

4.2. Miller-Rabinin alkulukutesti

Määritellään Millerin testi, johon Miller-Rabinin alkulukutesti pohjautuu. Havainnollistetaan määritelmää myös esimerkin avulla.

MÄÄRITELMÄ 4.12. Olkoon $n \in \mathbb{N}$ siten, että $n - 1 = 2^s t$, missä $s \in \mathbb{N} \cup \{0\}$ ja $t \in \mathbb{N}$ on pariton. Luku n läpäisee Millerin testin kannalle a, jos joko

$$a^t \equiv 1 \mod (n)$$

tai

$$a^{2^j t} \equiv -1 \mod (n)$$

jollakin j, jolle pätee $0 \leq j \leq s - 1$.

ESIMERKKI 4.13. Luku 49 läpäisee Millerin testin kannoille $1, 18, 19, 30, 31$ ja 48, sillä $49 - 1 = 2^4 \cdot 3$ sekä

$$1^3 \equiv 18^3 \equiv 30^3 \equiv 1 \mod (49)$$

ja

$$19^{2^0 \cdot 3} \equiv 31^{2^0 \cdot 3} \equiv 48^{2^0 \cdot 3} \equiv -1 \mod (49).$$

Miller-Rabinin alkulukutesti perustuu siihen, että alkuluvut läpäisevät Millerin testin. Osoitetaan tämä seuraavassa lauseessa ja havainnollistetaan tulosta esimerkin avulla.

LAUSE 4.14. *Olkoot $q \in \mathbb{N}$ alkuluku ja $a \in \mathbb{N}$ siten, että $q \nmid a$. Tällöin q läpäisee Millerin testin kannalle a.*

TODISTUS. Olkoon $q - 1 = 2^s t$ siten, että $t \in \mathbb{N}$ on pariton ja $s \in \mathbb{N} \cup \{0\}$. Olkoon $x_k = a^{\frac{q-1}{2^k}} = a^{2^{s-k} t}$ kaikilla $k = 0, 1, 2, \ldots, s$. Fermat'n pienen lauseen 2.17 nojalla saadaan $x_0 = a^{q-1} \equiv 1 \mod (q)$. Koska $x_1^2 = (a^{\frac{q-1}{2}})^2 = x_0 \equiv 1 \mod (q)$, niin $q | (x_1^2 - 1)$. Tästä saadaan edelleen, että $q | (x_1 - 1)$ tai $q | (x_1 + 1)$, sillä $x_1^2 - 1 = (x_1 - 1)(x_1 + 1)$. Näin ollen pätee joko $x_1 \equiv -1 \mod (q)$ tai $x_1 \equiv 1 \mod (q)$. Jos $x_1 \equiv 1 \mod (q)$, niin vastaavasti joko $x_2 \equiv -1 \mod (q)$ tai $x_2 \equiv 1 \mod (q)$, sillä $x_2^2 = x_1 \equiv 1 \mod (q)$. Yleisesti, jos havaitaan, että

$$x_0 \equiv x_1 \equiv x_2 \equiv \cdots \equiv x_k \equiv 1 \mod (q)$$

kaikilla $k < s$, niin jälleen joko $x_{k+1} \equiv -1 \mod (q)$ tai $x_{k+1} \equiv 1 \mod (q)$, sillä $x_{k+1}^2 = x_k \equiv 1 \mod (q)$.

Jatkamalla menettelyä kaikilla $k = 1, 2, \ldots, s$, huomataan, että joko $x_k \equiv 1 \mod (q)$ kaikilla $k = 1, 2, \ldots, s$, tai $x_k \equiv -1 \mod (q)$ jollakin $k \in \mathbb{Z}$. Näin ollen q läpäisee Millerin testin kannalle a. □

ESIMERKKI 4.15. Luku 7 läpäisee Millerin testin kannoille $1, 2, 3, 4, 5$ ja 6, sillä $7 - 1 = 2^1 \cdot 3$ sekä $1^3 \equiv 2^3 \equiv 4^3 \equiv 1 \mod (7)$ ja $3^{2^0 \cdot 3} \equiv 5^{2^0 \cdot 3} \equiv 6^{2^0 \cdot 3} \equiv -1 \mod (7)$.

Alkulukujen lisäksi on olemassa yhdistettyjä lukuja, jotka läpäisevät Millerin testin. Määritellään nämä ja havainnollistetaan määritelmää esimerkin avulla.

MÄÄRITELMÄ 4.16. Luku n on vahva pseudoalkuluku kannalle a, jos n on yhdistetty luku, joka läpäisee Millerin testin kannalle a.

