Sisällöstä

Lukuteorian kurssi on ensisijaisesti tarkoitettu opettajalinjan maisterikurssiksi. Tämä näkyy mm. siten, että perinteisesti lukuteoriaan kuuluvan materiaalin lisäksi kurssi sisältää jonkin verran sellaista lukuihin liittyvää asiaa, jonka voi toivoa kuuluvan matematiikan opettajan yleissivistykseen, mutta jota ei ole käsitelty muilla kursseilla. Toisaalta kurssin sisältämän teorian määrä on verrattain vähäinen; samoja perustyökaluja sovelletaan useassa eri yhteydessä. Tavoitteena on se, että ainakin nämä perustyökalut (jotka tulevat osin vastaan myös lukion lukuteorian kursseilla) opittaisiin hallitsemaan kunnolla.

Kurssi käy hyvin myös sovelletun matematiikan opiskelijoille johtuen siitä, että monet matematiikan sovellutukset perustuvat lukuteoriaan ja moniin sovellutuksiin päästään käsiksi ns. alkeellisella lukuteorialla. Kurssilla käsitellään myös käytännön sovellutuksia, joista tiedonsalaus lienee tätä nykyä keskeisin.

Kurssille voi osallistua vaikkei olisi käynytkään algebran kurssia. Algebran kurssin käyneille alkuosa sisältää jonkin verran kertausta, koska jaollisuuden perusominaisuudet keskeisenä työkaluna on hyvä käsitellä alkeista lähtien huolella.

Oppimateriaali

Jokseenkin kaikki kurssilla käsiteltävät asiat löytyvät kirjasta *Rosen: Elementary number theory and it's applications*. Kuitenkaan Rosenin kirjaa ei seurata systemaattisesti.

1 Lukujärjestelmät

1.1 Jakoyhtälö

Sovitaan merkinnöistä

$$\begin{aligned}
&\mathbf{N} = \{\, 1, 2, \dots \} \quad (\text{luonnolliset luvut}),\\
&\mathbf{Z} = \{\, \cdots -2, -1, 0, 1, 2, \dots \} \quad (\text{kokonaisluvut}),\\
&\mathbf{Z}_+ = \{\, 0, 1, 2, \dots \} \quad (\text{positiiviset kokonaisluvut}),\\
&\mathbf{R} = \text{reaaliluvut}.
\end{aligned}$$

Pidämme kokonaislukujen algebralliset "perusominaisuudet"tunnettuna. Erityisesti seuraavat kaksi lemmaa oletetaan tunnetuksi.

Lemma 1.1.1 *Jokaisessa epätyhjässä ei-negatiivisten kokonaislukujen osajoukossa on pienin luku.*

Lause 1.1.2 (Jakoyhtälö) Olkoot $a, b \in \mathbf{Z}$, $b \neq 0$. Tällöin on olemassa yksikäsitteisesti määrätyt luvut $q, r \in \mathbf{Z}$ siten, että

$$a = bq + r \quad \text{ja} \quad 0 \leq r < |b|.$$

Nimityksiä Lauseessa 1.1.2 a on *jaettava*, b *jakaja*, q *kokonaisosa* ja r on *jakojäännös*.

Esimerkki 1.1.3 (a) Olkoon $a \in \mathbf{Z}$. Jakoyhtälön mukaan a on muotoa $a = 2q$ tai muotoa $a = 2q + 1$, missä $q \in \mathbf{Z}$. Ensimmäisessä tapauksessa a on *parillinen* ja toisessa tapauksessa a on *pariton*.

(b) Osoitetaan, että parittoman luvun neliö on aina muotoa $8k + 1$, $k \in \mathbf{Z}$?

Tapa 1: Jos n on pariton, $n = 2k + 1$ jollekin $k \in \mathbf{Z}$. Näin ollen $n^2 = 4k^2 + 4k + 1 = 4(k(k + 1)) + 1$. Riittää siis osoittaa, että $k(k + 1)$ on aina parillinen. Tämä on selvää, jos k on muotoa $k = 2k'$. Jos taas $k = 2k' + 1$, niin

$$k(k + 1) = (2k' + 1)(2k' + 2) = 2k''$$

jollekin $k'' \in \mathbf{Z}$.

Tapa 2: Luku n on muotoa $4k + r$, missä $r = 0, 1, 2, 3$. Koska n on pariton, välttämättä $r = 1$ tai $r = 3$. Jos $r = 1$, saadaan

$$(4k + 1)^2 = 16k^2 + 8k + 1 = 8(2k^2 + k) + 1.$$

Jos taas $r = 3$, saadaan

$$(4k + 3)^2 = 16k^2 + 24k + 9 = 8(2k^2 + 3k + 1) + 1.$$

Todetaan, että tulos on kummassakin tapauksessa vaadittavaa muotoa.

Määritelmä 1.1.4 Luku $a \in \mathbf{Z}$ on luvun $b \in \mathbf{Z}$ *tekijä* jos $b = ak$ jollakin $k \in \mathbf{Z}$.

Jos a on b:n tekijä, merkitään $a \mid b$. Jos a ei ole b:n tekijä, merkitään $a \nmid b$.

Huomautus 1.1.5 Olkoon $a \mid b$. Jos $b \neq 0$, niin $|a| \leq |b|$. Nimittäin $b = ak$ jollakin $k \in \mathbf{Z}$, joten

$$|b| = |ak| = |a||k| \geq |a|,$$

sillä $|k| \geq 1$ kaikilla $k \in \mathbf{Z} \setminus \{0\}$.

Lause 1.1.6 Olkoon $b > 1$ kokonaisluku ja olkoon $N \in \mathbf{N}$. Tällöin on olemassa yksikäsitteiset luvut $m \in \mathbf{Z}_+$ ja $a_i \in \mathbf{Z}$ siten, että $a_m \neq 0$,

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0$$

ja $0 \leq a_i \leq b - 1$ kaikilla $i = 0, 1, \ldots, m$.

Lauseessa 1.1.6 lukua b sanotaan *kantaluvuksi* ja merkitään lyhyesti

$$N = (a_m a_{m-1} \ldots a_1 a_0)_b = a_m a_{m-1} \ldots a_1 a_{0_b}.$$

Jos $b = 10$ jätetään sulut sekä kantaluku pois eli merkitään vain

$$N = a_m a_{m-1} \ldots a_1 a_0.$$

Huomautus

- Kullekin luvulle $0, \ldots, b-1$ on ensin sovittu oma symbolimerkintä, esimerkiksi 10-järjestelmä perustuu arabeilta perittyihin symboleihin 0,1,2,3,4,5,6,7,8,9.
- Kymmenjärjestelmä levisi arabeilta Eurooppaan 1200-luvulta lähtien mm. Fibonaccin Liber Abacin ansiosta (liite).
- Babylonialaiset käyttivät 60-järjestelmää, mayat 20-järjestelmää.

Esimerkki Ennen todistusta tarkastellaan lukua 103 3- ja 8-järjestelmissä. Soveltamalla toistuvasti jakoyhtälöä saadaan

$$103 = 8 \cdot 12 + 7 = 8(8 \cdot 1 + 4) + 7 = 1 \cdot 8^2 + 4 \cdot 8 + 7 \cdot 8^0 = (147)_8$$

ja

$$\begin{aligned} 103 &= 3 \cdot 34 + 1 = 3(3 \cdot 11 + 1) + 1 = 11 \cdot 3^2 + 3 + 3^0 \\ &= (3 \cdot 3 + 2) \cdot 3^2 + 3 + 3^0 \\ &= 3^4 + 2 \cdot 3^2 + 3 + 3^0 = (10211)_3. \end{aligned}$$

Todistus. Olemassaolo: Jakoyhtälön nojalla

$$N = q_0 b + a_0, \quad 0 \leq a_0 \leq b-1.$$

Tässä $q_0 \geq 0$. Jos nimittäin $q_0 < 0$, niin $N < 0$, ristiriita. Jos $q_0 = 0$ eli $0 < N \leq b-1$, esitys pätee (tällöin $N = a_0$). Jos taas $q_0 > 0$, jaetaan q_0 kantaluvulla b ja saadaan

$$q_0 = q_1 b + a_1, \quad 0 \leq a_1 \leq b-1.$$

Tässä $0 \leq q_1 < q_0$. Jatkamalla samaan tapaan löydetään aidosti laskevasti ei-negatiiviset luvut $q_0, q_1, \ldots, q_m = 0$ siten, että

$$q_{i-1} = q_i b + a_i 0 \quad \text{ja} \quad 0 \leq a_i \leq b-1$$

kaikilla $i = 1, \ldots, m$. Sijoittamalla saadaan

$$\begin{aligned} N &= q_0 b + a_0 = (q_1 b + a_1) b + a_0 = q_1 b^2 + a_1 b + a_0 = (q_2 b + a_2) b^2 + a_1 b + a_0 \\ &= q_2 b^3 + a_2 b^2 + a_1 b + a_0 = \cdots = q_{m-1} b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0 \\ &= a_m b^m + \cdots + a_1 b + a_0, \end{aligned}$$

sillä $q_{m-1} = q_m b + a_m = a_m$.

Yksikäsitteisyys: Oletetaan, että luvulla N on kaksi vaadittua muotoa olevaa esitystä eli

$$a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0 = N = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0,$$

missä $0 \leq a_i \leq b-1$, $0 \leq c_i \leq b-1$, $a_m \neq 0$ ja $c_n \neq 0$. Voidaan olettaa, että $m \geq n$. Merkitään $c_i = 0$ kun $n+1 \leq i \leq m$. Vähentämällä esitykset puolittain toisistaan ja merkitsemällä $d_i := a_i - c_i$ saadaan

$$d_m b^m + d_{m-1} b^{m-1} + \cdots + d_1 b + d_0 = 0.$$

Oletetaan vastoin väitettä, että esitykset eivät ole samat. Tällöin $d_i \neq 0$ jollekin $i = 0, \ldots, m$ ja löydetään pienin luku

$$j := \min\{\, i = 0, \ldots, m \mid d_i \neq 0 \,\}.$$

Siis

$$d_m b^m + d_{m-1} b^{m-1} + \cdots + d_j b^j = 0.$$

Ratkaisemalla tästä d_j saadaan, että $d_j = kb$ jollekin $k \in \mathbf{Z}$. Näin ollen $b \mid d_j$. Toisaalta

$$-b < -c_j \leq d_j = a_j - c_j < b,$$

joten $k = 0$ ja $d_j = 0$ (Huomautus 1.1.5). Siis antiteesi johtaa ristiriitaan eli väite pätee. □

Esimerkki 1.1.7 (a) Tietokoneet käyttävät kantalukuina 2:n potensseja, esim. luvut 2, 8, 16. *Binäärijärjestelmässä* kantalukuna on 2. *Heksadesimaalijärjestelmässä* eli 16-järjestelmässä luvuille $0, 1, \ldots, 15$ käytetään symboleja $0, 1, \ldots, 9, A, B, C, D, E, F$ (vastaavassa järjestyksessä). Heksadesimaaliluvut saadaan muunnetuksi 10-järjestelmään yksinkertaisesti kirjoittamalla

$$A35B0F_{16} = 10 \cdot 16^5 + 3 \cdot 16^4 + 5 \cdot 16^3 + 11 \cdot 6^2 + 0 \cdot 16 + 15 = 10705679.$$

Samaan tapaan voidaan yleisesti suorittaa muunnos b-järjestelmästä 10-järjestelmään.

(b) 10-järjestelmän luku N muunnetaan b-järjestelmään Lauseen 1.1.6 todistuksen mukaisesti:

- jaetaan N luvulla b eli kirjoitetaan yhtälö $N = bq_0 + a_0$,
- saatu kokonaisosa q_0 jaetaan edelleen b:llä eli kirjoitetaan $q_0 = bq_1 + a_0$,
- jatketaan tähän tapaan kunnes saadaan kokonaisosaksi $q_m = 0$.

Tällöin $N = (a_m a_{m-1} \ldots a_1 a_0)_b$. Käytännössä kannattaa kirjoittaa jakoyhtälöt alekkain ja poimia kertoimet a_i jakojäännöksistä alhaalta ylöspäin. Esimerkiksi luvun 143 binääriesitys saadaan kirjoittamalla

$$\begin{aligned}
143 &= 2 \cdot 71 + 1 \\
71 &= 2 \cdot 35 + 1 \\
35 &= 2 \cdot 17 + 1 \\
17 &= 2 \cdot 8 + 1 \\
8 &= 2 \cdot 4 + 0 \\
4 &= 2 \cdot 2 + 0 \\
2 &= 2 \cdot 1 + 0 \\
1 &= 2 \cdot 0 + 1
\end{aligned}$$

ja poimimalla kertoimet a_i. Siis $q_7 = 0$ ja $a_7 = 1$ eli $143 = 10001111_2$.

(c) Tietokoneiden kannalta on kätevää se, että muunnokset binäärijärjestelmästä järjestelmään jonka kantaluku on 2^i, ovat helposti toteutettavissa. Esimerkiksi

$$1111011_2 = 2^6 + 2^5 + 2^4 + 2^3 + 2^1 + 2^0 = (2^4)^1(1 + 2 + 4) + (2^4)^0(1 + 2 + 8) = 7B_{16}.$$

Vastaavalla tavalla onnistuvat muunnokset minkä hyvänsä järjestelmien välillä, joiden kantaluvut ovat b ja b^i, $b > 1$.

2 Kokonaislukujen jaollisuus

2.1 Suurin yhteinen tekijä

Jos $a \mid b$, sanomme myös että b on *jaollinen* luvulla a.

Lemma 2.1.1 (i) Jos $a \mid b$ ja $c \mid d$, niin $ac \mid bd$.

(ii) Ehdot $a \mid b$ ja $b \mid a$ ovat voimassa jos ja vain jos $a = b$ tai $a = -b$.

(iii) Jos $a \mid b_i$ kaikilla $i = 1, \ldots, n$, niin

$$a \mid b_1c_1 + \ldots + b_nc_n$$

kaikille $c_i \in \mathbf{Z}$, $i = 1, \ldots, n$.

Todistus. (i) ja (iii) harjoitustehtävä.

Todistetaan (ii): Oletetaan, että $a \mid b$ ja $b \mid a$. Tällöin on olemassa luvut k_1, $k_2 \in \mathbf{Z}$ siten, että $b = k_1a$ ja $a = k_2b$. Erityisesti $a = 0$ jos ja vain jos $b = 0$. Voidaan siis olettaa $a \neq 0$, $b \neq 0$, jolloin myös $k_1 \neq 0$, $k_2 \neq 0$. Kirjoittamalla

$$ab = (k_2b)(k_1a) = (k_1k_2)(ab),$$

ja supistamalla saadaan $k_1k_2 = 1$. Tämä on mahdollista vain silloin kun $k_1 = k_2 = 1$ tai $k_1 = k_2 = -1$. Siis $a = b$ tai $a = -b$. Käänteinen implikaatio on ilmeinen. □

Määritelmä 2.1.2 Lukujen $a_1, \ldots, a_n \in \mathbf{Z}$, joista ainakin yksi on nollasta eroava, *suurin yhteinen tekijä* $\text{syt}(a_1, \ldots, a_n)$ on luku

$$\text{syt}(a_1, \ldots, a_n) = \max\left\{k \in \mathbf{N} : \ k \mid a_i \text{ kaikilla } i = 1, \ldots, n\right\}$$

Huomautus Erityisesti

$$\text{syt}(a_1, \ldots, a_n) \leq |a_{i_0}|,$$

jos $a_{i_0} \neq 0$. Nollan mukana ololla ei ole vaikutusta suurimpaan yhteiseen tekijään. Näin on sen vuoksi, että $a \mid 0$ kaikilla $a \in \mathbf{Z}$.

Esimerkki Lukujen 12 ja 30 suurin yhteinen tekijä on 6. Tämä perustellaan Euklideen algoritmilla tai kirjoittamalla kanoniset esitykset

$$12 = 2^2 \cdot 3, \quad 30 = 2 \cdot 3 \cdot 5.$$

(perustelu myöhemmin). Luvun 6 voi kirjoittaa lukujen 12 ja 30 lineaarikombinaationa. Esimerkiksi

$$6 = 12 \cdot (-2) + 30 \cdot 1 \text{ tai } 6 = 12 \cdot 8 + 30 \cdot (-3).$$

Lineaarikombinaatioesitys ei ole yksikäsitteinen.

Lause 2.1.3 Olkoot $a_1, \ldots a_n \in \mathbf{Z}$ siten, että $a_{i_0} \neq 0$ jollekin $i_0 \in \{1, \ldots, n\}$. Tällöin

$$\text{syt}(a_1, \ldots a_n) = \min\left(\mathbf{N} \cap \left\{x_1 a_1 + \ldots + x_n a_n : x_i \in \mathbf{Z}\right\}\right).$$

Todistus. Olkoon

$$A = \mathbf{N} \cap \Big\{ \sum_{i=1}^{n} x_i a_i \;\Big|\; x_i \in \mathbf{Z} \Big\}.$$

Tällöin $A \neq \emptyset$, sillä $|a_{i_0}| \in A$. Lemman 1.1.1 nojalla A sisältää pienimmän alkion $d = \min A$. Koska $d \in A$, on olemassa $x_i \in \mathbf{Z}$ siten, että

$$d = \sum_{i=1}^{n} x_i a_i.$$

Jakoyhtälön mukaan löydetään $q_i, r_i \in \mathbf{Z}$ siten, että

$$a_i = dq_i + r_i, \quad 0 \leq r_i < d, \quad i = 1, \ldots, n.$$

Nyt

$$r_i = a_i - dq_i = a_i - \Big(\sum_{i=1}^{n} x_i a_i\Big) q_i,$$

joten jakojäännökset r_i ovat lukujen a_i lineaarikombinaatioita. Koska $0 \leq r_i < d$ ja d on A:n pienin luku, on välttämättä $r_i = 0$ kaikilla $i = 1, \ldots, n$. Siis d on eräs lukujen $a_1, \ldots, a_n$ yhteisistä tekijöistä. Olkoon $c \in \mathbf{N}$ mielivaltainen lukujen $a_1, \ldots, a_n$ yhteinen tekijä, ts. $c \mid a_i$ kaikilla $i = 1, \ldots, n$. Lemman 2.1.1 (iii) mukaan $c \mid d$, josta seuraa $c \leq d$ (Huomautus 1.1.5). □

Seuraus 2.1.4 Olkoot $a_1, \ldots a_n \in \mathbf{Z}$ siten, että $a_{i_0} \neq 0$ jollekin $i_0 \in \{1, \ldots, n\}$. Tällöin

$$\text{syt}(a_1, \ldots, a_n) = 1$$

jos ja vain jos

$$\sum_{i=1}^{n} x_i a_i = 1$$

joillekin $x_i \in \mathbf{Z}$, $i = 1, \ldots, n$.

Todistus. Implikaatio vasemmalta oikealle sisältyy Lauseen 2.1.3 väitteeseen. Jos kääntäen $\sum_{i=1}^{n} x_i a_i = 1$ joillekin $x_i \in \mathbf{Z}$, niin $1 \in \mathbf{N} \cap \{x_1 a_1 + \ldots + x_n a_n : x_i \in \mathbf{Z}\}$ ja Lauseen 2.1.3 mukaan

$$1 = \min\left(\mathbf{N} \cap \{x_1 a_1 + \ldots + x_n a_n : x_i \in \mathbf{Z}\}\right) = \text{syt}(a_1, \ldots a_n).$$

□

Esimerkki 2.1.5 (a) Jos $n \in \mathbf{N}$, niin $\text{syt}(n, n+1) = 1$. Nimittäin

$$1 = n + 1 - n = 1 \cdot (n+1) + (-1) \cdot n,$$

joten väite pätee Seurauksen 2.1.4 nojalla.