ESIMERKKI 4.17. Luku 49 on vahva pseudoalkuluku kannoille $1, 18, 19, 30, 31$ ja 48, sillä $49 = 7^2$ ja se läpäisee Millerin testin edellä mainituille kannoille.

Todistetaan vielä tutkielman viimeisenä tuloksena lause, joka on toinen tutkielman päätuloksista. Deterministinen alkulukutesti seuraa suoraan tästä tuloksesta.

LAUSE 4.18. *Olkoon $n \in \mathbb{N}$ pariton yhdistetty luku. Tällöin n läpäisee Millerin testin enintään $\frac{n-1}{4}$ kannalle a, joille pätee $1 \leq a \leq n-1$.*

TODISTUS. Olkoon $n - 1 = 2^s t$, missä $s, t \in \mathbb{N}$ siten, että t on pariton. Jotta n olisi vahva pseudoalkuluku kannalle a, pätee joko

$$a^t \equiv 1 \mod (n)$$

tai

$$a^{2^j t} \equiv -1 \mod (n),$$

jollakin $j \in \mathbb{Z}$ siten, että $0 \leq j \leq s-1$. Molemmissa tapauksissa pätee myös

$$a^{n-1} \equiv 1 \mod (n).$$

Olkoon luvun n alkutekijäesitys $n = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$. Lemman 4.9 nojalla kongruenssiyhtälölle $x^{n-1} \equiv 1 \mod (q_h^{e_h})$, missä $h = 1, 2, \ldots, r$, on olemassa

$$\operatorname{syt}(n-1, q_h^{e_h-1}(q_h - 1)) = \operatorname{syt}(n-1, q_h - 1)$$

keskenään epäkongruenttia ratkaisua. Siis Kiinalaisen jäännöslauseen 2.14 nojalla kongruenssiyhtälölle $x^{n-1} \equiv 1 \mod (n)$ on olemassa täsmälleen $\prod_{h=1}^{r} \operatorname{syt}(n-1, q_h-1)$ keskenään epäkongruenttia ratkaisua.

Tarkastellaan tapausta, missä luvun n alkutekijäesitys sisältää alkutekijän $q_k^{e_k}$, jonka eksponentti $e_k \geq 2$. Tällöin

$$\frac{q_k - 1}{q_k^{e_k}} = \frac{1}{q_k^{e_k-1}} - \frac{1}{q_k^{e_k}} \leq \frac{2}{9},$$

sillä suurin mahdollinen arvo saadaan, kun $q_k = 3$ ja $e_k = 2$. Tästä saadaan edelleen, että

$$\prod_{h=1}^{r} \operatorname{syt}(n-1, q_h - 1) \leq \prod_{h=1}^{r} (q_h - 1) \leq \left(\prod_{h=1, h \neq k}^{r} q_h \right) \left(\frac{2}{9} q_k^{e_k} \right) \leq \frac{2}{9} n.$$

Koska $\frac{2}{9} n \leq \frac{1}{4}(n-1)$ kaikille $n \geq 9$, nähdään, että

$$\prod_{h=1}^{r} \operatorname{syt}(n-1, q_h - 1) \leq \frac{n-1}{4}.$$

Siis on olemassa enintään $\frac{n-1}{4}$ kokonaislukua $1 \leq a \leq n-1$ siten, että n on vahva pseudoalkuluku kannalle a.

Tarkastellaan tapausta, missä luvun n alkutekijäesitys on $n = q_1 q_2 \cdots q_r$, missä $q_1, q_2, \ldots, q_r$ ovat toisistaan eroavia parittomia alkulukuja. Olkoon $q_i - 1 = 2^{s_i} t_i$ kaikilla $i = 1, 2, \ldots, r$, missä $s_i, t_i \in \mathbb{N}$ ja t_i on pariton. Järjestetään alkutekijät $q_1, q_2, \ldots, q_r$ tarvittaessa uudelleen siten, että $s_1 \leq s_2 \leq \cdots \leq s_r$. Huomataan, että

$$\operatorname{syt}(n-1, q_i - 1) = 2^{\min(s, s_i)} \operatorname{syt}(t, t_i).$$