(b) Kuinka väite perustellaan jakoyhtälön avulla?

Antiteesi: On olemassa $a > 1$ siten, että $n = ak$ ja $n + 1 = ak'$ joillekin $k, k' \in \mathbf{N}$. Tällöin

$$n + 1 = ak + 1 = ak'.$$

Tämä on ristiriidassa jakoyhtälön yksikäsitteisyysväitteen kanssa, sillä jaettaessa luku $n + 1$ luvulla a on saatu kaksi erilaista jakojäännöstä 0 ja 1.

Euklideen algoritmi

Kahden luonnollisen luvun suurin yhteinen tekijä voidaan määrätä Euklideen algoritmilla seuraavasti:

Esimerkki

$$\begin{aligned} 123 &= 78{\cdot}1 + 45 \\ 78 &= 45{\cdot}1 + 33 \\ 45 &= 33{\cdot}1 + 12 \\ 33 &= 12{\cdot}2 + 9 \\ 12 &= 9{\cdot}1 + 3 \\ 9 &= 3{\cdot}3. \end{aligned}$$

Siis $\text{syt}(78, 123) = 3$.

Kun Euklideen algoritmissa edetään alhaalta ylöspäin, saadaan $3 = \text{syt}(78, 123)$ esitettyä lukujen 78 ja 123 lineaarikombinaationa kirjoittamalla

$$\begin{aligned} 3 &= 12 - 9 = 12 - (33 - 2 \cdot 12) = 3{\cdot}12 - 33 = 3(45{-}33) - 33 = 3{\cdot}45 - 4{\cdot}33 \\ &= 3{\cdot}45 - 4(78{-}45) = 7{\cdot}45 - 4{\cdot}78 = 7(123{-}78) - 4{\cdot}78 = 7{\cdot}123 - 11{\cdot}78. \end{aligned}$$

On olemassa myös laskennallisesti tehokkaampia tapoja määrätä lineaarikombinaatio, ks. esimerkiksi Rosen: Elementary number theory, s. 85.

Esimerkki 2.1.6 Euklideen algoritmi perustuu seuraavaan apuhavaintoon: Jos $a, b, c \in \mathbf{N}$, niin

$$\text{syt}(bc + a, b) = \text{syt}(a, b). \tag{1}$$

Tätä varten riittää näyttää, että joukoille

$$\begin{aligned} A_1 &:= \{\, k \in \mathbf{Z} \,:\, k \mid (bc+a) \text{ ja } k \mid b \,\}, \\ A_2 &:= \{\, k \in \mathbf{Z} \,:\, k \mid a \text{ ja } k \mid b \,\}, \end{aligned}$$

pätee $A_1 = A_2$. Jos $k \in A_2$, niin $k \mid a$ ja $k \mid b$. Lemman 2.1.1 (iii) nojalla $k \mid bc + a$. Siis $k \in A_1$ eli on todettu, että $A_2 \subset A_1$. Tällöin pätee $\text{syt}(bc + a, b) \geq \text{syt}(a, b)$. Käänteinen epäyhtälö päätellään vastaavasti Lemman 2.1.1 avulla (harjoitustehtävä).

Lause 2.1.7 (Eukleideen algoritmi) Olkoot $a > b > 0$ siten, että $b \nmid a$. Merkitään $a = r_0$, $b = r_1$, ja kirjoitetaan jakoyhtälöt

$$\begin{aligned} r_0 &= r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1, \\ r_1 &= r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_n q_{n+1} + 0. \end{aligned}$$

Tällöin $r_n = \text{syt}(a, b)$ eli $\text{syt}(a, b)$ on viimeinen nollasta eroava jakojäännös algoritmissa.

Todistus. Algoritmissa saadaan aidosti pienenevä jono jakojäännöksiä $r_0 > r_1 > r_2 > \ldots \geq 0$, joten jossakin vaiheessa saadaan $r_{n+1} = 0$.

Jos $b \nmid a$, niin Esimerkin 2.1.6 yhtälön (1) toistuva soveltaminen osoittaa, että

$$\begin{aligned} \text{syt}(a, b) = \text{syt}(r_0, r_1) &= \text{syt}(r_1 q_2 + r_2, r_1) = \text{syt}(r_1, r_2) \\ &= \text{syt}(r_2 q_2 + r_3, r_2) = \text{syt}(r_2, r_3) \\ &\vdots \\ &= \text{syt}(r_{n-1}, r_n) = \text{syt}(r_n q_{n+1}, r_n) = r_n. \end{aligned}$$

□

2.2 Fibonaccin luvut

Tarkastellaan seuraavaksi sitä, kuinka monta yhtälöä Euklideen algoritmi vaatii. Tämä tieto tarvitaan sen arviointiin kuinka paljon tietokoneaikaa algoritmin suorittaminen vaatii.

Fibonaccin lukujono (f_n) määritellään rekursiivisesti asettamalla

$$f_1 = f_2 = 1 \quad \text{ja} \quad f_{n+2} = f_{n+1} + f_n \quad \text{kaikilla } n \in \mathbf{N}.$$

Siis jonon alkupään luvut ovat $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$.

Kultainen luku *Kultaisella luvulla (kultaisella suhteella)* α tarkoitetaan yhtälön

$$\alpha^2 = \alpha + 1$$

positiivista ratkaisua

$$\alpha = \frac{1 + \sqrt{5}}{2}.$$

Kultaisella luvulla on monenlaisia yhteyksiä Fibonaccin lukujonoon. Esimerkiksi pätee:

Lemma 2.2.1 Fibonaccin luvuille

$$f_n > \alpha^{n-2}$$

kaikilla $n \geq 3$.

Todistus. Induktiotodistus (harjoitustehtävä). $\square$

Huomautus 2.2.2 Voidaan myös osoittaa, että

$$\lim_{n\to\infty} \frac{f_{n+1}}{f_n} = \alpha.$$

On helppo todeta, että α on ainoa mahdollinen raja-arvo: Jos oletetaan, että $x = \lim_{n\to\infty} \frac{f_{n+1}}{f_n}$ on olemassa, niin kirjoittamalla

$$\frac{f_{n+1}}{f_n} = \frac{f_n + f_{n-1}}{f_n} = 1 + \frac{f_{n-1}}{f_n} = 1 + \frac{1}{f_n/f_{n-1}}$$

ja ottamalla raja-arvot puolittain, saadaan

$$x = 1 + \frac{1}{x} \quad \text{eli} \quad x^2 = x + 1.$$

Tässä on helppo nähdä, että $1 \leq x \leq 2$. Näin ollen ratkaisu on $x = \alpha$, sillä toinen ratkaisu $\beta := \frac{1-\sqrt{5}}{2}$ on negatiivinen. Raja-arvon olemassaolo ei ole kuitenkaan triviaalia!

Binet'n kaavana tunnettu tulos sanoo, että

$$f_n = \frac{1}{\sqrt{5}} \left(\alpha^n - \beta^n\right).$$

Fibonaccin luvuilla (ja niiden yleistyksillä Lucas-luvuilla) on runsaasti mielenkiintoisia analyyttisiä ja lukuteoreettisia ominaisuuksia.

Lause 2.2.3 (Lame'n lause) Olkoot $a > b > 0$. Tällöin luvun $\text{syt}(a, b)$ määrääminen Euklideen algoritmilla vaatii korkeintaan $5k$ jakoyhtälöä, missä k on desimaalien lukumäärä kokonaisluvun b 10-järjestelmäesityksessä.

Todistus. Olkoot $r_0 = a$, $r_1 = b$. Euklideen algoritmin suorittaminen vaatii jakoyhtälöt

$$\begin{aligned}
r_0 &= r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_n q_{n+1} + 0.
\end{aligned}$$

Siis tarvittavia yhtälöitä on n kappaletta. Havaitaan, että kertoimille q_i pätee yleisesti $q_i \geq 1$ ja erityisesti $q_{n+1} \geq 2$. Jos nimittäin $q_i \leq 0$ jollekin $i = 1, \ldots, n-1$, niin

$$r_{i-2} = r_{i-1} q_i + r_i \leq r_i,$$

mikä on ristiriita sen kanssa, että jakojäännökset muodostavat aidosti laskevan jonon. Samoin, jos $q_{n+1} \leq 1$, niin tapauksessa $q_{n+1} = 1$ päädytään ristiriitaan $r_{n-1} = r_n q_{n+1} = r_n$ ja tapauksessa $q_{n+1} \leq 0$ päädytään ristiriitaan $r_{n-1} = r_n q_{n+1} \leq 0$.

Näin ollen

$$\begin{aligned} r_n &\geq 1 = f_2, \\ r_{n-1} &\geq 2r_n \geq 2f_2 = f_3, \\ r_{n-2} &\geq r_{n-1} + r_n \geq f_3 + f_2 = f_4, \\ &\vdots \\ r_2 &\geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n, \\ b &= r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}. \end{aligned}$$

Siis $b \geq f_{n+1}$. Lemman 2.2.1 mukaan $f_{n+1} > \alpha^{n-1}$, joten yhdistämällä epäyhtälöt saadaan $b > \alpha^{n-1}$. Koska $\log_{10} \alpha > \frac{1}{5}$, päädytään arvioon

$$\log_{10} b > (n-1) \log_{10} \alpha > \frac{n-1}{5}$$

ottamalla $\log_{10}$ puolittain. Siis $n - 1 < 5 \log_{10} b$. Lopuksi, jos luvulla b on k desimaaliyksikköä, niin $b < 10^k$, ja siis

$$\log_{10} b < k \log_{10} 10 = k.$$

Siis $n - 1 < 5k$, joten $n \leq 5k$. $\square$

Jo Lame'n lauseesta voi päätellä, että Euklideen algoritmi on varsin nopea suorittaa tietokoneella. Siitä on myös olemassa parannettuja nopeampia versioita.

Huomautus 2.2.4 Useamman luvun suurin yhteinen tekijä voidaan määrätä Euklideen algoritmin ja rekursiokaavan

$$syt(a_1, \ldots, a_n) = syt(a_1, \ldots, a_{n-2}, syt(a_{n-1}, a_n)) \tag{2}$$

avulla.

2.3 Alkuluvut ja tekijöihin jako

Määritelmä 2.3.1 Luku $a > 1$ on *alkuluku*, jos sillä on vain triviaalit tekijät ± 1 ja $\pm a$. Lukua $a > 1$ sanotaan *yhdistetyksi*, jos a ei ole alkuluku.

Seuraava yksinkertainen jaollisuuslemma on keskeinen.

Lemma 2.3.2 (Eukleideen lemma) Jos $a \mid bc$ ja $\text{syt}(a, b) = 1$, niin $a \mid c$.

Todistus. Koska $\text{syt}(a, b) = 1$, on olemassa kokonaisluvut u ja v, joille $au + bv = 1$. Kun tämä yhtälö kerrotaan luvulla c, saadaan $cau + cbv = c$. Koska $a \mid bc$, on $bc = ra$ jollekin $r \in \mathbf{Z}$ ja siten

$$c = cau + cbv = cau + (ra)v = a(cu + rv).$$

Siis $a \mid c$. $\square$

Lemma 2.3.3 Luonnollinen luku $p \geq 2$ on alkuluku jos ja vain jos kaikilla $a, b \in \mathbf{N}$ pätee implikaatio

$$p \mid ab \quad \Longrightarrow \quad p \mid a \text{ tai } p \mid b. \tag{3}$$

Todistus. Oletetaan ensin, että p on alkuluku. Olkoot a, $b \in \mathbf{N}$ sellaisia, että $p \mid ab$. Koska p on alkuluku, on joko $\text{syt}(p, a) = 1$ tai $\text{syt}(p, a) = p$. Jos $\text{syt}(p, a) = p$, niin $p \mid a$. Jos taas $\text{syt}(p, a) = 1$, saadaan Lemman 2.3.2 mukaan $p \mid b$.

Oletetaan kääntäen, että implikaatio (3) pätee kaikilla $a, b \in \mathbf{N}$.

Antiteesi: p ei ole alkuluku. Antiteesin seurauksena luvulla p on esitys $p = st$, missä $1 < s < p$ ja $1 < t < p$. Koska $p \mid st$, niin implikaation (3) mukaan $p \mid s$ tai $p \mid t$. Tällöin $p \leq s$ tai $p \leq t$, mikä on ristiriita. □

Huomautus Olennaista on, että alkuluvun tapauksessa implikaatio (3) pätee kaikilla $a, b \in \mathbf{N}$. Esimerkiksi, jos $p = 4,\ a = 8,\ b = 3$, niin $p \mid ab$ ja $p \mid a$, joten implikaatio pätee valituille a, b vaikka $p = 4$ ei ole alkuluku. Kuitenkin esimerkiksi ehdosta $4 \mid 60$ ***ei seuraa***, että $4 \mid 6$ tai $4 \mid 10$.

Seuraus 2.3.4 Jos p on alkuluku ja $a_1, \ldots, a_n \in \mathbf{N}$ siten, että $p \mid a_1 a_2 \cdots a_n$, niin $p \mid a_i$ jollakin $i = 1, \ldots, n$.

Todistus. Induktiolla (harjoitustehtävä). □

Lause 2.3.5 (Aritmetiikan peruslause) Jokainen luonnollinen luku $n \geq 2$ on esitettävissä järjestetystä vaille yksikäsitteisellä tavalla tulona

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, \tag{4}$$

missä p_i:t ovat eri alkulukuja ja $a_i \in \mathbf{N}$.

Todistus. Olemassaolo: Olkoon S niiden luonnollisten lukujen joukko, jotka eivät ole alkulukujen tuloja. Osoitetaan, että S on tyhjä joukko.

Antiteesi: S on epätyhjä. Tällöin joukossa S on pienin alkio m. Koska $m \in S$, m ei ole alkuluku, joten $m = ab$ joillekin $1 < a < m$ ja $1 < b < m$. Silloin $a \notin S$ ja $b \notin S$, koska m on joukon S pienin alkio. Näin ollen a ja b ovat esitettävissä alkulukujen tuloina. Mutta tällöin myös $m = ab$ on alkulukujen tulo, mikä on ristiriita. Siis S on tyhjä joukko.

Yksikäsitteisyys: Antiteesi: On olemassa luonnollisia lukuja, joilla on kaksi erilaista alkutekijäesitystä. Olkoon m pienin tällainen luku. Siis

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = m = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}, \tag{5}$$

missä vasemman- ja oikeanpuoleiset esitykset ovat erit. Nyt $p_1 \mid q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$, joten Seurauksen 2.3.4 nojalla $p_1 \mid q_i$ jollekin $i = 1, 2, \ldots, s$. Näin ollen $q_i = k p_1$ jollekin $k \in \mathbf{N}$. Mutta p_1 ja q_i ovat alkulukuja, joten välttämättä $k = 1$ ja siis $p_1 = q_i$. Jaetaan esitys (5) luvulla $p_1 = q_i$, jolloin

$$m' := \frac{m}{p_1} = p_1^{a_1 - 1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{a_1} \cdots q_i^{a_i - 1} \cdots q_s^{a_s}.$$

Nyt m' on luku, jolle ylläolevat kaksi alkutekijäesitystä ovat erilaiset (jos näin ei olisi, myös luvun m esitykset olisivat samanlaiset). Koska $m' < m$, on päädytty ristiriitaan luvun m valinnan kanssa. □

Esitystä (4) kutsutaan luvun n *kanoniseksi esitykseksi* tai *alkutekijäesitykseksi*.

Esimerkki 2.3.6 Jo antiikin kreikkalaiset tunsivat lukuteoreettisen todistuksen sille, että $\sqrt{2}$ on irrationaalinen. Todistetaan tässä yleisempi väite: Olkoon α algebrallisen yhtälön

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0$$

reaalinen ratkaisu, missä $c_i \in \mathbf{Z}$. Tällöin joko α on kokonaisluku tai irrationaalinen.

Perustelu: Oletetaan, että $\alpha \in \mathbf{Q}$ ja osoitetaan, että $\alpha \in \mathbf{Z}$. Esitetään α supistetussa muodossa $\alpha = \frac{a}{b}$, missä $\text{syt}(a, b) = 1$ ja $b \neq 0$. Sijoittamalla α yhtälöön saadaan

$$(a/b)^n + c_{n-1}(a/b)^{n-1} + \cdots + c_1(a/b) + c_0 = 0.$$

Kertomalla puolittain luvulla b^n saadaan

$$a^n + c_{n-1}a^{n-1}b + \cdots c_1 a b^{n-1} + c_0 b^n = 0.$$

Tästä seuraa, että $b \,|\, a^n$. Oletetaan, että $b \neq \pm 1$. Tällöin luvulla b on alkutekijä p. Koska $p \,|\, b$ ja $b \,|\, a^n$, niin $p \,|\, a^n$. Seurauksen 2.3.4 nojalla $p \,|\, a$, mikä on ristiriidassa oletuksen $\text{syt}(a, b) = 1$ kanssa (sillä $p \,|\, b$). Siis $b = \pm 1$ eli $\alpha = \pm a$.

Väitteen nojalla esimerkiksi luvut $\sqrt{3}$, $\sqrt[3]{5}$ ja $\sqrt[10]{17}$ ovat irrationaalisia. Nimittäin nämä ovat yhtälön $x^n = a$, $a \in \mathbf{Z}$, ratkaisuja, mutta eivät ole kokonaislukuja.