Lemman 4.9 nojalla kongruenssiyhtälöllä $x^t \equiv 1 \mod (q_i)$ on $T_i = \operatorname{syt}(t, t_i)$ keskenään epäkongruenttia ratkaisua. Lemman 4.11 nojalla konruenssiyhtälöllä $x^{2^j t} \equiv -1 \mod (q_i)$ on $2^j T_i$ keskenään epäkongruenttia ratkaisuja, kun $1 < j \leq s_i - 1$ ja muutoin ratkaisuja ei ole. Täten Kiinalaisen jäännöslauseen 2.14 nojalla kongruenssiyhtälölle $x^t \equiv 1 \mod (n)$ on olemassa täsmälleen $T_1 T_2 \cdots T_r$ keskenään epäkongruenttia ratkaisua ja kongruenssiyhtälölle $x^{2^j t} \equiv -1 \mod (n)$ on olemassa täsmälleen $2^{jr} T_1 T_2 \cdots T_r$ keskenään epäkongruenttia ratkaisua, kun $1 < j \leq s_1 - 1$. Näin ollen on olemassa yhteensä

$$T_1 T_2 \cdots T_r \left(1 + \sum_{j=0}^{s_1 - 1} 2^{jr}\right) = T_1 T_2 \cdots T_r \left(1 + \frac{2^{r s_1} - 1}{2^r - 1}\right)$$

kokonaislukua $1 \leq a \leq n-1$ siten, että n on vahva pseudoalkuluku kannalle a.

Koska

$$\phi(n) = (q_1 - 1)(q_2 - 1) \cdots (q_r - 1) = t_1 t_2 \cdots t_r 2^{s_1 + s_2 + \cdots + s_r},$$

voidaan osoittaa, että

$$T_1 T_2 \cdots T_r \left(1 + \frac{2^{r s_1} - 1}{2^r - 1}\right) \leq \frac{\phi(n)}{4},$$

mikä todistaa halutun tuloksen. Koska $T_1 T_2 \cdots T_r \leq t_1 t_2 \cdots t_r$, riittää osoittaa, että

$$\left(1 + \frac{2^{r s_1} - 1}{2^r - 1}\right) / 2^{s_1 + s_2 + \cdots + s_r} \leq \frac{1}{4}. \tag{4.5}$$

Koska $s_1 \leq s_2 \leq \cdots \leq s_r$, niin

$$\begin{aligned}
\left(1 + \frac{2^{r s_1} - 1}{2^r - 1}\right) / 2^{s_1 + s_2 + \cdots + s_r} &\leq \left(1 + \frac{2^{r s_1} - 1}{2^r - 1}\right) / 2^{r s_1} \\
&= \frac{1}{2^{r s_1}} + \frac{2^{r s_1} - 1}{2^{r s_1}(2^r - 1)} \\
&= \frac{1}{2^{r s_1}} + \frac{1}{2^r - 1} - \frac{1}{2^{r s_1}(2^r - 1)} \\
&= \frac{1}{2^r - 1} + \frac{2^r - 2}{2^{r s_1}(2^r - 1)} \\
&\leq \frac{1}{2^r - 1} + \frac{2^r - 2}{2^{r \cdot 1}(2^r - 1)} \\
&= \frac{2^r + 2^r - 2}{2^r(2^r - 1)} = \frac{2^r - 1}{2^{r-1}(2^r - 1)} = \frac{1}{2^{r-1}}.
\end{aligned}$$

Tästä epäyhtälöstä saadaan, että yhtälö (4.5) on totta, kun $r \geq 3$.

Kun $r = 2$, $n = q_1 q_2$ siten, että $q_1 - 1 = 2^{s_1} t_1$, $q_2 - 1 = 2^{s_2} t_2$ ja $s_1 \leq s_2$. Jos $s_1 < s_2$, yhtälö (4.5) on jälleen totta, sillä

$$\begin{aligned}
\left(1 + \frac{2^{2s_1} - 1}{3}\right) / 2^{s_1+s_2} &= \left(1 + \frac{2^{2s_1} - 1}{3}\right) / \left(2^{2s_1} \cdot 2^{s_2 - s_1}\right) \\
&= \left(\frac{3 + 2^{2s_1} - 1}{3 \cdot 2^{2s_1}}\right) / 2^{s_2 - s_1} \\
&= \left(\frac{2^{2s_1 - 1} + 1}{3 \cdot 2^{2s_1 - 1}}\right) / 2^{s_2 - s_1} \\
&= \left(\frac{1}{3} + \frac{1}{3 \cdot 2^{2s_1 - 1}}\right) / 2^{s_2 - s_1} \\
&\leq \left(\frac{1}{3} + \frac{1}{3 \cdot 2^{2s_1 - 1}}\right) / 2 \\
&\leq \left(\frac{1}{3} + \frac{1}{3 \cdot 2}\right) \cdot \frac{1}{2} = \frac{1}{4}.
\end{aligned}$$