Esimerkki Suurin yhteinen tekijä löydetään kätevästi kanonisen esityksen avulla, jos ne ovat käytettävissä. Esimerkiksi

$$200 = 2^3 \cdot 5^2 \quad \text{ja} \quad 420 = 2^2 \cdot 3 \cdot 5 \cdot 7.$$

Poimimalla korkeimmat yhteiset alkutekijäpotenssit esityksistä saadaan

$$\text{syt}(200, 420) = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 20.$$

Lemma 2.3.7 (S.y.t. kanonisen esityksen avulla) Olkoot $a_1, \ldots, a_n \in \mathbf{N}$ ja olkoon

$$a_i = \prod_{j=1}^{k} p_j^{m_{ij}} \tag{6}$$

luvun a_i modifioitu kanoninen esitys siten, että joukko $\{\, p_1, \ldots, p_k \,\}$ koostuu kaikista lukujen $a_1, \ldots, a_n$ alkutekijöistä ja $m_{ij} = 0$ mikäli $p_j \nmid a_i$. Tällöin

$$\text{syt}(a_1, \ldots, a_n) = \prod_{j=1}^{k} p_j^{\min\{\, m_{ij} | i=1,\ldots,n \,\}}. \tag{7}$$

Todistus. Merkitään

$$d := \prod_{j=1}^{k} p_j^{min\{\, m_{ij} | i=1,\ldots,n \,\}}.$$

On selvää, että $d \,|\, a_i$ kaikilla $i = 1, \ldots, n$. Siis d on eräs lukujen $a_1, \ldots, a_n$ yhteinen tekijä. Olkoon $c \in \mathbf{N}$ siten, että $c \,|\, a_i$ kaikilla $i = 1, \ldots, n$. Siis $a_i = s_i c$ kaikilla $i = 1, \ldots, n$, joten luvulla c ei ole alkutekijöitä, jotka eivät esiintyisi joukossa $\{\, p_1, \ldots, p_k \,\}$. Olkoon

$$c = \prod_{j=1}^{k} p_j^{m_j}$$

luvun c muotoa (6) oleva modifioitu kanoninen esitys. Ehdosta $a_i = s_i c$ ja kanonisen esityksen yksikäsitteisyydestä seuraa, että $m_j \leq m_{ij}$ kaikilla i ja j. Siispä

$$m_j \leq \min\{\, m_{ij} \mid i = 1, \ldots, n \,\},$$

joten $c \leq d$. $\square$

Määritelmä 2.3.8 Lukujen $a_1, \ldots, a_n \in \mathbf{N}$ *pienin yhteinen monikerta* $\text{pym}(a_1, \ldots, a_n)$ on luku

$$\text{pym}(a_1, \ldots, a_n) := \min\{\, k \in \mathbf{N} : a_i \,|\, k \text{ kaikilla } i = 1, \ldots, n \,\}.$$

Huomautus Määritelmässä esiintyvä joukko on epätyhjä, sillä $a_i \,|\, (a_1 \cdots a_n)$ kaikilla $i = 1, \ldots, n$. Erityisesti

$$\text{pym}(a_1, \ldots, a_n) \leq a_1 \cdots a_n.$$

Matkimalla Lemman 2.3.7 todistusta todetaan (tarkastelu sivuutetaan):

Lemma 2.3.9 (P.y.m. kanonisen esityksen avulla) Olkoot $a_1, \ldots, a_n \in \mathbf{N}$ ja olkoon

$$a_i = \prod_{j=1}^{k} p_j^{m_{ij}}$$

luvun a_i modifioitu kanoninen esitys, missä alkutekijäjoukko $\{\, p_1, \ldots, p_k \,\}$ koostuu kaikista lukujen $a_1, \ldots, a_n$ alkutekijöistä ja $m_{ij} = 0$ mikäli $p_j \nmid a_i$. Tällöin

$$\text{pym}(a_1, \ldots, a_n) = \prod_{j=1}^{k} p_j^{\max\{\, m_{ij} \mid i = 1, \ldots, n \,\}}.$$

Esimerkki Siis esimerkiksi kanonisista esityksistä

$$200 = 2^3 \cdot 3^0 \cdot 5^2 \cdot 7^0, \quad 420 = 2^2 \cdot 3 \cdot 5 \cdot 7,$$

poimimalla saadaan $\text{pym}(200, 420) = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1 = 4200$.

Yhdistämällä lemmat 2.3.7 ja 2.3.9 todetaan:

Seuraus 2.3.10 Olkoot $a, b \in \mathbf{N}$. Tällöin

$$\text{syt}(a, b) \cdot \text{pym}(a, b) = ab.$$

Todistus. Harjoitustehtävä. $\square$

Huomautus Seurauksen tulos *ei päde* useammalle kuin kahdelle alkiolle.

2.4 Alkulukujen jakaantumisesta

Jo Eukleides osasi päätellä, että alkulukuja on ääretön määrä. Hänen ideansa yleistää sen havainnon, että esimerkiksi luvut

$$p = 2 \cdot 3 \cdot 5 + 1 = 31 \quad \text{ja} \quad p = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$$

ovat alkulukuja, ks. harjoitustehtävä.

Esimerkki 2.4.1 (a) Dirichlet todisti seuraavan tuloksen: Jos $a, b \in \mathbf{N}$ toteuttavat ehdon $\text{syt}(a, b) = 1$, niin aritmeettinen lukujono $(an + b)_{n \in \mathbf{N}}$ sisältää äärettömän määrän alkulukuja.

Todistetaan väite erikoistapauksessa $a = 4$, $b = 3$. Osoitetaan ensin, että tulo qr on muotoa $4n + 1$ jos sekä q että r ovat muotoa $4n + 1$. Olkoot $q = 4n_1 + 1$ ja $r = 4n_2 + 1$. Tällöin

$$qr = (4n_1 + 1)(4n_2 + 1) = 16n_1n_2 + 4n_1 + 4n_2 + 1 = 4(4n_1n_2 + n_1 + n_2) + 1,$$

joten väite pätee.

Tehdään antiteesi: Muotoa $4n + 3$ olevia alkulukuja on vain äärellinen määrä. Olkoot $p_0 = 3$, $p_1, \ldots, p_r$ nämä alkuluvut ja olkoon

$$Q := 4p_1 \cdots p_r + 3.$$

Tällöin luvulla Q on ainakin yksi alkutekijä muotoa $4n + 3$. Jos nimittäin näin ei ole, eli kaikki alkutekijät ovat muotoa $4n + 1$, niin myös Q on muotoa $4n + 1$ alkuosan perusteella. Tällöin

$$Q = 4p_1 \cdots p_r + 3 = 4n + 1,$$

mikä on ristiriidassa jakoyhtälön yksikäsitteisyysväitteen kanssa.

Riittää osoittaa, että mikään alkuluvuista $p_0, p_1, \ldots, p_r$ ei jaa lukua Q. Luku 3 ei jaa lukua Q, sillä jos $3 \mid Q$, niin $3 \mid Q - 3$ eli

$$Q - 3 = p_1 \cdots p_r = 3k,$$

mikä on ristiriidassa kanonisen esityksen yksikäsitteisyyden kanssa. Toisaalta, jos $i = 1, \ldots, r$, niin p_i ei jaa lukua Q, sillä jos $p_i \mid Q$, niin $p_i \mid Q - 4p_1 \cdots p_r$ eli

$$3 = Q - 4p_1 \cdots p_r = p_1k,$$

mikä on ristiriita. Väite on todistettu.

(b) Kaikilla $n \in \mathbf{N}$ on olemassa n peräkkäistä yhdistettyä lukua. Esimerkiksi luvut

$$(n + 1)! + 2, (n + 1)! + 3, \ldots, (n + 1)! + n + 1$$

ovat yhdistettyjä, sillä jos $2 \leq j \leq n + 1$, niin $j \mid (n + 1)!$ ja siis $j \mid (n + 1)! + j$.

Huomautus 2.4.2 (a) Jos p_n on n:s alkuluku, niin

$$\sum_{n=1}^{\infty} \frac{1}{p_n} = \infty,$$

ts. alkulukujen käänteisluvuista muodostettu sarja hajaantuu. Tämän todisti ensimmäisenä Euler.

(b) Eulerin tulos voidaan edelleen parantaa muotoon: On olemassa vakiot c_1, c_2 s.e.

$$c_1 \log\,(\log\ k) \leq \sum_{n=1}^{k} \frac{1}{p_n} \leq c_2 \log\,(\log\ k).$$

Siis Eulerin sarjan osasummat kasvavat olennaisesti "samaa vauhtia"kuin $\log\,(\log\ k)$.

(c) Alkulukulauseen nimellä tunnettu tulos sanoo, että lukumääräfunktio

$$\Pi(n) := \text{ niiden alkulukujen lukumäärä, jotka ovat} \leq n$$

toteuttaa ehdon

$$\lim_{n\to\infty} \frac{\Pi(n)}{n} \cdot \log\ n = 1.$$

Alkulukulauseen todistivat ensimmäisenä Hadamard ja de la Vallee-Ponsiu 1896 kompleksianalyysin avulla. Selberg esitti 1949 alkulukulauseelle "alkeellisen"todistuksen (=todistus, joka ei käytä kompleksianalyysiä).

(d) Kuuluisa todistamaton *Goldbachin konjektuuri* sanoo, että jokainen parillinen kakkosta suurempi luku voidaan esittää kahden alkuluvun summana. Esimerkiksi

$$10 = 5 + 5 = 3 + 7,\ 24 = 5 + 19 = 7 + 17 = 11 + 13.$$

(e) Toinen kuuluisa todistamaton konjektuuri sanoo, että alkulukukaksosia on ääretön määrä. Alkulukukaksosista puhutaan silloin, kun molemmat luvut $6k \pm 1$ ovat alkulukuja, $k \in \mathbf{N}$.

3 Kongruenssi

3.1 Kongruenssirelaation perusominaisuudet

Jatkossa $m \in \mathbf{N}$ on ns. *moduloluku* ellei toisin ilmoiteta.

Määritelmä 3.1.1 Olkoon $m \in \mathbf{N}$ ja olkoot $a, b \in \mathbf{Z}$. Tällöin a on *kongruentti luvun b kanssa modulo m*,

$$a \equiv b\,(\bmod m),$$

jos $m \mid a - b$. Jos $m \nmid a - b$, merkitään $a \not\equiv b\,(\bmod m)$.

Esimerkki Esimerkiksi $4 \equiv 1\,(\bmod 3)$, $4 \equiv 4\,(\bmod 3)$, $4 \equiv 7\,(\bmod 3)$, $4 \equiv 10\,(\bmod 3)$, jne.

Huomautus Jos $m \in \mathbf{N}$ ja $a \in \mathbf{Z}$, niin $m \mid a$ jos ja vain jos $a \equiv 0\,(\bmod m)$. Yleisesti, jakoyhtälö $a = qm + r$ pätee jos ja vain jos $a \equiv r\,(\bmod m)$. Jos tässä $0 \leq r < m$, sanomme lukua r a:n *jakojäännökseksi modulo m*.

Lemma 3.1.2 (Kongruenssi on ekvivalenssi) Olkoot $a, b, c, d \in \mathbf{Z}$. Tällöin

(i) $a \equiv a \,(\mathrm{mod}\, m)$ ***(refleksiivisyys),***

(ii) Jos $a \equiv b \,(\mathrm{mod}\, m)$, niin $b \equiv a \,(\mathrm{mod}\, m)$ ***(symmetrisyys),***

(iii) Jos $a \equiv b \,(\mathrm{mod}\, m)$ ja $b \equiv c \,(\mathrm{mod}\, m)$, niin $a \equiv c \,(\mathrm{mod}\, m)$ ***(transitiivisuus).***

Todistus. Todistetaan malliksi (iii). Jos $a \equiv b \,(\mathrm{mod}\, m)$ ja $b \equiv c \,(\mathrm{mod}\, m)$, niin $m \mid a - b$ ja $m \mid b - c$. Siis on olemassa $k_1, k_2 \in \mathbf{Z}$ siten, että $a - b = k_1 m$ ja $b - c = k_2 m$. Laskemalla yhtälöt yhteen saadaan $a - c = (k_1 + k_2)m$. Siis $m \mid a - c$ eli $a \equiv c \,(\mathrm{mod}\, m)$. $\square$

Lemma 3.1.3 (Kongruenssiaritmetiikan perussäännöt) Olkoot $a, b, c, d \in \mathbf{Z}$. Tällöin

(i) $a \equiv b \,(\mathrm{mod}\, m)$ ja $c \equiv d \,(\mathrm{mod}\, m) \;\Rightarrow\; a + c \equiv b + d \,(\mathrm{mod}\, m)$,

(ii) $a \equiv b \,(\mathrm{mod}\, m)$ ja $c \equiv d \,(\mathrm{mod}\, m) \;\Rightarrow ac \equiv bd \,(\mathrm{mod}\, m)$.

Todistus. Harjoitustehtävä. $\square$

Esimerkki 3.1.4 (a) Erityisesti kongruenssiyhtälöön voidaan lisätä puolittain kokonaisluku ja kongruenssiyhtälö voidaan kertoa puolittain kokonaisluvulla. Induktiolla päätellään, että

$$a \equiv b \,(\mathrm{mod}\, m) \Rightarrow a^k \equiv b^k \,(\mathrm{mod}\, m)$$

kaikilla $k \in \mathbf{N}$: Jos implikaatio pätee arvolla k, niin kertomalla yhtälöt $a \equiv b \,(\mathrm{mod}\, m)$ ja $a^k \equiv b^k \,(\mathrm{mod}\, m)$ puolittain saadaan implikaatio indeksin arvolla $k + 1$.

(b) Kohdan (a) nojalla pätee esimerkiksi: Koska $2 \equiv 5 \,(\mathrm{mod}\, 3)$, niin $2^{100} \equiv 5^{100} \,(\mathrm{mod}\, 3)$ ja edelleen

$$2^{100} + 5 \equiv 5^{100} + 2 \,(\mathrm{mod}\, 3).$$

Kongruenssiyhtälössä *ei yleisesti* päde tulon supistussääntö. Esimerkiksi

$$14 \equiv 8 \,(\mathrm{mod}\, 6) \quad \text{eli} \quad 7 \cdot 2 \equiv 4 \cdot 2 \,(\mathrm{mod}\, 6).$$

Kuitenkin $7 \not\equiv 4 \,(\mathrm{mod}\, 6)$ eli lukua 2 ei voi supistaa pois. Supistussääntö pätee kuitenkin seuraavassa muodossa.

Lause 3.1.5 (Tulon supistussääntö) Olkoot $a, b, c \in \mathbf{Z}$. Tällöin

$$ac \equiv bc \,(\mathrm{mod}\, m) \;\Rightarrow\; a \equiv b \left(\mathrm{mod}\, \frac{m}{syt(m, c)}\right).$$

Erityisesti, jos $syt(m, c) = 1$, niin supistussääntö

$$ac \equiv bc \,(\mathrm{mod}\, m) \;\Rightarrow a \equiv b \,(\mathrm{mod}\, m)$$

pätee.

Esimerkki Soveltamalla Lausetta 3.1.5 yhtälöön $2 \cdot 7 \equiv 2 \cdot 4 \,(\mathrm{mod}\, 6)$ saadaan

$$7 \equiv 4 \left(\mathrm{mod}\, \frac{6}{\mathrm{syt}(6, 2)}\right).$$

Lauseen 3.1.5 todistamiseksi tarvitaan aputulos:

Lemma 3.1.6 Olkoot $a_1, \ldots, a_n \in \mathbf{Z}$ siten, että $a_{i_0} \neq 0$ jollekin i_0 ja olkoon $d = syt(a_1, \ldots, a_n)$. Tällöin

$$\text{syt}\Big(\frac{a_1}{d}, \ldots, \frac{a_n}{d}\Big) = 1.$$

Todistus. Lauseen 2.1.3 mukaan

$$d = \sum_{i=1}^{n} a_i x_i$$

joillekin $i = 1, \ldots, n$. Jakamalla lineaarikombinaatio luvulla d saadaan

$$1 = \frac{d}{d} = \sum_{i=1}^{n} (\frac{a_i}{d}) x_i.$$

Tässä $\frac{a_i}{d} \in \mathbf{Z}$, sillä $d \,|\, a_i$ kaikilla i. Väite pätee Seurauksen 2.1.4 nojalla. □

Lauseen 3.1.5 todistus. Olkoon $d = syt(m, c)$. Koska $ac \equiv bc \pmod m$, niin $m \mid ac - bc$. Siis $(a-b)c = km$ jollekin $k \in \mathbb{Z}$. Jakamalla puolittain luvulla d saadaan

$$(a-b)\frac{c}{d} = k \cdot \frac{m}{d}.$$

Tässä $\frac{c}{d}, \frac{m}{d} \in \mathbf{Z}$, sillä $d = syt(m, c)$. Siis $\frac{m}{d} \mid (a-b)\frac{c}{d}$. Lemman 3.1.6 mukaan $syt(\frac{m}{d}, \frac{c}{d}) = 1$, joten Lemman 2.3.2 nojalla $\frac{m}{d} \,|\, a - b$. Siis $a \equiv b \,(\bmod \frac{m}{d})$.

Kongruenssiluokat modulo m

Olkoon $m \in \mathbf{N}$ ja $a \in \mathbf{Z}$. Tällöin joukkoa

$$[a] = [a]_m := \{\, k \in \mathbf{Z} \mid k \equiv a \,(\bmod m) \,\}$$

kutsutaan luvun a *määräämäksi kongruenssiluokaksi modulo* m (tai luvun a *määräämäksi jäännösluokaksi modulo* m).

Esimerkki Jos $m = 3$, niin

$$\begin{aligned}
[0] &= \{\cdots -6, -3, 0, 3, 6, 9, \ldots\} = [3], \\
[1] &= \{\cdots -5, -2, 1, 4, 7, 10, \ldots\} = [4], \\
[2] &= \{\cdots -4, -1, 2, 5, 8, 11, \ldots\} = [5].
\end{aligned}$$

Jakoyhtälöstä seuraa, että kongruenssirelaatiossa modulo m erillisiä ekvivalenssiluokkia on täsmälleen m kappaletta:

Lause 3.1.7 Jokaisella $m \in \mathbf{N}$ luokat $[0]$, $[1]$, …, $[m-1] \,(\bmod m)$ ovat pareittain pistevieraita ja niiden yhdiste on $\mathbf{Z}$.

Todistus. Olkoon $k \in \mathbf{Z}$ mielivaltainen. Jakoyhtälön mukaan on olemassa $q, r \in \mathbf{Z}$ siten, että

$$k = qm + r, \quad 0 \leq r < m.$$

Tällöin $k \in [r]$, sillä $k \equiv r \,(\bmod m)$. Siis $k \in [r]$ jollakin $r = 0, 1, \ldots, m-1$, joten $\mathbf{Z} \subseteq [0] \cup \cdots \cup [m-1]$. Käänteinen inkluusio on triviaali. Pareittain pistevierautta koskeva väite harjoitustehtävä. □

3.2 Lineaarinen kongruenssi

Muotoa

$$ax \equiv b \ (\mathrm{mod}\, m) \tag{8}$$

olevaa kongruenssia, missä $a, b \in \mathbf{Z}$ ja $n \in \mathbf{N}$ ovat annettuja, sanotaan *(yhden muuttujan) lineaariseksi kongruenssiyhtälöksi*.

Huomautus 3.2.1 (i) Jos $ax_1 \equiv b \ (\mathrm{mod}\ m)$ ja $x_1 \equiv x_2 \ (\mathrm{mod}\ m)$, niin $ax_1 \equiv ax_2 \ (\mathrm{mod}\ m)$ ja edelleen symmetrisyyden ja transitiivisuuden nojalla $ax_2 \equiv b \ (\mathrm{mod}\ m)$.

(ii) Jos $ax_1 \not\equiv b \ (\mathrm{mod}\ m)$ ja $x_1 \equiv x_2 \ (\mathrm{mod}\ m)$, niin $ax_2 \not\equiv b \ (\mathrm{mod}\ m)$. Nimittäin olettamalla, että $ax_2 \equiv b \ (\mathrm{mod}\ m)$ saadaan $ax_1 \equiv b \ (\mathrm{mod}\ m)$ kuten kohdassa (i).

Kohtien (i) ja (ii) nojalla joko annetun kongruenssiluokan modulo m kaikki luvut ovat yhtälön (8) ratkaisuja tai yksikään kongruenssiluokan luvuista ei ole ratkaisu. Erityisesti yhtälön (8) ratkaisut voivat olla yksikäsitteisiä vain kongruenssiluokan mielessä.

Esimerkki Luvun x jakojäännös mod m toteuttaa ehdon $x \equiv r \ (\mathrm{mod}\ m)$. Siksi Huomautuksen 3.2.1 nojalla yhtälön (8) ratkaisemiseksi riittää tutkia kaikki mahdolliset jakojäännökset, so. luvut $0, 1, \ldots, m-1$. Esimerkiksi kokeilemalla havaitaan, että luvuista $0, 1, \ldots, 11$ ainoastaan 3 ja 9 toteuttavat yhtälön

$$2x \equiv 6 \ (\mathrm{mod}\ 12).$$

Kaikkien ratkaisujen joukko on siis $[3] \cup [9]$. Vastaavasti todetaan kokeilemalla, että yksikään luvuista $0, 1, \ldots, 11$ ei toteuta yhtälöä

$$4x \equiv 6 \ (\mathrm{mod}\ 12).$$

Näin ollen yhtälöllä ei ole lainkaan ratkaisuja.