Kun $s_1 = s_2$, $\text{syt}(n-1, q_1 - 1) = 2^s T_1$ ja $\text{syt}(n-1, q_2 - 1) = 2^s T_2$. Oletetaan sitten, että $q_1 > q_2$. Huomataan, että $T_1 \neq t_1$, sillä $(q_1 - 1) | (n-1)$, jos $T_1 = t_1$, jolloin

$$n = q_1 q_2 \equiv q_2 \equiv 1 \mod (q_1 - 1),$$

mistä saadaan edelleen ristiriita $q_1 < q_2$. Koska $T_1 \neq t_1$, niin $T_1 \leq \frac{t_1}{3}$. Vastaavasti, jos $q_1 < q_2$, niin $T_2 \neq t_2$, joten $T_2 \leq \frac{t_2}{3}$. Siis $T_1 T_2 \leq \frac{t_1 t_2}{3}$ ja koska

$$\begin{aligned}
\left(1 + \frac{2^{2s_1} - 1}{3}\right) / 2^{2s_1} &= \frac{3 + 2^{2s_1} - 1}{3 \cdot 2^{2s_1}} \\
&= \frac{2^{2s_1} + 2}{3 \cdot 2^{2s_1}} \\
&= \frac{1}{3} + \frac{1}{3 \cdot 2^{2s_1 - 1}} \\
&\leq \frac{1}{3} + \frac{1}{3 \cdot 2} = \frac{1}{2},
\end{aligned}$$

saadaan

$$T_1 T_2 \left(1 + \frac{2^{2s_1} - 1}{3}\right) \leq \frac{t_1 t_2 2^{2s_1}}{6} = \frac{t_1 t_2 2^{s_1 + s_2}}{6} = \frac{\phi(n)}{6}.$$

Näin ollen lauseen viimeinenkin tapaus pätee, sillä

$$\frac{\phi(n)}{6} \leq \frac{n-1}{6} < \frac{n-1}{4}.$$

□

Miller-Rabinin alkulukutesti on deterministinen testi ja se seuraa suoraan edellisestä lauseesta. Testaamalla riittävän monta kantaa, voidaan todeta varmasti, onko kyseessä alkuluku vai yhdistetty luku. Riittävän monen kannan testaaminen on kuitenkin käytännössä mahdottoman hidasta. Sen takia usein käytetäänkin testin probabilistista versiota, jonka algoritmi antaa yleensä riittävän tarkan arvion sille, onko kyseessä alkuluku.

Miller-Rabinin probabilistinen alkulukutesti toimii seuraavalla algoritmilla:

Olkoon $n \in \mathbb{Z}$ pariton ja oletetaan, että $n-1 = 2^s t$, missä $s \in \mathbb{N} \cup \{0\}$ ja $t \in \mathbb{N}$ on pariton.

1. Valitaan k satunnaista kokonaislukua $a_1, ..., a_k$, siten, että $1 < a_i < n$ kaikilla $i = 1, ..., k$.

2. a) Lasketaan syt(a_i, n) Eukleideen algoritmin avulla. Jos syt$(a_i, n) > 1$, niin n on yhdistetty luku ja testin voi lopettaa.

b) i) Lasketaan $m_i = a_i^t \mod (n)$ Jos $m_i = \pm 1$, niin n on vahva pseudoalkuluku kannalle a_i ja siirrytään seuraaavaan indeksiin i.

ii) Muutoin lasketaan $k_j = a_i^{2^j t} \mod (n)$, missä $j = 1, ..., s-1$. Jos $k_j \equiv -1 \mod (n)$, niin n on vahva pseudoalkuluku kannalle a_i ja siirrytään seuraaavaan indeksiin i. Jos taas $k_j \not\equiv -1 \mod (n)$, niin siirrytään seuraaavaan indeksiin j.

iii) Jos $k_j \not\equiv -1 \mod (n)$ kaikilla $j = 1, ..., s-1$, niin n on yhdistetty luku ja testin voi lopettaa.