Lause 3.2.2 Olkoon $m \in \mathbf{N}$ ja olkoot $a, b \in \mathbf{Z}$ siten, että $a \not\equiv 0 \ (\mathrm{mod}\, m)$ ja $d = syt(a, m)$. Tällöin

(i) Jos $d \nmid b$, kongruenssilla $ax \equiv b \ (\mathrm{mod}\ m)$ ei ole ratkaisuja.

(ii) Jos $d \mid b$, niin kongruenssin $ax \equiv b \ (\mathrm{mod}\ m)$ ratkaisujoukko on d:n kongruenssiluokan yhdiste.

Lauseen 3.2.2 lineaarinen kongruenssi palautuu klassisen *Diofantoksen yhtälön*

$$ax + by = c$$

ratkaisemiseen. Tässä $a, b, c \in \mathbf{Z}$ ovat annettuja ja tarkoitus on löytää $x, y \in \mathbf{Z}$, jotka toteuttavat yhtälön.

Esimerkki 3.2.3 Tarkastellaan yhtälöä $2x \equiv 7 \ (\mathrm{mod}\, 1111)$. Tämä pätee jos ja vain jos $1111 \mid 2x - 7$ mikä pätee jos ja vain jos

$$2x + 1111y = 7$$

joillekin $x, y \in \mathbf{Z}$. Selvästi $syt(2, 1111) = 1$, joten on olemassa $x', y' \in \mathbf{Z}$, joille $2x' + 1111y' = 1$. Kertomalla yhtälö puolittain luvulla 7 saadaan

$$7 = 2(7x') + 1111(7y'),$$

joten $x = 7x'$ ja $y = 7y'$ ovat eräät ratkaisut. Siis ratkaisuun päädytään suurimpaan yhteiseen tekijään liittyvän lineaarikombinaation kautta. Tämän löytämiseksi kirjoitetaan Euklideen algoritmi

$$\begin{aligned} 1111 &= 555 \cdot 2 + 1, \\ 2 &= 2 \cdot 1 + 0, \end{aligned}$$

josta saadaan $1 = 1111 - 2 \cdot 555$. Siis $7 = 2(-3885) + 1111 \cdot 7$ eli $x' = -3885$ ja $y' = 7$ on eräs tarkasteltavan Diofantoksen yhtälön ratkaisuista

Lause 3.2.4 Olkoot $a, b \in \mathbf{Z} \setminus \{0\}$, $c \in \mathbf{Z}$ ja $d = syt(a, b)$.

(i) Jos $d \nmid c$, niin yhtälöllä

$$ax + by = c \tag{9}$$

ei ole ratkaisuja $x, y \in \mathbf{Z}$.

(ii) Jos $d \mid c$, niin yhtälöllä (9) on ratkaisuja siten, että mikäli $x_0, y_0 \in \mathbf{Z}$ on eräs ratkaisu, niin kaikki ratkaisut $x, y \in \mathbf{Z}$ saadaan yhtälöistä

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n, \quad n \in \mathbf{Z}. \tag{10}$$

Todistus. (i) Oletetaan vastoin väitettä, että luvuille $x, y \in \mathbf{Z}$ pätee $ax + by = c$. Koska $d \mid a$ ja $d \mid b$, niin $d \mid ax + by$ eli $d \mid c$. Tämä on ristiriidassa oletuksen kanssa.

(ii) Olkoon $d \mid c$. Lauseen 2.1.3 mukaan $d = as + bt$ joillekin $s, t \in \mathbf{Z}$. Koska $d \mid c$, niin $c = kd$ ja siis

$$c = kd = k(as + bt) = a(ks) + b(kt).$$

Näin ollen yhtälöllä (9) on ainakin ratkaisu $x_0 = ks$, $y_0 = kt$.

Osoitetaan seuraavaksi, että kaikki muotoa (10) olevat lukuparit ovat ratkaisuja. Olkoot

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n,$$

jollekin $n \in \mathbf{Z}$. Tällöin

$$ax + by = a(x_0 + \frac{b}{d}n) + b(y_0 - \frac{a}{d}n) = ax_0 + \frac{ab}{d}n + by_0 - \frac{ab}{d}n = ax_0 + by_0 = c.$$

Siis x, y on ratkaisu.

Näytetään lopuksi, että muita kuin muotoa (10) olevia ratkaisuja ei ole. Olkoon $au + bv = c$ joillekin $u, v \in \mathbf{Z}$. Tällöin

$$au + bv = ax_0 + by_0,$$

joten

$$a(u - x_0) = b(y_0 - v)$$

ja edelleen

$$\frac{a}{d}(u - x_0) = \frac{b}{d}(y_0 - v).$$

Koska $syt(\frac{a}{d}, \frac{b}{d}) = 1$ (Lemma 3.1.6), saadaan Lemman 2.3.2 nojalla, että $\frac{a}{d} \mid y_0 - v$. Siis jollekin $n \in \mathbf{Z}$ pätee $\frac{a}{d} \cdot n = y_0 - v$ eli $v = y_0 - \frac{a}{d}n$. Sijoittamalla v yhtälöön $a(u - x_0) = b(y_0 - v)$ saadaan edelleen

$$a(u - x_0) = b\Big(y_0 - (y_0 - \frac{a}{d}n)\Big) = \frac{ba}{d}n,$$

joten jakamalla a:lla seuraa $u = x_0 + \frac{b}{d}n$. Sijoittamalla tämä yhtälöön $a(u - x_0) = b(y_0 - v)$ saadaan $\frac{ab}{d}n = b(y_0 - v)$, mistä jakamalla b:llä seuraa $v = y_0 - \frac{ab}{d}n$. $\square$

Esimerkki Oletetaan, että pankkiautomaatti antaa vain 20 euron ja 50 euron seteleitä. Millä tavoin setelit voidaan valita, kun halutaan nostaa rahaa 530 euroa?

Olkoon

$$x = \text{ 20 euron seteleiden lkm}, \quad y = \text{ 50 euron seteleiden lkm}.$$

On siis ratkaistava Diofantoksen yhtälö

$$20x + 50y = 530,$$

missä $x \geq 0$ ja $y \geq 0$. Nyt $\text{syt}(20, 50) = 10$ ja $\text{syt}(20, 50) \mid 530$, joten ratkaisuja on olemassa. Eräs ratkaisu löydetään luvun $\text{syt}(20, 50)$ lineaarikombinaation avulla. Lineaarikombinaatioksi saadaan (tässä suoraan hatusta) $10 = 50 - 2 \cdot 20$, ja kertomalla lineaarikombinaatio luvulla 53 saadaan

$$530 = 50 \cdot 53 - 106 \cdot 20,$$

eli $x_0 = -106$ ja $y_0 = 53$. Tämä ratkaisu ei kuitenkaan toteuta reunaehtoja! Kaikki ratkaisut saadaan yhtälöistä

$$x = -106 + \frac{50}{10}n = -106 + 5n, \quad y = 53 - \frac{20}{10}n = 53 - 2n, \quad n \in \mathbf{Z}.$$

Koska $-106 + 5n \geq 0$ ja $53 - 2n \geq 0$, saadaan n:lle rajat $n \geq \frac{106}{5} = 21\frac{1}{5}$ ja $n \leq \frac{53}{2} = 26\frac{1}{2}$. Siis $n \in \{22, 23, 24, 25, 26\}$ ja ratkaisuparit (x, y) ovat $(4, 9)$, $(9, 7)$, $(14, 5)$, $(19, 3)$, $(24, 1)$.

Diofantoksen yhtälön ratkaisu johtaa lineaarisen kongruenssin ratkaisuun:

Lauseen 3.2.2 todistus. (i). Olkoon $d \nmid b$, missä $d = syt(a, m)$. Luku $x \in \mathbf{Z}$ toteuttaa yhtälön

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

jos ja vain jos $ax + ym = b$ joillekin $x, y \in \mathbf{Z}$, joten Lauseen 3.2.4 nojalla kongruenssilla ei ole ratkaisuja.

(ii) Olkoon $d \mid b$. Lauseen 3.2.4 mukaan yhtälön $ax + ym = b$ ratkaisujoukko on

$$x = x_0 + \frac{m}{d}n, \quad y = y_0 - \frac{a}{d}n, \quad n \in \mathbf{Z},$$

missä (x_0, y_0) on jokin ratkaisu. Siis luvut

$$x = x_0 + \frac{m}{d}n, \quad n \in \mathbf{Z}, \tag{11}$$

muodostavat kongruenssin $ax \equiv b \pmod{m}$ ratkaisujoukon.

Tarkastellaan lopuksi ratkaisuja

$$x = x_0 + \frac{m}{d}t, \quad t = 0, 1, \ldots, d-1. \tag{12}$$

Riittää osoittaa, että

(1) ratkaisut (12) ovat pareittain ei-kongruentteja modulo m,

(2) jokainen ratkaisu (11) on kongruentti modulo m jonkin ratkaisun (12) kanssa.

Väite (1): Antiteesi: On olemassa $0 \le t_1 < t_2 \le d-1$ siten, että

$$x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2 \pmod{m}.$$

Tällöin

$$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \pmod{m}.$$

Nyt $\text{syt}(m, \frac{m}{d}) = \frac{m}{d}$, joten tulon supistussäännön (Lause 3.1.5) nojalla

$$t_1 \equiv t_2 \pmod{d}.$$

Näin ollen $d \mid t_1 - t_2$, mistä seuraa $d \le t_2 - t_1$. Tämä on ristiriidassa ehdon $0 \le t_1 < t_2 \le d-1$ kanssa, joten väite (1) pätee.

Väite (2): Olkoon $x = x_0 + \frac{m}{d}n$ eräs ratkaisu. Jakamalla n luvulla d saadaan jakoyhtälö

$$n = qd + r, \quad 0 \le r \le d-1.$$

Tällöin

$$x_0 + \frac{m}{d}n = x_0 + \frac{m}{d}(qd + r) = x_0 + mq + \frac{m}{d}r \equiv x_0 + \frac{m}{d}r \pmod{m},$$

sillä $mq \equiv 0 \pmod{m}$. Tässä $r = 0, 1, \ldots, d-1$, joten myös (2) pätee. □

Esimerkki Ratkaistaan kongruenssiyhtälö

$$987x \equiv 520 \pmod{1597}.$$

Euklideen algoritmin avulla saadaan lineaarikombinaatio

$$1 = \text{syt}(1597, 987) = -377 \cdot 1597 + 610 \cdot 987.$$

Yksityiskohdat sivuutetaan tässä. Koska $1 = \text{syt}(1597, 987)$, ratkaisu on yksikäsitteinen kongruenssiluokkana. Lineaarikombinaatiosta saadaan edelleen

$$520 = (-377 \cdot 520)1597 + (610 \cdot 520)987$$

eli

$$(610 \cdot 520)987 - 520 = (-377 \cdot 520)1597.$$

Siis ratkaisu on $x = 610 \cdot 520 = 317200 \equiv 994 \pmod{1597}$. Huomaa, että ratkaisu ilmoitetaan yleensä jakojäännöksen avulla. Tässä $317200 - 994 = 1597 \cdot 198$.

Huomautus 3.2.5 Lauseen 3.2.2 tärkein tapaus on se, jossa $d = syt(a, m) = 1$. Tällöin yhtälöllä

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

on kongruenssiluokan mielessä yksikäsitteinen ratkaisu kaikilla $b \in \mathbf{Z}$.

Määritelmä 3.2.6 Olkoon $m \in \mathbf{N}$ ja $a \in \mathbf{Z}$ siten, että $syt(a, m) = 1$. Tällöin kongruenssin

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

ratkaisun x jakojäännöstä modulo m kutsutaan *luvun a käänteisluvuksi modulo m*. Käänteisluvulle modulo m käytetään merkintää $\overline{a} \pmod{m}$.

Esimerkki 3.2.7 (a) Määrätään $\overline{12} \pmod{1001}$. Tätä varten kirjoitetaan euklideen algoritmi suurimman yhteisen tekijän $\text{syt}(12, 1001) = 1$ määräämiseksi. Saadaan

$$\begin{aligned} 1001 &= 83 \cdot 12 + 5, \\ 12 &= 2 \cdot 5 + 2, \\ 5 &= 2 \cdot 2 + 1, \end{aligned}$$

josta johdetaan lineaarikombinaatio

$$1 = 5 \cdot 1001 - 417 \cdot 12.$$

Siis $12(-417) - 1 = -5 \cdot 1001$, joten eräs ratkaisu tarkasteltavalle kongruenssiyhtälölle $12x \equiv 1 \pmod{1001}$ on $x_0 = -417$. Tämän luvun jakojäännös modulo 1001 on 584, sillä $-417 = -1 \cdot 1001 + 584$. Siis $\overline{12} = 584 \pmod{1001}$.

(b) Jos kongruenssiyhtälössä $ax \equiv b \pmod{m}$, $syt(a, m) = 1$, tunnetaan luvun a käänteisluku $\overline{a} \pmod{m}$, on yhtälön ratkaiseminen helppoa (vrt. yhtälö $ax = b$ reaaliluvuille). Tarkastellaan esimerkiksi yhtälöä

$$12x \equiv 7 \pmod{1001}.$$

Nyt $\overline{12} = 584$, joten

$$12 \cdot 584 \equiv 1 \pmod{1001}$$

ja kertomalla puolittain luvulla 7 saadaan

$$7 \cdot 12 \cdot 584 \equiv 12(7 \cdot 584) \equiv 7 \pmod{1001}.$$

Siis eräs ratkaisu on $7 \cdot 584 = 4088$. Ratkaisuksi saadaan jakojäännöksen avulla 84, sillä $4088 = 4 \cdot 1001 + 84$. (Tarkistus: $12 \cdot 84 - 7 = 1001$.)

Toisin: Kertomalla yhtälö $12x \equiv 7 \pmod{1001}$ puolittain luvulla 584 saadaan

$$584 \cdot 12x \equiv 584 \cdot 7 \pmod{1001}.$$

Koska toisaalta $584 \cdot 12 \equiv 1 \pmod{1001}$, niin kertomalla puolittain luvulla x saadaan

$$584 \cdot 12x \equiv x \pmod{1001}.$$

Transitiivisuuden nojalla

$$x \equiv 584 \cdot 7 \pmod{1001}.$$

3.3 Kiinalainen jäännöslause

Esimerkki (a) Mikä on pienin pariton luonnollinen luku, jolla on 3:lla jaettaessa jakojäännös 2 ja 5:llä jaettaessa jakojäännös 3?
Kongruenssikielellä: Määrää pienin $x \in \mathbf{N}$, jolle

$$\begin{cases} x \equiv 1 \ (\mathrm{mod}\, 2) \\ x \equiv 2 \ (\mathrm{mod}\, 3) \\ x \equiv 3 \ (\mathrm{mod}\, 5). \end{cases}$$

Alkeellisin ratkaisu ongelmaan löydetään, kun listataan ehdot toteuttavia lukuja modulo 2, 3, 5 ja poimitaan pienin:

$x \equiv 1 \ (\mathrm{mod}\, 2) \implies x = 1, 3, 5, ...$ eli x on pariton luonnollinen luku
$x \equiv 2 \ (\mathrm{mod}\, 3) \implies x = 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, 38, 41, 44, 47, 50, 53, ...$
$x \equiv 3 \ (\mathrm{mod}\, 5) \implies x = 2, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, ...$

Siis pienin yhteinen luonnollinen luku on 23, seuraavaksi pienin on 53.

Huom! Jos $x \equiv 23 \ (\mathrm{mod}\, 30)$, niin x on yhtälöryhmän ratkaisu. Esimerkiksi, ehto $x \equiv 23 \ (\mathrm{mod}\, 30)$ implikoi, että $x \equiv 23 \ (\mathrm{mod}\, 5)$ ja yhdistämällä tämä tietoon $23 \equiv 3 \ (\mathrm{mod}\, 5)$ saadaan transitiivisuuden nojalla $x \equiv 3 \ (\mathrm{mod}\, 5)$. Yhtälöt modulo 2 ja 3 käsitellään vastaavasti.

(b) Jos moduloluvut eivät ole pareittain suhteellisia alkulukuja, kohdan (a) tyyppisellä yhtälöryhmällä ei välttämättä ole ratkaisua. Esimerkiksi yhtälöryhmällä

$$\begin{cases} x \equiv 1 \ (\mathrm{mod}\, 2) \\ x \equiv 2 \ (\mathrm{mod}\, 4) \end{cases}$$

ei ole ratkaisua, sillä ylemmän yhtälön ratkaisut ovat parittomia ja alemman ratkaisut ovat parillisia.

Jos yhtälöitä on vähän ja luvut ovat pieniä, seuraava iteratiivinen metodi on kätevä:

Esimerkki 3.3.1 Tarkastellaan yhtälöryhmää

$$\begin{cases} x \equiv 1 \ (\mathrm{mod}\ 3) \\ x \equiv 2 \ (\mathrm{mod}\ 5) \\ x \equiv 3 \ (\mathrm{mod}\ 7). \end{cases}$$

Jos x toteuttaa ylimmän yhtälön, se on muotoa $x = 3t + 1$ jollekin $t \in \mathbf{Z}$. Sijoittamalla toiseen yhtälöön saadaan

$$3t + 1 \equiv 2 \ (\mathrm{mod}\, 5),$$

ja siis

$$3t \equiv 1 \ (\mathrm{mod}\, 5).$$

Ratkaisemalla kongruenssi saadaan $t \equiv 2 \ (\mathrm{mod}\, 5)$. Siis $t = 5u + 2$ jollekin $u \in \mathbf{Z}$, joten

$$x = 3t + 1 = 3(5u + 2) + 1 = 15u + 7.$$

Sijoittamalla tämä kolmanteen yhtälöön saadaan

$$15u + 7 \equiv 3 \ (\mathrm{mod}\, 7),$$

mistä seuraa

$$15u \equiv -4 \,(\mathrm{mod}\, 7) \iff u \equiv 3 \,(\mathrm{mod}\, 7).$$

Tässä jälkimmäinen esitys perustuu yhtälöihin $15 \equiv 1 \,(\mathrm{mod}\, 7)$ ja $-4 \equiv 3 \,(\mathrm{mod}\, 7)$. Siis $u = 7v + 3$, joten luvulle x saadaan esitys

$$x = 15u + 7 = 15(7v + 3) + 7 = 105v + 52.$$

Näin ollen $x \equiv 52 \,(\mathrm{mod}\, 105)$.

Huomautus Iteratiivisen metodin etuna on se, että metodi toimii vaikka moduloluvut eivät olisi pareittain suhteellisia alkulukuja, vrt. muinainen intialainen munaongelma.

Lause 3.3.2 (Kiinalainen jäännöslause) Olkoot $m_1, \ldots, m_r \in \mathbf{N}$ pareittain suhteellisia alkulukuja, so. syt$(m_i, m_j) = 1$ aina kun $i \neq j$. Tällöin kongruenssiryhmän

$$\begin{cases} x \equiv a_1 \,(\mathrm{mod}\, m_1) \\ \quad \vdots \\ x \equiv a_r \,(\mathrm{mod}\, m_r) \end{cases} \tag{13}$$

ratkaisu on yksikäsitteinen modulo $M := m_1 \cdots m_r$ kaikilla $a_1, \ldots, a_r \in \mathbf{Z}$. Eräs ratkaisu on

$$x_0 = \sum_{i=1}^{r} a_i M_i \overline{M_i},$$

missä $M_i := \frac{M}{m_i}$ ja $\overline{M_i}$ on luvun M_i käänteisluku modulo m_i kaikilla $i = 1, \ldots, r$.

Lauseen 3.3.2 tyyppiä olevia ongelmia ja niiden ratkaisuja on löydetty kiinalaisista ja intialaisista kirjoitelmista jo 100-luvulta lähtien.

Esimerkki 3.3.3 Ratkaistaan Esimerkin 3.3.1 yhtälöryhmä

$$\begin{cases} x \equiv 1 \,(\mathrm{mod}\, 3) \\ x \equiv 2 \,(\mathrm{mod}\, 5) \\ x \equiv 3 \,(\mathrm{mod}\, 7) \end{cases}$$

Lauseen 3.3.2 avulla. Nyt

$$M = 3 \cdot 5 \cdot 7 = 105,\ M_1 = \frac{105}{3} = 35,\ M_2 = \frac{105}{5} = 21,\ M_3 = \frac{105}{7} = 15.$$

Lukujen M_i käänteislukujen $y_i := \overline{M_i}$ modulo m_i löytämiseksi ratkaistaan kongruenssit

$$35y_1 \equiv 1 \,(\mathrm{mod}\, 3), \quad 21y_2 \equiv 1 \,(\mathrm{mod}\, 5), \quad 15y_3 \equiv 1 \,(\mathrm{mod}\, 7),$$

jotka sievenevät muotoon

$$2y_1 \equiv 1 \,(\mathrm{mod}\, 3), \quad y_2 \equiv 1 \,(\mathrm{mod}\, 5), \quad y_3 \equiv 1 \,(\mathrm{mod}\, 7)$$

käyttäen kongruensseja

$$35 \equiv 2 \,(\mathrm{mod}\, 3), \quad 21 \equiv 1 \,(\mathrm{mod}\, 5), \quad 15 \equiv 1 \,(\mathrm{mod}\, 7).$$

Käänteisluvuiksi saadaan $\overline{M}_1 = 2$, $\overline{M}_2 = 1$, $\overline{M}_3 = 1$. Lauseen 3.3.2 mukaan ratkaisu on

$$x_0 = \sum_{i=1}^{3} a_i M_i \overline{M_i} = 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 157 \equiv 52 \,(\mathrm{mod}\, 105).$$

Ratkaisu ilmoitetaan yleensä jakojäännöksen modulo M avulla!

Huomautus Lauseen 3.3.2 ratkaisumetodi voidaan helposti toteuttaa tietokoneella. Olennaista on se, että vaadittava algoritmi on hyvin tehokas eli toimii hyvinkin suurilla luvuilla lyhyessä tietokoneajassa.

Kiinalaisen jäännöslauseen todistamiseksi tarvitsemme kaksi aputulosta:

Lemma 3.3.4 Olkoot $a_1, \ldots, a_n, b \in \mathbf{Z}$ siten, että $\mathrm{syt}(a_i, b) = 1$ kaikilla $i = 1, \ldots, n$. Tällöin

$$\mathrm{syt}(a_1 \cdots a_n, b) = 1.$$

Todistus. Todetaan väite induktiolla: (i) Tapaus $n = 2$ on todistettu harjoitustehtävänä.

(ii) Oletetaan, että väite pätee n:n alkion tapauksessa, $n \geq 2$. Olkoot $a_1, \ldots, a_{n+1}, b \in \mathbf{Z}$ siten, että $\mathrm{syt}(a_i, b) = 1$ kaikilla $i = 1, \ldots, n+1$. Induktio-oletuksen nojalla $\mathrm{syt}(a_1 \cdots a_n, b) = 1$, joten kohdan (i) perusteella $\mathrm{syt}(a_1 \cdots a_n a_{n+1}, b) = 1$. $\square$

Lemma 3.3.5 Olkoot $m_1, \ldots, m_r \in \mathbf{N}$. Jos $a \equiv b \,(\mathrm{mod}\, m_i)$ kaikilla $i = 1, \ldots, r$, niin

$$a \equiv b \,(\mathrm{mod}\ \mathrm{pym}(m_1, \ldots, m_r)).$$

Erityisesti, jos luvut $m_1, \ldots, m_r \in \mathbf{N}$ ovat pareittain suhteellisia alkulukuja, niin

$$a \equiv b \,(\mathrm{mod}\, m_1 \cdots m_r).$$

Huomautus Jos luvut $m_1, \ldots, m_r \in \mathbf{N}$ ovat pareittain suhteellisia alkulukuja, niin kahdella luvulla m_i ja m_j, $i \neq j$, ei ole yhteisiä alkutekijöitä. Esimerkiksi, jos

$$m_1 = 2^3 5^2, \quad m_2 = 3^4 7^3, \quad m_3 = 11^4,$$

niin

$$m_1 m_2 m_3 = 2^3 5^2 3^4 7^3 11^4$$

ja oikea puoli on selvästi sama kuin kaavan

$$\prod_{j=1}^{5} p_j^{\max\{m_{ij} : i=1,2,3\}} = \mathrm{pym}(m_1, m_2, m_3)$$

antama lauseke tässä tapauksessa.

Todistus. Olkoon

$$m_i = \prod_{j=1}^{k} p_j^{m_{ij}}$$

luvun m_i modifioitu kanoninen esitys, missä alkutekijäjoukko $\{ p_1, \ldots, p_k \}$ koostuu kaikista lukujen $m_1, \ldots, m_r$ alkutekijöistä ja $m_{ij} = 0$ mikäli $p_j \nmid m_i$. Koska $a \equiv b \pmod{m_i}$ kaikilla $i = 1, \ldots, r$, niin

$$a \equiv b \pmod{p_j^{m_{ij}}}$$

kaikilla $i = 1, \ldots, r$ ja $j = 1, \ldots, k$. Siis erityisesti

$$a \equiv b \pmod{p_j^{\max\{m_{ij} : i=1,\ldots,r\}}}$$

kaikilla $j = 1, \ldots, k$, joten kaikki alkutekijäpotenssit $p_j^{\max\{m_{ij} : i=1,\ldots,r\}}$, $j = 1, \ldots, k$, ovat mukana luvun $a - b$ kanonisessa esityksessä. Kanonisen esityksen yksikäsitteisyydestä seuraa, että

$$a \equiv b \pmod{\prod_{j=1}^{k} p_j^{\max\{m_{ij} : i=1,\ldots,r\}}}.$$

Lemman 2.3.9 nojalla

$$a \equiv b \pmod{\operatorname{pym}(m_1, \ldots, m_r)}.$$

Edelleen, jos luvut $m_1, \ldots, m_r \in \mathbf{N}$ ovat pareittain suhteellisia alkulukuja, niin

$$\max\{ m_{ij} : i = 1, \ldots, r \} = \sum_{i=1}^{r} m_{ij}$$

kaikilla j. Nimittäin, jos näin ei ole, eli jos

$$\max\{ m_{ij} : i = 1, \ldots, r \} < \sum_{i=1}^{r} m_{ij}$$

jollekin j, niin joillekin $i \neq i^*$ pätee $m_{ij}, m_{i^*j} \in \mathbf{N}$. Lemmasta 2.3.7 seuraa, että

$$\operatorname{syt}(m_i, m_{i^*}) \geq p_j^{\min\{m_{ij}, m_{i^*j}\}} > 1,$$

mikä on ristiriidassa oletuksen kanssa. Lemman 2.3.9 nojalla

$$\begin{aligned} \operatorname{pym}(m_1, \ldots, m_r)) &= \prod_{j=1}^{k} p_j^{\max\{m_{ij} : i=1,\ldots,r\}} = \prod_{j=1}^{k} p_j^{\sum_{i=1}^{r} m_{ij}} \\ &= \prod_{j=1}^{k} \prod_{i=1}^{r} p_j^{m_{ij}} = \prod_{i=1}^{r} \prod_{j=1}^{k} p_j^{m_{ij}} = m_1 \cdots m_r. \end{aligned}$$

□

Lauseen 3.3.2 todistus. Koska $\operatorname{syt}(m_i, m_j) = 1$ aina kun $i \neq j$, niin Lemman 3.3.4 nojalla $\operatorname{syt}(M_i, m_i) = 1$ kaikilla $i = 1, \ldots, r$. Näin ollen kongruenssilla

$$M_i y \equiv 1 \pmod{m_i}$$

on yksikäsitteinen ratkaisu $\overline{M}_i$ modulo m_i.

Osoitetaan, että

$$x_0 = \sum_{i=1}^{r} a_i M_i \overline{M_i}$$

on kongruenssiyhtälöryhmän (13) ratkaisu. Olkoon $i \in \{1, \ldots, r\}$. Koska $m_i \mid M_j$ kun $j \neq i$, niin

$$M_j \equiv 0 \pmod{m_i}$$

kaikilla $j \neq i$. Näin ollen

$$a_j M_j \overline{M_j} \equiv 0 \pmod{m_i}$$

kaikilla $j \neq i$, joten

$$x_0 \equiv \sum_{j=1}^{r} a_j M_j \overline{M}_j \equiv a_i M_i \overline{M}_i \pmod{m_i}.$$

Mutta $M_i \overline{M}_i \equiv 1 \pmod{m_i}$, joten $a_i M_i \overline{M}_i \equiv a_i \pmod{m_i}$. Transitiivisuuden nojalla

$$x_0 \equiv a_i M_i \overline{M}_i \equiv a_i \pmod{m_i}.$$

Tämä pätee jokaisella $i = 1, \ldots, r$, joten x_0 on kongruenssiryhmän (13) ratkaisu.

Todistetaan lopuksi ratkaisun yksikäsitteisyys modulo M: Olkoot x_1 ja x_2 yhtälöryhmän (13) ratkaisuja. Tällöin transitiivisuuden nojalla

$$x_1 \equiv a_i \equiv x_2 \pmod{m_i}$$

kaikilla $i = 1, \ldots, r$, joten Lemman 3.3.5 mukaan $x_1 \equiv x_2 \pmod{M}$. Toisaalta, jos x_1 on yhtälöryhmän (13) ratkaisu ja $x_1 \equiv x_2 \pmod{M}$, niin erityisesti $x_1 \equiv x_2 \pmod{m_i}$ kaikilla $i = 1, \ldots, r$. Ehdosta $x_1 \equiv a_i \pmod{m_i}$ seuraa transitiivisuuden (ja symmetrisyyden) nojalla, että $x_2 \equiv a_i$ kaikilla $i = 1, \ldots, r$. $\square$

3.4 Fermat'n pieni lause ja Wilsonin lause

Lemma 3.4.1 Olkoon p alkuluku. Tällöin $x^2 \equiv 1 \pmod{p}$ jos ja vain jos $x \equiv 1 \pmod{p}$ tai $x \equiv -1 \pmod{p}$.

Todistus. Jos $x \equiv \pm 1 \pmod{p}$, niin $x^2 \equiv (\pm 1)^2 \pmod{p}$ eli $x^2 \equiv 1 \pmod{p}$. Oletetaan kääntäen, että $x^2 \equiv 1 \pmod{p}$ eli $p \mid x^2 - 1$. Tällöin $p \mid (x-1)(x+1)$ ja Lemman 2.3.3 nojalla $p \mid x - 1$ tai $p \mid x + 1$. Siis $x - 1 \equiv 0 \pmod{p}$ tai $x + 1 \equiv 0 \pmod{p}$ eli $x \equiv 1 \pmod{p}$ tai $x \equiv -1 \pmod{p}$. $\square$

Lemmaa 3.4.1 hyödynnetään seuraavassa kahdessa klassisessa 1600-luvun tuloksessa.

Lause 3.4.2 (Wilsonin lause) Jos p on alkuluku, niin

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

Huomautus Wilson itse ei todistanut lausettaan vaan ensimmäisen todistuksen esitti Lagrange 1770-luvulla. Tarkastellaan todistuksen ideaa ensin tapauksessa $n = 11$. Koska $\overline{2} = 6$, $\overline{3} = 4$, $\overline{5} = 9$, $\overline{7} = 8$ modulo 11, niin

$$\begin{aligned} 10! &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\ &\equiv 1 \cdot 10(2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \equiv 10 \cdot 1^5 \equiv 10 \equiv -1 \ (\mathrm{mod}\, 11). \end{aligned}$$

Lauseen 3.4.2 todistus. Voidaan olettaa, että $p > 2$, jolloin $p - 1$ on parillinen. Jokaista lukua a, $1 \leq a \leq p-1$, vastaa yksikäsitteinen käänteisluku $\overline{a}$ modulo p joukosta $\{1, \ldots, p-1\}$. Lemman 3.4.1 nojalla ainoat luvut joukossa $\{1, \ldots, p-1\}$, jotka ovat itsensä käänteislukuja, ovat 1 ja $p - 1$. Näin ollen joukko $\{2, \ldots, p-2\}$ jakautuu $\frac{p-3}{2}$ kappaleeseen luku-käänteislukupareja, joiden tulot ovat $\equiv 1 \ (\mathrm{mod}\, p)$. Siis

$$2 \cdot 3 \cdots (p-2) \equiv 1 \ (\mathrm{mod}\, p),$$

mistä seuraa, että

$$(p-1)! \equiv p - 1 \equiv -1 \ (\mathrm{mod}\, p).$$

□

Wilsonin lauseen kongruenssi itseasiassa karakterisoi alkuluvut:

Seuraus 3.4.3 Olkoon $n > 1$. Tällöin n on alkuluku jos ja vain jos

$$(n-1)! \equiv -1 \ (\mathrm{mod}\, n).$$

Todistus. Harjoitustehtävä. □

Määritelmä 3.4.4 Olkoon $m \in \mathbf{N}$. Joukko $A \subset \mathbf{Z}$ on *täydellinen jäännössysteemi modulo* m (lyhyesti t.j.s. mod m), jos A on m:n alkion joukko, jonka luvut ovat pareittein ei-kongruentteja modulo m.

Esimerkki 3.4.5 (a) Esimerkiksi

- Joukko $\{\, 0, 1, 2, 3 \,\}$ on t.j.s. mod 4.
- Joukko $\{\, -4, 1, 2, 6 \,\}$ ei ole t.j.s. mod 4, sillä $2 \equiv 6 \ (\mathrm{mod}\, 4)$.
- Joukko $\{\, -4, 9, 6, -17 \,\}$ on t.j.s. mod 4.

(b) Jos $m \in \mathbf{N}$, niin $\{\, 0, 1, \ldots, m-1 \,\}$ on t.j.s. mod m. Yleisesti m:n alkion joukko A on t.j.s. mod m täsmälleen silloin kun joukon A alkioiden jakojäännösten modulo m joukko yhtyy joukkoon $\{\, 0, 1, \ldots, m-1 \,\}$, ks. 3.4.7.

Lemma 3.4.6 Olkoot $m \in \mathbf{N}$ ja $a, b \in \mathbf{Z}$ siten, että $\mathrm{syt}(a, m) = 1$. Jos joukko $\{\, x_1, \ldots, x_m \,\}$ on t.j.s. mod m, niin myös joukko

$$A = \{\, ax_1 + b, \ldots, ax_m + b \,\}$$

on t.j.s. mod m.

Todistus. Harjoitustehtävä. □

Esimerkki Olkoon $m = 7$ ja $a = 3$. Tarkastellaan joukkoa

$$A = \{\, 3i \mid i = 0, 1, \ldots, 6 \,\}.$$

Nyt

$$\begin{aligned}
3 \cdot 0 &\equiv 0 \pmod 7 \\
3 \cdot 1 &\equiv 3 \pmod 7 \\
3 \cdot 2 &\equiv 6 \pmod 7 \\
3 \cdot 3 &\equiv 2 \pmod 7 \\
3 \cdot 4 &\equiv 5 \pmod 7 \\
3 \cdot 5 &\equiv 1 \pmod 7 \\
3 \cdot 6 &\equiv 4 \pmod 7).
\end{aligned}$$

Lemma 3.4.7 Olkoon $A = \{\, x_1, \ldots, x_m \,\}$ t.j.s. mod m ja olkoon r_i luvun x_i jakojäännös modulo m, $i = 1, \ldots, m$. Tällöin

$$\{\, r_1, \ldots, r_m \,\} = \{\, 0, 1, \ldots, m - 1 \,\}.$$

Todistus. Harjoitustehtävä. □

Lause 3.4.8 (Fermat'n pieni lause) Olkoon p alkuluku ja olkoon $a \in \mathbf{Z}$ siten, että $p \nmid a$. Tällöin

$$a^{p-1} \equiv 1 \ (\bmod p). \tag{14}$$

Esimerkki Tarkastellaan todistuksen ideaa tapauksessa $p = 7, a = 3$. Nyt joukko

$$\{\, 3x : x = 0, 1, 2, 3, 4, 5, 6 \,\}$$

on t.j.s. modulo 7 (Lemma 3.4.6) ja koska luvun $3 \cdot 0 = 0$ jakojäännös modulo 7 on luku 0, saadaan (Lemma 3.4.7)

$$(1 \cdot 3) \cdot (2 \cdot 3) \cdot (3 \cdot 3) \cdot (4 \cdot 3) \cdot (5 \cdot 3) \cdot (6 \cdot 3) \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod 7$$

eli

$$6! \cdot 3^6 \equiv 6! \equiv 6! \cdot 1 \ (\bmod 7).$$

Koska $\text{syt}(6!, 7) = 1$, voidaan $6!$ supistaa kongruenssiyhtälössä Lemman 3.1.5 nojalla. Siis

$$3^6 \equiv 1 \pmod 7).$$

Fermat'n pienen lauseen todistus. Lemman 3.4.6 nojalla lukujoukko

$$A = \{0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a\}$$

on t.j.s. modulo p. Kullakin $i = 0, 1, \ldots, p - 1$, kirjoitetaan jakoyhtälö

$$ia = q_i p + r_i, \quad 0 \leq r_i \leq p - 1.$$

Huomaa, että $r_0 = 0$, sillä $0 \cdot a = 0 \cdot p + 0$. Koska A on t.j.s. modulo p, on Lemman 3.4.7 seurauksena

$$\{ r_1, \ldots, r_{p-1} \} = \{ 1, \ldots, p-1 \}. \tag{15}$$

Kertomalla yhtälön (15) lukujoukot puolittain ja ottamalla huomioon kongruenssi $ia \equiv r_i \pmod{p}$ saadaan

$$(1 \cdot a)(2 \cdot a) \cdots ((p-1) \cdot a) \equiv (p-1)! \pmod{p},$$

eli

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

Koska syt$(p, (p-1)!) = 1$ voidaan kertoma $(p-1)!$ supistaa, mistä väite

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

Seuraus 3.4.9 Olkoon p alkuluku ja $a \in \mathbf{Z}$ siten, että $p \nmid a$. Tällöin $\overline{a} = a^{p-2}$ modulo p. Edelleen, kaikilla $b \in \mathbf{Z}$, lineaarisen kongruenssin $ax \equiv b \pmod{p}$ ratkaisu on $x \equiv a^{p-2}b \pmod{p}$.

Todistus. Fermat'n pienen lauseen nojalla

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

joten käänteislukua koskeva väite on selvä.

Oletetaan, että x toteuttaa yhtälön $ax \equiv b \pmod{p}$. Kertomalla puolittain luvulla a^{p-2} saadaan

$$a^{p-2}ax \equiv a^{p-2}b \pmod{p} \iff a^{p-1}x \equiv a^{p-2}b \pmod{p}.$$

Toisaalta yhtälöstä $a^{p-1} \equiv 1 \pmod{p}$ seuraa $a^{p-1}x \equiv x \pmod{p}$, joten transitiivisuuden nojalla

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

□

Esimerkki Fermat'n pientä lausetta käytetään tyypillisesti potenssimuotoisten lukujen sieventämiseen moduloaritmetiikassa, eli ns. *modulaarisessa potenssiin korotuksessa*.