3. Toistetaan vaihetta 2 kaikilla $i = 1, ..., k$ tai kunnes huomataan, että n on yhdistetty luku.

4. Todennäköisyys sille, että n on alkuluku, on suurempi kuin $1 - (\frac{1}{4})^k$.

LUKU 5

RSA-menetelmät

Tämän luvun tarkoituksena on tutustua alkulukutestien hyödytämiseen käytännön sovelluksissa. Luvun alussa esitellään yleisesti julkisen avaimen salausmenetelmät ja sen jälkeen keskitytään RSA-menetelmiin, joiden toiminta perustuu tehokkaiden alkulukutestien olemassaoloon. Tämän luvun päälähteenä on [**1**] ja lisäksi apuna on käytetty myös lähdettä [**3**].

Nykyaikana suojattuja tietoja joudutaan usein lähettämään avoimessa verkossa. Tällaisia tapauksia ovat esimerkiksi verkkopankissa asiointi sekä maksutapahtumat verkossa. Tämä sai aikaan julkisen avaimen salausmenetelmien kehittymiseen. Perusajatuksena on muodostaa yksisuuntainen funktio, joka on helppo toteuttaa, mutta sen käänteisfunktio on vaikea selvittää. Tästä syystä viestin salaaminen on helppoa, mutta sen purkaminen on erittäin vaikeaa, ellei käänteisfunktiota tiedä.

Julkisten avaimien järjestelmien perusrakenne on menetelmästä riippumatta hyvin samankaltainen. Henkilö X haluaa lähettää viestin henkilölle Y. Salausmenetelmä f_X henkilölle X on julkista tietoa, kuten myös f_Y henkilölle Y. Toisaalta salauksenpurkualgoritmit f_X^{-1} ja f_Y^{-1} ovat salaisia ja vain henkilöt X ja Y tuntevat omansa. Olkoon P viesti, jonka henkilö X haluaa lähettää henkilölle Y. Hän lähettää viestin $f_Y f_X^{-1}(P)$. Purkaakseen koodin Y lisää viestiin f_Y^{-1}, jonka vain hän tietää. Tällöin hän saa tietoonsa $f_Y^{-1}(f_Y f_X^{-1}(P)) = f_X^{-1}(P)$. Sen jälkeen hän etsii f_X, mikä on julkisesti saatavilla ja sitä hyödyntäen selvittää $f_X(f_X^{-1}(P)) = P$.

Yksi yleisimmin käytetyistä julkisen avaimen salausjärjestelmistä on RSA-algoritmi, jonka Ron Rivest, Adi Shamir ja Len Adelman kehittivät vuonna 1977. Algoritmin toiminta perustuu siihen, että nykyaikaisten laskentaohjelmistojen sekä alkulukutestien avulla kuka tahansa voi löytää vain muutamassa minuutissa kaksi noin 100-numeroista alkulukua p ja q sekä luvun e, jolle pätee $\text{syt}(e, \phi(pq)) = 1$. Kun vaaditut luvut p, q ja e ovat valittu, salaaminen tapahtuu muutamassa sekunnissa. Sen sijaan luvun $n = pq$ jakaminen tekijöihin ei ole mahdollista kohtuullisessa ajassa tehokkaimmillakaan tietokoneohjelmistoilla, sillä vielä ei ole olemassa suurille alkulukuvuille toimivaa tekijöihinjakoalgoritmia. RSA-menetelmässä käytettiin aluksi noin 100-numeroisia alkulukuja, mutta tietotekniikan ja tekijöihinjakoalgoritmien kehittyessä on jouduttu siirtymään huomattavasti suurempiin alkulukuihin. Tämän takia jatkuvasti kehitetään uusiakin salausmenetelmiä.

RSA-menetelmä toimii seuraavasti: Henkilö X valitsee satunnaisesti kaksi suurta alkulukua p_X ja q_X sekä kokonaisluvun e_X, jolle pätee

$$\text{syt}(e_X, \phi(p_X q_X)) = \text{syt}(e_X, (p_X - 1)(q_X - 1)) = 1.$$

Alkuluvut valitaan alkulukutestien avulla. Valitaan jokin suuri pariton luku m ja testataan, onko kyseessä alkuluku. Jos m on alkuluku, valitaan se, mutta jos m on yhdistetty luku tutkitaan alkulukutestien avulla luvut $m + 2, m + 4, \ldots$, kunnes löydetään

ensimmäinen alkuluku p_X. Sama prosessi toistamalla saadaan q_X. Vastaavasti valitaan uusi luku m ja testataan kunnes löydetään e_X, jolle pätee $\text{syt}(e_X, \phi(p_X q_X)) = 1$. Valittujen alkulukujen täytyy olla suuria.