Määrätään malliksi luvun 3^{201} jakojäännös modulo 11. Fermat'n pienen mukaan

$$3^{10} \equiv 1 \pmod{11}.$$

Toisaalta jakoyhtälön mukaan $201 = 20 \cdot 10 + 1$, joten

$$3^{201} = (3^{10})^{20} 3 \equiv 1^{20} \cdot 3 \equiv 3 \pmod{11}.$$

Siis kysytty jakojäännös on 3.

3.5 Pseudoalkuluvut

Pseudoalkuluvuilla tarkoitetaan yhdistettyjä lukuja, jotka käyttäytyvät jonkin kriteerin mielessä samalla tavalla kuin alkuluvut. Pseudoalkulukuja käytetään hyväksi mm. alkulukutestauksessa.

Huomautus 3.5.1 Jos p on alkuluku, niin

$$a^p \equiv a \ (\mathrm{mod}\, p)$$

kaikilla $a \in \mathbf{Z}$ (harjoitustehtävä).

Pitkään ajateltiin, että Huomautus 3.5.1 voidaan kääntää. Tiettävästi esim. Leibniz uskoi konjektuuriin: Jos

$$2^n \equiv 2 \ (\mathrm{mod}\ n),$$

niin n on alkuluku. Tämä väite pitää paikkansa aina lukuun $n = 341 = 11 \cdot 31$ saakka.

Esimerkki 3.5.2 Tarkastellaan lukua $341 = 11 \cdot 31$. Fermat'n pienen lauseen mukaan

$$2^{10} \equiv 1 \ (\mathrm{mod}\, 11),$$

joten

$$2^{340} = (2^{10})^{34} \equiv 1 \ (\mathrm{mod}\, 11).$$

Toisaalta

$$2^{340} = (2^5)^{68} = (32)^{68} \equiv 1^{68} \equiv 1 \ (\mathrm{mod}\, 31).$$

Lemman 3.3.5 nojalla

$$2^{340} \equiv 1 \ (\mathrm{mod}\, 341) \quad \text{eli} \quad 2^{341} \equiv 2 \ (\mathrm{mod}\, 341).$$

Määritelmä 3.5.3 Olkoon $b > 1$. Yhdistetty luku $n \in \mathbf{N}$ on *b-kantainen pseudoalkuluku*, jos

$$b^n \equiv b \ (\mathrm{mod}\, n).$$

Huomautus Siis luku $341 = 11 \cdot 31$ on 2-kantainen pseudoalkuluku.

Lause 3.5.4 2-kantaisia pseudoalkulukuja on ääretön määrä.

Todistus. Olkoon n 2-kantainen pseudoalkuluku, ts. $r = ns$, missä $1 < r < n$ ja $1 < s < n$ ja $2^n \equiv 2$ (mod n). (Ainakin 341 on tälläinen). Riittää osoittaa, että myös

$$m := 2^n - 1$$

on 2-kantainen pseudoalkuluku. Esityksestä

$$2^n - 1 = 2^{rs} - 1 = (2^r - 1)\left((2^r)^{s-1} + (2^r)^{s-2} + \ldots + 2^r + 1\right)$$

seuraa, että $2^n - 1$ on yhdistetty. Toisaalta kongruenssioletuksen mukaan $2^n - 2 = kn$ jollekin $k \in \mathbf{Z}$, joten

$$2^{m-1} = 2^{2^n - 2} = 2^{kn}.$$

Edelleen

$$2^{kn} - 1 = (2^n - 1)\left((2^n)^{k-1} + \ldots + 2^n + 1\right),$$

joten $(2^n - 1) \mid (2^{kn} - 1)$. Yhdistämällä tekijärelaatiot saadaan $m \mid (2^{m-1} - 1)$ eli

$$2^{m-1} \equiv 1 \pmod{m}.$$

Tästä seuraa $2^m \equiv 2 \pmod{m}$, joten $m = 2^n - 1$ on 2-kantainen pseudoalkuluku. $\square$

Itseasiassa on olemassa lukuja, jotka ovat b-kantaisia pseudoalkulukuja kaikille $b > 1$. Näitä kutsutaan keksijänsä R. D. Carmichaelin (1879-1967) mukaan Carmichaelin luvuiksi.

Määritelmä 3.5.5 Yhdistetty luku $n \in \mathbf{N}$ on *Carmichaelin luku* jos

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

kaikille $b \in \mathbf{N}$, joille $\text{syt}(b, n) = 1$.

Huomautus 3.5.6 Jos $\text{syt}(b, n) = 1$ ja n on Carmichaelin luku, niin kertomalla Määritelmän 3.5.5 kongruenssi luvulla b saadaan

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

Näin ollen n on b-kantainen pseudoalkuluku. Voidaan osoittaa edelleen, että Carmichaelin luvulle n pätee

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

myös tapauksessa $\text{syt}(b, n) > 1$. Tämä kuitenkin sivuutetaan.

Kääntäen, jos n on b-kantainen pseudoalkuluku kaikilla $\text{syt}(b, n) = 1$, niin supistamalla yhtälöstä

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

b puolittain todetaan, että n on Carmichaelin luku.

Siis: Luku n on Carmichaelin luku jos ja vain jos n on b-kantainen pseudoalkuluku kaikilla $b > 1$.

Esimerkki 3.5.7 Luku $561 = 3 \cdot 11 \cdot 17$ on Carmichaelin luku (pienin sellainen). Tämän toteamiseksi olkoon $b > 1$ siten, että $\text{syt}(b, 561) = 1$. Tällöin

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

Fermat'n pienen lauseen nojalla

$$b^2 \equiv 1 \pmod{3}, \quad b^{10} \equiv 1 \pmod{11}, \quad b^{16} \equiv \pmod{17}.$$

Tästä seuraa, että

$$\begin{aligned} b^{560} &= (b^2)^{280} \equiv 1 \pmod{3}, \\ b^{560} &= (b^{10})^{56} \equiv 1 \pmod{11}, \\ b^{560} &= (b^{16})^{35} \equiv 1 \pmod{17}, \end{aligned}$$

joten Lemman 3.3.5 nojalla

$$b^{560} \equiv 1 \pmod{561}.$$

Esimerkin ilmiö ei ole sattumaa, sillä yleisesti pätee:

Lause 3.5.8 Luku n on Carmichaelin luku jos ja vain jos n on muotoa

$$n = p_1 \cdots p_r,$$

missä p_i:t ovat erillisiä alkulukuja ja $p_i - 1 \mid n - 1$ kaikilla $i = 1, \ldots r$.

Todistus. Jos n on vaadittua muotoa, niin yleistämällä Esimerkin 3.5.7 päättely todetaan, että n on Carmichaelin luku (harjoitustehtävä). Käänteisen väitteen todistus on syvällinen; se joudutaan tässä sivuuttamaan. □

Huomautus Vuonna 1992 todistettiin, että Carmichaelin lukuja on ääretön määrä. Erityisesti b-kantaisia pseudoalkulukuja on ääretön määrä kaikilla $b > 1$.

Pseudoalkuluvut ja alkulukutestaus

Pseudoalkulukuja käytetään hyväksi ns. *probabilistisessa alkulukutestauksessa*. Tämä perustuu siihen, että ehdon

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

toteuttavia yhdistettyjä lukuja on verrattain harvassa ja toisaalta on olemassa tehokkaita algoritmeja, joilla kongruenssiehto voidaan nopeasti tarkistaa.

Esimerkki Tarkastellaan lukuja $n \leq 10^{10}$. Näistä tiedetään:

- Alkulukuja on 455052512 kpl.
- 2-kantaisia pseudoalkulukuja on 14884 kpl.

Toisin sanoen luvuista $n \leq 10^{10}$ läpäisee testin $2^n \equiv 2 \pmod{n}$ noin 4.55 prosenttia ja näistä noin 0.003 prosenttia ei ole alkulukuja.

Millerin b-testi Oletetaan, että $n > 2$ on alkuluku. Tällöin $n - 1$ on parillinen ja se on aritmetiikan peruslauseen nojalla esitettävissä yksikäsitteisesti muodossa

$$n - 1 = 2^s t,$$

missä t on pariton. Olkoon $1 < b < n$. Fermat'n pienen lauseen mukaan

$$b^{n-1} \equiv 1 \pmod{n}.$$

Merkitsemällä $a = b^{(n-1)/2}$ kongruenssi saa muodon

$$a^2 \equiv 1 \pmod{n}.$$

Oletuksen mukaan n on alkuluku, joten (Lemma 3.4.1)

$$a \equiv 1 \pmod{n} \quad \text{tai} \quad a \equiv -1 \pmod{n}.$$

Jos nyt $a \equiv 1 \pmod{n}$ ja $s \geq 2$, voidaan päättely toistaa. Tällöin ehdosta

$$(b^{(n-1)/4})^2 \equiv 1 \pmod{n}$$

seuraa Lemman 3.4.1 nojalla, että

$$b^{\frac{n-1}{4}} \equiv 1 \pmod{n} \quad \text{tai} \quad b^{\frac{n-1}{4}} \equiv -1 \pmod{n}.$$

Yleisesti, jos

$$b^{(n-1)/2^j} \equiv 1 \pmod{n}$$

indeksin arvoilla $j = 0, \ldots, k$, missä $k \in \{ 0, 1, \ldots, s-1 \}$, niin

$$b^{(n-1)/2^{k+1}} \equiv 1 \pmod{n} \quad \text{tai} \quad b^{(n-1)/2^{k+1}} \equiv -1 \pmod{n}.$$

Erityisesti, jos $k = s - 1$, saadaan (koska $\frac{n-1}{2^s} = t$)

$$b^t \equiv 1 \pmod{n} \quad \text{tai} \quad b^t \equiv -1 \pmod{n}.$$

Siis, jos lasketaan luvut $b^t, b^{2t}, \ldots, b^{\frac{n-1}{2}}, b^{n-1}$ modulo n, niin alkuluvun $n > 2$ tapauksessa voi esiintyä vain vaihtoehdot:

(1) $b^{(n-1)/2^j} \equiv 1 \pmod{n}$ kaikilla $j = 0, \ldots, s$;

(2) $b^{(n-1)/2^j} \equiv -1 \pmod{n}$ jollekin $j = 1, \ldots, s$.

Esimerkki (a) Tutkitaan lukua $n = 2^3 \cdot 19799 + 1 = 158393$. Nyt $s = 3$ ja $t = 19799$. Maplen mod-komentoa käyttäen saadaan

$$2^t = 2^{19799} \equiv 96153 \pmod{158393}.$$

Edelleen

$$2^{2t} \equiv 96153^2 \equiv 158392 \equiv -1 \pmod{158393}.$$

Näin ollen luku n voi olla alkuluku.

(b) Tutkitaan lukua $n = 2^4 \cdot 19799 + 1 = 316785$. Nyt $s = 4$ ja $t = 19799$. Maplen mod-komentoa käyttäen saadaan

$$2^t = 2^{19799} \equiv 188108 \pmod{316785}.$$

Edelleen

$$2^{2t} \equiv 188108^2 \equiv 51949 \pmod{316785},$$

$$2^{4t} \equiv 51949^2 \equiv 7186 \pmod{316785}$$

ja

$$2^{8t} = 2^{\frac{n-1}{2}} \equiv 7186^2 \equiv 2641 \pmod{316785}.$$

Koska $2^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{316785}$, niin kyseessä ei voi olla alkuluku. Itseasiassa Maplen ifactor-komentoa käyttäen saadaan kanoninen esitys $316785 = 3 \cdot 5 \cdot 7^2 \cdot 431$.

Määritelmä 3.5.9 Olkoon $n > 2$ pariton luku siten, että $n-1 = 2^s t$, missä t on pariton. Tällöin n läpäisee *Millerin b-kantaluvun testin* luvulle $b > 1$, jos

$$b^t \equiv 1 \ (\mathrm{mod}\, n)$$

tai

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

jollakin $j = 0, \ldots, s-1$.

Edellä on todistettu:

Lause 3.5.10 Jos n on alkuluku ja $1 < b < n$, niin n läpäisee Millerin b-kantaluvun testin.

Millerin testin ideana on siis se, että määrätään luvut $b^t, \ldots, b^n$ parittomalle luvulle n, josta ei tiedetä onko se alkuluku vai ei! Jos saadaan yo. muotoa oleva lukujoukko, n on todennäköisesti alkuluku.

Huomautus (a) Millerin testissä lasketaan ensin luku b^t (modulo n). Seuraava luku taulukon vaakarivillä saadaan neliöimällä edellinen modulo n.

(b) Lukuja riittää laskea niin pitkään, että saadaan $\equiv -1$ (mod n) olettaen, että tämä tapahtuu viimeistään potenssille $b^{\frac{n-1}{2}}$. Jos $b^{\frac{n-1}{2}} \equiv \pm 1$ (mod n) *ei päde*, niin n ei ole alkuluku.

Huomautus 3.5.11 Osa yhdistetyistä luvuista läpäisee myös Millerin b-kantaluvun testin. On helppo osoittaa, että jos n on yhdistetty luku joka läpäisee Millerin b-testin, niin n on b-kantainen pseudoalkuluku (harjoitustehtävä).

Määritelmä 3.5.12 Jos $n > 2$ ei ole alkuluku, mutta se läpäisee Millerin b-testin, lukua n sanotaan *b-kantaiseksi vahvaksi pseudoalkuluvuksi*.

Esimerkki Olkoon $n = 2047$, jolloin $n - 1 = 2046 = 2 \cdot 1023$. Siis $s = 1$ ja $t = 1023$. Nyt

$$2^{1023} = (2^{11})^{93} = (2048)^{93} \equiv 1^{93} = 1 \ (\mathrm{mod}\ 2047).$$

Koska $2047 = 23 \cdot 89$, niin 2047 on 2-kantainen vahva pseudoalkuluku.

Voidaan osoittaa, että myös vahvoja pseudoalkulukuja on ääretön määrä kaikilla kantaluvuilla $b > 1$. Kuitenkaan ei ole olemassa "vahvoja Carmichaelin"lukuja:

Lause 3.5.13 Jos $n > 2$ on pariton yhdistetty luku, niin n läpäisee Millerin b-testin korkeintaan $\frac{n-1}{4}$:lle kantaluvulle b joukosta $\{1, \ldots n-1\}$.

Todistus. Lause voidaan todistaa alkeellisin metodein, mutta todistus on työläs ja vaatii käsitteistöä, jota tässä vaiheessa ei ole käytettävissä. □

Lause 3.5.13 johtaa välittömästi tärkeään *probabilistiseen alkulukutestiin*:

Lause 3.5.14 (Rabinin testi) Olkoon $n \in \mathbf{N}$ pariton. Valitaan umpimähkään k kertaa b joukosta $\{1, \ldots, n-1\}$ ja suoritetaan kullakin kerralla Millerin b-testi. Jos n on yhdistetty, niin n läpäisee kaikki k Millerin b-testiä todennäköisyydellä $\leq 4^{-k}$.

Huomautus Jos Lauseessa 3.5.14 valitaan $k = 100$, niin todennäköisyys sille, että yhdistetty luku tulkitaan alkuluvuksi on korkeintaan $4^{-100} < 10^{-60}$ ("tähtitieteellisen pieni"). Rabinin testi on yleisesti käytetty testi todella suurten lukujen testaamiseen, sillä voidaan riittävän nopeasti testata esimerkiksi 200-numeroisia lukuja. Alkulujen testaukseen on olemassa kirjava joukko metodeja, joista osa on "probalistisia"ja osa "varmoja". Jos ns. yleistetty Riemannin hypoteesi on tosi (kuten useat lukuteoreetikot uskovat), on olemassa tehokas Millerin testiin perustuva algoritmi joka *varmuudella* ratkaisee sen onko luku alkuluku vai ei.

4 Multiplikatiiviset funktiot

4.1 Eulerin funktio ja Eulerin lause

Määritelmä 4.1.1 *Eulerin funktion* $\phi : \mathbf{N} \to \mathbf{N}$ arvo $\phi(n)$ ilmoittaa lukujen $a \in \{1, \ldots, n\}$ lukumäärän, joille $\text{syt}(a, n) = 1$.

Esimerkki $\phi(8) = 4$, sillä luvuista $1, \ldots, 8$ täsmälleen luvut $1, 3, 5, 7$ ovat suhteellisia alkulukuja luvun 8 kanssa. Toisaalta $\phi(7) = 6$, sillä luvuista $1, \ldots, 7$ täsmälleen luvut $1, 2, 3, 4, 5, 6$ ovat suhteellisia alkulukuja luvun 7 kanssa.

Huomautus Jos $n \geq 3$, niin

$$2 \leq \phi(n) \leq n - 1.$$

Nimittäin aina $\text{syt}(n, n) > 1$ ja $syt(n - 1, n) = 1$.

Lemma 4.1.2 Olkoon $n > 1$. Tällöin n alkuluku jos ja vain jos $\phi(n) = n - 1$.

Todistus. Harjoitustehtävä. □

Lemma 4.1.3 Olkoon $a \equiv b \pmod n$. Tällöin $\text{syt}(a, n) = 1$ jos ja vain jos $\text{syt}(b, n) = 1$.

Todistus. Oletetaan, että $\text{syt}(a, n) = 1$. Tällöin $1 = ak_1 + nk_2$ joillekin $k_1, k_2 \in \mathbf{Z}$. Toisaalta kongruenssioletuksesta saadaan $a - b = k_3 n$. Sijoittamalla $a = b + k_3 n$ saadaan

$$1 = (b + k_3 n)k_1 + nk_2 = bk_1 + (k_3 k_1 + k_2)n.$$

Näin ollen $\text{syt}(b, n) = 1$. Käänteinen implikaatio nähdään vaihtamalla lukujen a ja b roolit päättelyssä. □

Määritelmä 4.1.4 *Redusoidulla jäännössysteemillä modulo n (r.j.s mod n)* tarkoitetaan joukkoa $A \subset \mathbf{Z}$, joka toteuttaa ehdot (i)-(iii):

(i) Joukossa A on $\phi(n)$ alkiota,

(ii) $\text{syt}(x, n) = 1$ kaikilla $x \in A$,

(iii) $x \not\equiv y \pmod n$ aina kun $x, y \in A$, $x \neq y$.

Esimerkki 4.1.5 Joukko $\{1, 3, 5, 7\}$ on r.j.s. mod 8. Yleisesti, jos

$$a \equiv 1 \pmod 8, \quad b \equiv 3 \pmod 8, \quad c \equiv 5 \pmod 8, \quad d \equiv 7 \pmod 8,$$

niin $\{a, b, c, d\}$ on r.j.s. mod 8. Katso Lemma 4.1.7 alla.

Lemma 4.1.6 Olkoon $\{a_1, \ldots, a_{\phi(n)}\}$ r.j.s. modulo n ja olkoon $b \in \mathbf{Z}$ siten, että $\text{syt}(b, n) = 1$. Tällöin joukko

$$A := \{\, ba_i \mid i = 1, \ldots, \phi(n) \,\}$$

on r.j.s. modulo n.

Todistus. Todistuksen idea samansuuntainen kuin t.j.s:n yhteydessä. Harjoitustehtävä. □

Lemma 4.1.7 Olkoon $\{a_1, \ldots, a_{\phi(n)}\}$ r.j.s. modulo n ja olkoon r_i luvun a_i jakojäännös modulo n, $i = 1, \ldots, \phi(n)$. Tällöin joukko $\{\, r_1, \ldots, r_{\phi(n)} \,\}$ on r.j.s. modulo n.

Todistus. Olkoon $R = \{\, r_1, \ldots, r_{\phi(n)} \,\}$. Joukossa R on selvästi $\phi(n)$ alkiota kunhan todetaan, että sen alkiot ovat pareittain ei-kongruentteja modulo n. Tehdään antiteesi: $r_i \equiv r_j \pmod n$ joillekin $i \neq j$. Koska $r_i \equiv a_i \pmod n$ ja $r_j \equiv a_j \pmod n$, saadaan transitiivisuuden ja symmetrisyyden nojalla $a_i \equiv a_j \pmod n$. Tämä on ristiriidassa r.j.s:n määritelmän kanssa.

On vielä todettava, että $\text{syt}(r_i, n) = 1$ kaikilla i. Tämä kuitenkin seuraa Lemmasta 4.1.3, sillä $\text{syt}(a_i, n) = 1$ ja $r_i \equiv a_i \pmod n$. □

Esimerkki Joukko $\{1, 3, 5, 7\}$ on r.j.s. mod 8. Nyt $\text{syt}(3, 8) = 1$, joten joukko

$$A = \{1 \cdot 3, 3 \cdot 3, 5 \cdot 3, 7 \cdot 3\}$$

on r.j.s. mod 8. Joukon A alkioiden jakojäännökset ovat

$$1 \cdot 3 \equiv 3 \text{ (mod 8)}, \quad 3 \cdot 3 \equiv 1 \text{ (mod 8)}, \quad 5 \cdot 3 \equiv 7 \text{ (mod 8)}, \quad 7 \cdot 3 \equiv 5 \text{ (mod 8)}.$$

Erityisesti,

$$3^4(1 \cdot 3 \cdot 5 \cdot 7) \equiv (1 \cdot 3)(3 \cdot 3)(5 \cdot 3)(7 \cdot 3) \equiv 1 \cdot 3 \cdot 5 \cdot 7 \text{ (mod 8)}.$$

Nyt $\text{syt}(1 \cdot 3 \cdot 5 \cdot 7, 8) = 1$, joten supistussäännön nojalla

$$3^4 \equiv 1 \pmod 8 \quad \text{eli} \quad 3^{\phi(8)} \equiv 1 \pmod 8.$$

Huomautus 4.1.8 Kaikilla $n \in \mathbf{N}$, eräs r.j.s. modulo n saadaan poimimalla ne luvut joukosta $\{\, 1, \ldots, n-1 \,\}$, jotka ovat suhteellisia alkulukuja luvun n kanssa. Helposti nähdään, että joukon $\{\, 1, \ldots, n-1 \,\}$ alkioista voidaan muodostaa vain yksi r.j.s. modulo n.

Jos nimittäin

$$A := \{\, a_1, \ldots, a_{\phi(n)} \,\} \subset \{1, \ldots, n-1\}$$

ja

$$B := \{\, b_1, \ldots, b_{\phi(n)} \,\} \subset \{1, \ldots, n-1\}$$

ovat molemmat redusoituja jäännössysteemejä modulo n ja on olemassa $x \in A$, $x \notin B$, niin joukossa $\{\, 1, \ldots, n-1 \,\}$ on ainakin $\phi(n) + 1$ lukua, jotka kaikki ovat suhteellisia alkulukuja n:n kanssa. Tämä on ristiriidassa Eulerin funktion määritelmän kanssa.

Lause 4.1.9 (Eulerin lause) Jos $n \in \mathbf{N}$ ja $a \in \mathbf{Z}$ siten, että $\text{syt}(a, n) = 1$, niin

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

Todistus. Olkoon $\{r_1, \ldots, r_{\phi(n)}\} \subset \{1, \ldots, n-1\}$ r.j.s. mod n (Huomautus 4.1.8). Lemman 4.1.6 nojalla joukko $\{ar_1, \ldots, ar_{\phi(n)}\}$ on r.j.s. mod n. Jos r_i' on luvun ar_i jakojäännös mod n, niin $ar_i \equiv r_i' \pmod{n}$ ja Lemman 4.1.7 mukaan $\{r_1', \ldots, r_{\phi(n)}'\} \subset \{1, \ldots, n-1\}$ on r.j.s mod n. Huomautuksen 4.1.8 nojalla

$$\{r_1', \ldots, r_{\phi(n)}'\} = \{r_1, \ldots, r_{\phi(n)}\}.$$

Kertomalla joukot puolittain saadaan

$$r_1 \cdots r_{\phi(n)} = r_1' \cdots r_{\phi(n)}' \equiv (ar_1) \cdots (ar_{\phi(n)}) = a^{\phi(n)}(r_1 \cdots r_{\phi(n)}) \pmod{n}.$$

Mutta $\text{syt}(r_1 \cdots r_{\phi(n)}, n) = 1$ (Lemma 3.3.4), joten $r_1 \cdots r_{\phi(n)}$ voidaan supistaa ja siten

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

□

Huomautus Eulerin lause on Fermat'n pienen lauseen yleistys, sillä jos p on alkuluku ja $p \nmid a$, niin $\text{syt}(p, a) = 1$. Toisaalta $\phi(p) = p - 1$.

Eulerin lauseen soveltamiseksi tarvitsemme tietoa funktion ϕ käyttäytymisestä. Tätä varten tarkastellaan seuraavaksi ϕ:n perusominaisuuksia.

Lemma 4.1.10 Olkoon p alkuluku ja $k \in \mathbf{N}$. Tällöin

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

Todistus. Olkoon $x \in \mathbf{N}$, $1 \leq x \leq p^k$. Koska

$$\text{syt}(x, p^k) > 1 \quad \Leftrightarrow \quad p \mid x \quad \Leftrightarrow \quad x = pk \text{ jollekin } k = 1, 2, \ldots, p^{k-1},$$

niin $\phi(p^k) = p^k - p^{k-1}$. □

Määritelmä 4.1.11 Funktiota $f : \mathbf{N} \to \mathbf{R}$ sanotaan *aritmeettiseksi funktioksi*.

Esimerkki Funktiot ϕ, $f(n) = n^\alpha$ ja $g(n) = \log n$, ovat esimerkkejä lukuteoriassa esiintyvistä aritmeettisista funktioista.

Määritelmä 4.1.12 Aritmeettinen funktio f on *multiplikatiivinen*, jos

$$f(mn) = f(m)f(n)$$

aina kun $\text{syt}(m, n) = 1$. Edelleen f on *täydellisesti multiplikatiivinen* jos

$$f(mn) = f(m)f(n)$$

kaikilla $m, n \in \mathbf{N}$.

Esimerkki Funktio $f(n) = n^\alpha$, $\alpha \in \mathbf{R}$, on täydellisesti multiplikatiivinen , sillä

$$f(mn) = (mn)^\alpha = m^\alpha n^\alpha = f(m)f(n).$$

Funktio $g(n) = \log n$ ei ole multiplikatiivinen, sillä esimerkiksi

$$g(6) = \log 6 = \log 3 \cdot 2 = \log 3 + \log 2 \neq (\log 3)(\log 2).$$

Myöskään ϕ ei ole täydellisesti multiplikatiivinen, sillä jos $m = 2^3$ ja $n = 2^4$, niin

$$\phi(mn) = \phi(2^7) = 2^7 - 2^6 = 2 \cdot 2^6 - 2^6 = 2^6 = 64,$$

mutta

$$\phi(m) = 2^3 - 2^2 = 4$$

ja

$$\phi(n) = 2^4 - 2^3 = 8.$$

Tutkitaan Eulerin funktion multiplikatiivisuutta esimerkin kautta. Olkoot $n = 4$ ja $m = 3$, jolloin $\text{syt}(m, n) = 1$. Esitetään luvut $1, \ldots, 12$ taulukkona

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12. \end{array}$$

Tässä kahden ensimmäisen pystyrivin luvut ovat suhteellisia alkulukuja 3:n kanssa, kolmannen pystyrivin alkioista yksikään ei ole suhteellinen alkuluku 3:n kanssa. Siis ainakin $\phi(12) \leq 8$. Kahden ensimmäisen pystyrivin alkioista kummastakin täsmälleen kaksi on suhteellisia alkulukuja 4:n kanssa. Siispä $\phi(12) = 4$. Toisaalta $\phi(4)\phi(3) = 2 \cdot 2 = 4$.

Lause 4.1.13 Eulerin funktio ϕ on multiplikatiivinen.

Todistus. On osoitettava, että $\phi(mn) = \phi(m)\phi(n)$ aina kun $\text{syt}(m, n) = 1$. Oletetaan, että $\text{syt}(m, n) = 1$ ja esitetään luvut $1, \ldots, mn$ taulukkona

$$\begin{array}{ccccccc} 1 & 2 & \cdots & r & \ldots & m \\ m+1 & m+2 & \cdots & m+r & \cdots & 2m \\ 2m+1 & 2m+2 & \cdots & 2m+r & \cdots & 3m \\ \vdots & \vdots & & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+r & \cdots & nm. \end{array}$$

Tarkastellaan ensin sitä, kuinka moni r:nnen pystyrivin luvuista on suhteellinen alkuluku m:n kanssa. Olkoon $1 \leq r \leq m$ ja oletetaan, että $d := \text{syt}(r, m) > 1$. Taulukon r:s pystyrivi koostuu luvuista $km + r$, missä $0 \leq k \leq n - 1$. Koska $d \mid r$ ja $d \mid m$, niin $d \mid km + r$ kaikilla $k = 0, \ldots, n - 1$. Siis, jos $syt(r, m) > 1$, niin yksikään r:nnen pystyrivin luvuista ei ole suhteellinen alkuluku m:n kanssa.

Oletetaan, että $\text{syt}(r, m) = 1$ ja tarkastellaan r:nnen pystyrivin lukuja. Nyt $\text{syt}(km+r, m) = 1$ kaikilla $k = 0, \ldots, n - 1$. Jos nimittäin $s \mid m$ ja $s \mid km + r$ jollekin $s > 1$, niin

$$s \mid (-k)m + 1 \cdot (km + r) \quad \text{eli} \quad s \mid r.$$

Tällöin $\text{syt}(r,m) \geq s > 1$, mikä on ristiriita. Siis kaikki r:nnen pystyrivin alkiot ovat suhteellisia alkulukuja m:n kanssa jos $\text{syt}(r,m) = 1$.

Tarkastellaan seuraavaksi sitä, kuinka moni r:nnen pystyrivin alkioista on suhteellinen alkuluku n:n kanssa jos $\text{syt}(r,m) = 1$. Oletuksesta $\text{syt}(m,n) = 1$ seuraa Lemman 3.4.6 nojalla, että r:n pystyrivin alkiot muodostavat täydellisen jäännössysteemin mod n. Tällöin täsmälleen $\phi(n)$ kappaletta pystyrivin alkioista on suhteellisia alkulukuja n:n kanssa (harjoitustehtävä).

Koska joukossa $1, \ldots, m$ on täsmälleen $\phi(m)$ lukua r, joille pätee $\text{syt}(r,m) = 1$, on joukossa $\{1, 2, \ldots, mn\}$ täsmälleen $\phi(m)\phi(n)$ lukua x, joille $\text{syt}(x,m) = 1$ ja $\text{syt}(x,n) = 1$. Mutta $\text{syt}(x,mn) = 1$ jos ja vain jos $\text{syt}(x,m) = 1$ ja $\text{syt}(x,n) = 1$ (ks. Lemma 3.3.4), joten

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

□

Esimerkki Multiplikatiivisuuden nojalla

$$\phi(72) = \phi(2^3 3^2) = \phi(2^3)\phi(3^2) = (2^3 - 2^2)(3^2 - 3) = 4 \cdot 6 = 24.$$

Lause 4.1.14 (Eulerin funktion kanoninen kaava) Olkoon

$$n = p_1^{a_1} \cdots p_r^{a_r}$$

luvun $n > 1$ kanoninen esitys. Tällöin

$$\phi(n) = \prod_{i=1}^{r} (p_i^{a_i} - p_i^{a_i - 1}) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$

Todistus. Soveltamalla toistuvasti Lausetta 4.1.13 ja Lemmaa 4.1.10 saadaan

$$\begin{aligned} \phi(n) &= \phi(p_1^{a_1} \cdots p_r^{a_r}) = \phi(p_1^{a_1})\phi(p_2^{a_2} \cdots p_r^{a_r}) = \cdots = \phi(p_1^{a_1}) \cdots \phi(p_r^{a_r}) \\ &= (p_1^{a_1} - p_1^{a_1 - 1}) \cdots (p_r^{a_r} - p_r^{a_r - 1}) = p_1^{a_1}(1 - p_1^{-1}) \cdots p_r^{a_r}(1 - p_r^{-1}) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i}). \end{aligned}$$

□

Huomautus Lauseen 4.1.14 esityksessä mielenkiintoista on se, että luvun $\phi(n)$ määräämiseksi riittää tuntea n:n alkutekijät, so. eksponentteja a_i ei tarvitse tietää.

Kanonisen kaavan avulla voidaan johtaa erilaisia Eulerin funktion ominaisuuksia:

Esimerkki 4.1.15 Osoitetaan, että $\phi(n)$ on parillinen kaikilla $n > 2$. Olkoon

$$n = p_1^{a_1} \cdots p_r^{a_r}$$

luvun $n > 2$ kanoninen esitys. Lauseen 4.1.14 nojalla

$$\phi(n) = \prod_{i=1}^{r} (p_i^{a_i} - p_i^{a_i - 1}) = \prod_{i=1}^{r} p_i^{a_i - 1}(p_i - 1).$$

Jos luvulla n on pariton alkutekijä p_i, niin $p_i - 1$ on parillinen ja siis $\phi(n)$ on parillinen. Jos taas luvun n ainoa alkutekijä on 2, ts. $n = 2^{a_1}$, niin oletuksen $n > 2$ seurauksena $a_1 \geq 2$. Tällöin $2^{a_1 - 1}$ on parillinen ja siis $\phi(n)$ on parillinen.

4.2 Muita multiplikatiivisia funktioita

Summafunktio σ ja *lukumääräfunktio* τ määritellään asettamalla

$$\begin{aligned} \sigma(n) : &= \text{luvun n positiivisten tekijöiden summa,} \\ \tau(n) : &= \text{luvun n positiivisten tekijöiden lukumäärä.} \end{aligned}$$

Huomautus Määritelmissä triviaalit positiiviset tekijät 1 ja n lasketaan mukaan. Siis σ ja τ ovat funktioita

$$\sigma(n) = \sum_{d \in \mathbf{N}, d \,|\, n} d$$

ja

$$\tau(n) = \sum_{d \in \mathbf{N}, d \,|\, n} 1.$$

Lemma 4.2.1 Olkoon p alkuluku ja $a \in \mathbf{N}$. Tällöin

$$\tau(p^a) = a + 1$$

ja

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

Todistus. Luvun p^a positiiviset tekijät ovat $1, p, p^2, \ldots, p^a$. Siis $\tau(p^a) = a + 1$. Toisaalta, geometrisen summan kaavaa käyttäen

$$1 + p + p^2 + \cdots + p^a = \frac{1 - p^{a+1}}{1 - p} = \frac{p^{a+1} - 1}{p - 1}.$$

□

Lemma 4.2.2 Olkoot $m, n \in \mathbf{N}$ siten, että $\text{syt}(m, n) = 1$ ja olkoon $d \in \mathbf{N}$. Tällöin $d \,|\, mn$ jos ja vain jos on olemassa yksikäsitteiset luvut $d_1, d_2 \in \mathbf{N}$ siten, että $d_1 \,|\, m$ ja $d_2 \,|\, n$ ja $d = d_1 d_2$.

Esimerkki Olkoon $m = 4 = 2^2$ ja $n = 15 = 3 \cdot 5$. Luvun $mn = 60$ tekijät voidaan kirjoittaa luvun 4 ja luvun 15 tekijöiden tuloina seuraavasti:

$$\begin{aligned} 1 &= 1 \cdot 1,\ 2 = 2 \cdot 1,\ 3 = 1 \cdot 3,\ 4 = 2^2 \cdot 1,\ 5 = 1 \cdot 5,\ 6 = 2 \cdot 3,\ 10 = 2 \cdot 5,\ 12 = 2^2 \cdot 3, \\ 15 &= 1 \cdot 3 \cdot 5,\ 20 = 2^2 \cdot 5,\ 30 = 2 \cdot 3 \cdot 5,\ 60 = 2^2 \cdot 3 \cdot 5. \end{aligned}$$

Erityisesti huomataan, että $\tau(60) = \tau(4)\tau(15)$.

Todistus. Implikaatio oikealta vasemmalle on ilmeinen. Käänteisen todistamiseksi voidaan olettaa, että $m > 1$ ja $n > 1$. Olkoot

$$m = p_1^{a_1} \cdots p_r^{a_r} \quad \text{ja} \quad n = q_1^{b_1} \cdots q_s^{b_s}$$

lukujen kanoniset esitykset. Koska $\text{syt}(m, n) = 1$, niin $\{ p_1, \ldots, p_r \} \cap \{ q_1, \ldots, q_s \} = \emptyset$ eli

$$mn = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}$$

on tulon mn kanoninen esitys. Jos $d \mid mn$, niin $dk = mn$ jollekin $k \in \mathbf{N}$ ja kanonisen esityksen yksikäsitteisyydestä seuraa, että

$$d = p_1^{a_1'} \cdots p_r^{a_r'} q_1^{b_1'} \cdots q_s^{b_s'},$$

missä $0 \leq a_i' \leq a_i$ ja $0 \leq b_j' \leq b_j$ kaikilla $i = 1, \ldots, r$ ja $j = 1, \ldots, s$. Merkitään

$$d_1 = p_1^{a_1'} \cdots p_r^{a_r'} \quad \text{ja} \quad d_2 = q_1^{b_1'} \cdots q_s^{b_s'}.$$

Tällöin $d_1 \mid m$, $d_2 \mid n$ ja $d_1 d_2 = d$. Lukujen d_1 ja d_2 yksikäsitteisyys seuraa Aritmetiikan peruslauseesta. □

Lause 4.2.3 Funktiot σ ja τ ovat multiplikatiivisia.

Todistus. Olkoot $m, n \in \mathbf{N}$ siten, että $\text{syt}(m, n) = 1$. Lemman 4.2.2 nojalla jokaista $d \in \mathbf{N}$ vastaa yksikäsitteinen tuloesitys $d = d_1 d_2$, missä $d_1, d_2 \in \mathbf{N}$, $d_1 \mid m$ ja $d_2 \mid n$. Näin ollen osittelulain nojalla

$$\sigma(mn) = \sum_{d \in \mathbf{N}, d \mid mn} d = \sum_{d_1, d_2 \in \mathbf{N}, d_1 \mid m, d_2 \mid n} d_1 d_2 = \sum_{d_1 \in \mathbf{N}, d_1 \mid m} d_1 \sum_{d_2 \in \mathbf{N}, d_2 \mid n} d_2 = \sigma(m)\sigma(n).$$

Toisaalta

$$\tau(mn) = \sum_{d \in \mathbf{N}, d \mid mn} 1 = \sum_{d_1 \in \mathbf{N}, d_1 \mid m} 1 \sum_{d_2 \in \mathbf{N}, d_2 \mid n} 1 = \tau(m)\tau(n).$$

□

Seuraus 4.2.4 Olkoon

$$n = p_1^{a_1} \cdots p_r^{a_r}$$

luvun $n > 1$ kanoninen esitys. Tällöin

$$\tau(n) = \prod_{i=1}^{r} (a_i + 1)$$

ja

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Todistus. Multiplikatiivisuuden ja Lemman 4.2.1 nojalla

$$\tau(n) = \tau(p_1^{a_1} \cdots p_r^{a_r}) = \tau(p_1^{a_1})\tau(p_2^{a_2} \cdots p_r^{a_r}) = \cdots = \tau(p_1^{a_1}) \cdots \tau(p_r^{a_r}) = \prod_{i=1}^{r} (a_i + 1).$$

Toinen väite vastaavasti. □

Muinaiset kreikkalaiset määrittelivät täydellisen luvun seuraavasti:

Määritelmä 4.2.5 Luku $n \in \mathbf{N}$ on *täydellinen*, jos $\sigma(n) = 2n$.