Kun luvut p_X, q_X ja e_X on löydetty, lasketaan $n_X = p_X q_X$ ja luvun e_X käänteisalkio d_X modulo $\phi(n_X)$. Tämän jälkeen henkilö X luo julkisen salausavaimen $K_X = (n_X, e_X)$, jolloin kaikkien tiedossa oleva salausalgoritmi on

$$f_X(P) \equiv P^{e_X} \mod (n_X),$$

missä $P \in \mathbb{Z}_{n_X}$ on viestiyksikkö. Tällöin salauksenpurkualgoritmi on

$$f_X^{-1}(C) \equiv P^{d_X} \mod (n_X).$$

Vastaavasti, henkilö Y valitsee samoilla ehdoilla luvut p_Y, q_Y ja e_Y, laskee $n_Y = p_Y q_Y$ ja luo julkisen salausavaimensa $K_Y = (n_Y, e_Y)$.

Jos X haluaa lähettää viestin henkilölle Y, joka voidaan vahvistaa olevan hänen lähettämänsä, lähettää hän viestin muodossa $f_Y(f_X^{-1}(P))$. Tällöin viestiin käsiksi pääseminen vaatisi luvun n_X tai n_Y tekijöihin jakamisen, mikä on alkulukujen tiheydestä johtuen paljon haastavampaa kuin alkulukujen p_X, q_X, p_Y ja q_Y aikaansaaminen.

Havainnollistetaan RSA-menetelmän käyttöä esimerkillä, jossa käytetään suhteellisen pieniä alkulukuja.

Esimerkki 5.1. Käytettään eksponenttina $e = 17$ ja salaamisen jäännösluokkana alkulukujen 37 ja 67 tuloa $n = 37 \cdot 67 = 2479$. Huomataan, että

$$\text{syt}(e, \phi(n)) = \text{syt}(17, 36 \cdot 66) = 1.$$

Viestin

SALAUSAVAIN

salaamiseksi RSA-menetelmän avulla muutetaan kirjaimet vastaamaan niiden kaksinumeroista järjestyslukua aakkosissa ja ryhmitellään nämä numerot nelinumeroisiksi lukujen lukujonoksi. Tällöin saadaan

$$(1901, 1201, 2119, 0122, 0109, 1424),$$

kun lisätään loppuun $X = 24$, jotta saadaan kaikista luvuista nelinumeroisia. Muutetaan jokainen luku salakirjoitukseksi luomalla salausavain

$$C \equiv P^{17} \mod (2479).$$

Esimerkiksi, kun salataan luku 1901, saadaan

$$C \equiv 1901^{17} \equiv 732 \mod (2479).$$

Salaamalla vastaavasti kaikki jonon muutkin luvut, saadaan salakirjoitukseksi

$$(0732, 1086, 2283, 0619, 2350, 1038).$$

RSA-menetelmällä salattujen viestien tulkitsemiseksi täytyy löytää luvun $e = 17$ käänteisalkio modulo $\phi(2479) = \phi(37 \cdot 67) = 36 \cdot 66 = 2376$. Lyhyt laskutoimitus Eukleideen algoritmin avulla kertoo, että $d = 1817$ on luvun $e = 17$ käänteisalkio modulo 2376.

Vastaavasti salakirjoituksen purkamiseen käytetään purkuavainta

$$P \equiv C^{1817} \mod (2479),$$

missä $0 \leq P \leq 2479$. Tämä pätee, sillä Eulerin lausetta 3.10 apuna käyttäen saadaan

$$C^{1817} \equiv \left(P^{17}\right)^{1817} \equiv \left(P^{2376}\right)^{13} P \equiv 1^{13} P \equiv P \mod (2479),$$

kun $\text{syt}(P, 2479) = 1$, joka pätee kaikille esimerkissä käytetyn lukujonon luvuille.

Viestiä lähettäessä julkaistaan luvut n ja e sekä viesti, johon on käytetty sekä lähettäjän purkuavainta, että vastaanottajan julkista salausavainta. Purkuavaimen eksponentti d sekä luvun n alkutekijät p ja q sen sijaan pidetään omana tietona.

Kirjallisuutta

[1] Benjamin Fine ja Gerhard Rosenberger: *Number Theory An Introduction via the Distribution of Primes*, Birkhäuser Boston, 2007.

[2] Gareth A. Jones ja J. Mary Jones: *Elementary Number Theory*, kahdeksas painos, Springer, 2005.

[3] Kenneth H. Rosen: *Elementary Number Theory And Its Applications*, Addison-Wesley, 1984.

[4] Eero Ruosteenoja: *Lukuteoria 1.* luentomuistiinpanot, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, 2018.