Esimerkki Luvut 6 ja 28 ovat täydellisiä, sillä

$$\sigma(6) = 1 + 2 + 3 + 6 = 12 \quad \text{ja} \quad \sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56.$$

Parilliset täydelliset luvut voidaan karakterisoida seuraavasti:

Lause 4.2.6 Luku $n > 1$ on parillinen täydellinen luku jos ja vain jos

$$n = 2^{p-1}(2^p - 1),$$

missä $p > 2$ siten, että $2^p - 1$ on alkuluku.

Huomautus Jo Euklides tunsi implikaation oikealta vasemmalle. Käänteisen implikaation todisti Euler.

Todistus. Implikaatio oikealta vasemmalle harjoitustehtävä.

Käänteisen implikaation todistamiseksi oletetaan, että n on parillinen täydellinen luku, eli $\sigma(n) = 2n$. Esitetään n muodossa $n = 2^s t$, missä $s \in \mathbf{N}$ ja t on pariton. Koska $\text{syt}(2^s, t) = 1$, saadaan Lauseen 4.2.3 ja Seurauksen 4.2.4 nojalla

$$\sigma(n) = \sigma(2^s t) = \sigma(2^s)\sigma(t) = (2^{s+1} - 1)\sigma(t).$$

Mutta n on täydellinen, joten

$$(2^{s+1} - 1)\sigma(t) = 2n = 2^{s+1}t. \tag{16}$$

Koska $\text{syt}(2^{s+1}, 2^{s+1} - 1) = 1$, Lemman 2.3.2 nojalla $2^{s+1} \mid \sigma(t)$. Siis $\sigma(t) = q2^{s+1}$ jollekin $q \in \mathbf{N}$. Sijoittamalla σ:n esitys yhtälöön (16) saadaan

$$(2^{s+1} - 1)q2^{s+1} = 2^{s+1}t.$$

Siis

$$(2^{s+1} - 1)q = t,$$

joten $q \mid t$, $q < t$. Osoitetaan, että $q = 1$. Jos olisi $q > 1$, niin luvulla t olisi ainakin positiiviset tekijät $1, t$ ja q. Tällöin $\sigma(t) \geq t + q + 1$. Tämä on ristiriidassa yhtälön

$$t + q = (2^{s+1} - 1)q + q = q2^{s+1} = \sigma(t)$$

kanssa. Näin ollen $q = 1$, $t = 2^{s+1} - 1$ ja $\sigma(t) = 2^{s+1}$. Koska $\sigma(t) = t + 1$, niin $t = 2^{s+1} - 1$ on alkuluku ja

$$n = 2^s(2^{s+1} - 1).$$

Voidaan siis valita $p = s + 1$ ja väite pätee. □

Huomautus Tiedetään, että $2^p - 1$ voi olla alkuluku vain silloin kun p on alkuluku (harjoitustehtävä). Lauseen 4.2.6 nojalla parilliset täydelliset luvut vastaavat yksi-yhteen muotoa $2^p - 1$ olevia alkulukuja.

Määritelmä 4.2.7 Muotoa

$$M_p := 2^p - 1, \quad p \text{ alkuluku},$$

olevia lukuja kutsutaan *Mersenne-luvuiksi*. Jos M_p on alkuluku, sitä sanotaan *Mersenne-alkuluvuksi*.

Huomautus Suurimmat tunnetut alkuluvut ovat jo pitkään olleet Mersenne-alkulukuja. Tämä johtuu siitä, että Mersenne-lukujen alkulukutestaukseen on olemassa hyvin tehokkaita testejä. Syyskuussa 2006 löydettiin toistaiseksi suurin tunnettu alkuluku

$$M_{232582657} = 2^{232582657} - 1.$$

Tässä luvussa on yli 9.8 miljoonaa desimaalia. Mersenne-alkulukuja tunnetaan lokakuussa 2007 44 kappaletta. Toistaiseksi ei ole kyetty todistamaan sitä, että Mersenne-alkulukuja olisi ääretön määrä.

Mitä tiedetään parittomista täydellisistä luvuista?

Esimerkki 4.2.8 Osoitetaan, että parittomalla täydellisellä luvulla on vähintään kolme alkutekijää.

Todetaan ensin, että alkuluvun potenssi ei voi olla pariton täydellinen luku. Olkoon $n = p^a$, missä $p > 2$ on alkuluku ja $a \in \mathbf{N}$. Tällöin

$$\sigma(n) = \frac{p^{a+1} - 1}{p - 1} < \frac{p^{a+1}}{p - 1} = \frac{np}{p - 1} = \frac{n}{1 - \frac{1}{p}} \leq \frac{n}{1 - \frac{1}{3}} = \frac{3}{2}n.$$

Näin ollen $\sigma(n) \neq 2n$ eli n ei ole täydellinen luku.

Oletetaan seuraavaksi, että n on muotoa $n = p^a q^b$, missä p ja q ovat parittomia alkulukuja ja $a, b \in \mathbf{N}$. Tällöin multiplikatiivisuuden nojalla

$$\begin{aligned}\sigma(n) &= \frac{(p^{a+1} - 1)(q^{b+1} - 1)}{(p - 1)(q - 1)} < \frac{p^{a+1}q^{b+1}}{(p - 1)(q - 1)} = \frac{npq}{(p - 1)(q - 1)} \\ &= \frac{n}{(1 - \frac{1}{p})(1 - \frac{1}{q})} \leq \frac{n}{(1 - \frac{1}{3})(1 - \frac{1}{5})} = \frac{15}{8}n.\end{aligned}$$

Siis $\sigma(n) \neq 2n$ eli n ei ole täydellinen luku.

Huomautus Esimerkin 4.2.8 tapaisen väitteen todistaminen muuttuu (hieman yllättäen) nopeasti hyvin komplisoiduksi alkutekijöiden lukumäärän kasvaessa; jo vähintään kahdeksan alkutekijän olemassaolon todistaminen vaatii noin 200 sivua. Lisäksi tiedetään mm. se, ettei yhtään paritonta täydellistä lukua $< 10^{300}$ ole olemassa. Yleisesti uskotaankin ettei parittomia täydellisiä lukuja ole lainkaan olemassa!

5 Kryptologia

Tarkastelemme seuraavaksi kongruenssiin perustuvien kryptaus- eli salakirjoitusmetodien kehitystä.

Tässä luvussa

- P on selvätekstin (plaintext) kirjain (tai kirjainyhdistelmä) numeromuodossa;
- C on kryptotekstin (cryptotext, riphertext) kirjain (tai kirjainyhdistelmä) numeromuodossa.

Kryptaus perustuu siihen, että muunnamme ensin kirjaimet numeroiksi. Yksinkertaisuuden vuoksi käytämme englantilaisiin aakkosiin perustuvaa kirjain-numero-vastaavuutta

$$
\begin{aligned}
A &= 0,\\
B &= 1,\\
C &= 2,\\
D &= 3,\\
E &= 4,\\
F &= 5,\\
G &= 6,\\
H &= 7,\\
I &= 8,\\
J &= 9,\\
K &= 10,\\
L &= 11,\\
M &= 12,\\
N &= 13,\\
O &= 14,\\
P &= 15,\\
Q &= 16,\\
R &= 17,\\
S &= 18,\\
T &= 19,\\
U &= 20,\\
V &= 21,\\
W &= 22,\\
X &= 23,\\
Y &= 24,\\
Z &= 25.
\end{aligned}
$$

5.1 Yksidimensionaalinen affiini kryptausmuunnos

Esimerkki Julius Caesar käytti *kryptausmuunnosta*

$$C \equiv P + 3 \pmod{26}, \quad 0 \leq C \leq 25.$$

Siis

Selväteksti:	A	B	C	D	E	$\cdots$	X	Y	Z	
	0	1	2	3	4	$\cdots$	23	24	25	$\leftarrow$ Muunnos
	3	4	5	6	7	$\cdots$	0	1	2	
Kryptoteksti:	D	E	F	G	H	$\cdots$	A	B	C	

Dekryptausmuunnos saadaan ratkaisemalla P muuttujan C funktiona kryptausmuunnoksesta, ts.

$$P \equiv C - 3 \text{ (mod 26)}, \quad 0 \leq P \leq 25.$$

Yleisesti 1-dimensionaalisessa affiinissa kryptausmuunnoksessa selvätekstin kirjain P muutetaan kryptotekstin kirjaimeksi C ehdolla

$$C \equiv aP + b \text{ (mod 26)}, \quad 0 \leq C \leq 25, \quad \text{(Kryptausmuunnos)}$$

missä $a, b \in \{0, 1, \ldots, 25\}$ ovat vakioita siten, että $\text{syt}(a, 26) = 1$. Tällöin dekryptausmuunnokseksi saadaan (harjoitustehtävä)

$$P \equiv \overline{a}(C - b) \pmod{26}, \quad 0 \leq P \leq 25, \quad \text{(Dekryptausmuunnos)}$$

missä $\overline{a}$ on luvun a käänteisluku modulo 26.

Esimerkki Olkoon

$$C \equiv 7P + 10 \text{ (mod 26)}, \quad 0 \leq C \leq 25. \tag{17}$$

Nyt $\text{syt}(7, 26) = 1$ ja käänteisluvuksi saadaan $\overline{7} = 15$ modulo 26, sillä $7 \cdot 15 = 105 = 4 \cdot 26 + 1$. Siis dekryptausmuunnos on muotoa

$$P \equiv 15(C - 10) \equiv 15C - 150 \equiv 15C + 6 \text{ (mod 26)}, \quad 0 \leq P \leq 25. \tag{18}$$

(Muunnoksen kertoimet esitetään jakojäännösten modulo 26 avulla).

(a) Kryptataan sana PLEASE muunnoksella (17):

P	L	E	A	S	E
15	11	4	0	18	4
		$\downarrow$			
11	9	12	10	6	12
L	J	M	K	G	M

Tässä esimerkiksi selvätekstin muuttujan arvolla $P = 4$ (selvätekstin kirjain E) saadaan

$$C \equiv 7 \cdot 4 + 10 \equiv 12 \pmod{26}$$

eli vastaava kryptotekstin arvo on $C = 12$.

(b) Dekryptaus suoritetaan muunnoksella (18):

L	J	M	K	G	M
11	9	12	10	6	12
		$\downarrow$			
15	11	4	0	18	4
P	L	E	A	S	E

Tässä esimerkiksi kryptotekstin muuttujan arvolla $C = 10$ (kryptotekstin kirjain K) saadaan

$$P \equiv 15 \cdot 10 + 6 \equiv 0 \pmod{26}$$

eli vastaava selvätekstin kirjain on A.

Huomautus Yksidimensionaalinen affiini kryptausmuunnos ei kelpaa vakavasti otettavaksi kryptausmetodiksi, sillä erilaisia muunnoksia on vain

$$26\phi(26) = 26\phi(2)\phi(13) = 26 \cdot 12 = 312 \text{ kpl.}$$

Ne voidaan kaikki helposti läpikäydä tietokoneella.

5.2 Modulaarista matriisialgebraa

Hill kehitti 1930-luvulla affiiniin muunnokseen perustuvan lohkosalakirjoitusmenetelmän. Kryptataan malliksi teksti THE GOLD ns. 2-*dimensionaalisella Hillin lohkosalakirjoituksella.* Tätä varten teksti ryhmitellään kahden kirjaimen *lohkoiksi*

$$\begin{array}{cccc} T\ H & E\ G & O\ L & D\ X \\ 19\ 7 & 4\ 6 & 14\ 11 & 3\ 23. \end{array}$$

Tässä ylimääräinen X on lisätty, jotta viimeisessäkin lohkossa on kaksi kirjainta.

Kryptataan ylläoleva teksti muunnoksella

$$\begin{aligned} C_1 &\equiv 5P_1 + 17P_2 \text{ (mod 26)} \\ C_2 &\equiv 4P_1 + 15P_2 \text{ (mod 26)}, \quad 0 \leq C_i \leq 25, \end{aligned}$$

missä P_1, P_2 on selvätekstin lukupari (lohko) ja C_1, C_2 on sitä vastaava kryptotekstin lukupari (lohko). Esimerkiksi, selvätekstin ensimmäinen lohko $19, 7$ muunnetaan lohkoksi $6, 25$, sillä

$$\begin{aligned} C_1 &\equiv 5 \cdot 19 + 17 \cdot 7 = 214 \equiv 6 \text{ (mod 26)}, \\ C_2 &\equiv 4 \cdot 19 + 15 \cdot 7 = 181 \equiv 25 \text{ (mod 26)}. \end{aligned}$$

Tähän tapaan kryptaamalla saadaan:

$$\begin{array}{cccc} T\ H & E\ G & O\ L & D\ X \\ 19\ 7 & 4\ 6 & 14\ 11 & 3\ 23 \\ & & \downarrow & \\ 6\ 25 & 18\ 2 & 23\ 13 & 16\ 19 \\ G\ Z & S\ C & X\ N & Q\ T. \end{array}$$

Dekryptauksen suorittamiseksi on kyettävä ratkaisemaan ns. modulaarinen yhtälöpari

$$\begin{aligned} C_1 &\equiv 5P_1 + 17P_2 \text{ (mod 26)} \\ C_2 &\equiv 4P_1 + 15P_2 \text{ (mod 26)} \end{aligned}$$

kun C_1 ja C_2 tunnetaan. Tämä onnistuu lineaarialgebrasta tutulla tavalla laajentamalla kongruenssin idea matriisialgebraan.

Merkitään

$$P = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix},\ C = \begin{pmatrix} C_1 \\ C_2 \end{pmatrix},\ A \in M_{2,2}(\mathbf{Z}),$$

eli lohkot ilmaistaan 2-ulotteisilla pystyvektoreilla ja muunnos annetaan 2×2-kokonaislukumatriisin avulla. Nyt Hillin muunnos voidaan esittää muodossa

$$C \equiv AP \text{ (mod 26)},$$

kun kongruenssi laajennetaan matriiseille seuraavasti:

Määritelmä 5.2.1 Olkoon $m \in \mathbf{N}$ ja olkoot $A, B \in M_{n,k}(\mathbf{Z})$, ts. A ja B ovat $n \times k$-matriiseja, joiden kertoimet a_{ij} ja b_{ij} ovat kokonaislukuja. Tällöin merkitään

$$A \equiv B \text{ (mod } m)$$

jos

$$a_{ij} \equiv b_{ij} \text{ (mod } m)$$

kaikilla $i = 1, \ldots, n$ ja $j = 1, \ldots, k$.

Lemma 5.2.2 Olkoot $A \equiv A' \pmod m$ ja $B \equiv B' \pmod m$. Tällöin

$$A + B \equiv A' + B' \text{ (mod m)} \quad \text{ja} \quad AB \equiv A'B' \text{ (mod m)},$$

kunhan A ja B ovat tyypiltään sellaiset, että matriisien summa ja tulo ovat määriteltyjä.

Todistus. Lemman väite seuraa rutiininomaisesti matriisien yhteen- ja kertolaskujen määritelmistä. Todetaan malliksi yhteenlaskua koskeva väite. Olkoot $A, A', B, B' \in M_{k,l}(\mathbf{Z})$. Matriisin $A + B$ (i, j):s kerroin on $a_{ij} + b_{ij}$ ja matriisin $A' + B'$ (i, j):s kerroin on $a'_{ij} +' b'_{ij}$. Koska $a_{ij} \equiv a'_{ij} \pmod m$ ja $b_{ij} \equiv b'_{ij} \pmod m$ kaikilla i, j, niin

$$a_{ij} + b_{ij} \equiv a'_{ij} +' b'_{ij} \pmod m$$

kaikilla i, j. $\square$

Lemma 5.2.3 Määritelmän 5.2.1 kongruenssi on ekvivalenssirelaatio.

Todistus. Väitteet seuraavat välittömästi kokonaislukukongruenssin vastaavista ominaisuuksista. Todetaan malliksi transitiivisuus: Olkoot $A \equiv B \pmod m$ ja $B \equiv C \pmod m$ eli $a_{ij} \equiv b_{ij} \pmod m$ ja $b_{ij} \equiv c_{ij} \pmod m$ kaikilla i, j. Transitiivisuuden nojalla $a_{ij} \equiv c_{ij} \pmod m$, joten $A \equiv C \pmod m$. $\square$

Käänteismatriisi modulo m Palautetaan mieleen, kuinka 2×2-matriisin käänteismatriisi saadaan aikaan. Olkoon

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

missä $a, b, c, d \in \mathbf{Z}$ siten, että $det\ A = ad - bc \neq 0$. Tässä erikoistapauksessa adjungoitu matriisi $adj\ A$ on muotoa

$$adj\ A = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}^T = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

ja A:n käänteismatriisi A^{-1} saadaan yhtälöstä

$$A^{-1} = \frac{1}{det\ A} adj\ A. \tag{19}$$

Huomautus Käänteismatriisin kaava (19) pätee yleisesti matriiseille $A \in M_{n,n}(\mathbf{R})$, $\det A \neq 0$, ks. Lineaarialgebra.

Lause 5.2.4 Olkoon $A \in M_{n,n}(\mathbf{Z})$ ja olkoon $\text{syt}(det\, A, m) = 1$. Tällöin

$$A\overline{A} \equiv I \text{ (mod } m) \quad \text{ja} \quad \overline{A}A \equiv I \text{ (mod } m),$$

missä

$$\overline{A} := \overline{det\, A}(adj\, A)$$

ja $\overline{det\, A}$ on determinantin $det\, A$ käänteisluku modulo m.

Todistus. Koska $\text{syt}(det\, A, m) = 1$, on $det\, A \neq 0$, sillä voidaan olettaa $m > 1$. Yhtälöstä (19) saadaan

$$A(adj\, A) = (adj\, A)A = (det\, A)I.$$

Kertomalla puolittain luvulla $\overline{\det A}$ saadaan

$$\overline{\det A}(A(adj\, A)) = \overline{\det A}((adj\, A)A) = \overline{\det A}((det\, A)I).$$

Käyttämällä tunnettuja matriisien laskusääntöjä

$$\alpha(XY) = (\alpha X)Y = X(\alpha Y)$$

(tässä X ja Y matriiseja, α skalaari) saadaan

$$A(\overline{det\, A}(adj\, A)) = (\overline{det\, A}(adj\, A))A = (\overline{det\, A}(det\, A))I.$$

Mutta $\overline{det\, A}(det\, A) \equiv 1 \ (\text{mod}\, m)$, joten

$$(\overline{det A}\ detA)I \equiv I \text{ (mod } m).$$

Lauseen väitteet seuraavat matriisikongruenssin transitiivisuudesta (Lemma 5.2.3). □

Nimitys Matriisia $\overline{A}$ kutsutaan matriisin A *käänteismatriisiksi modulo* m.

Sovelletaan Lausetta 5.2.4 dekryptaukseen Hillin kryptausmuunnoksen

$$C \equiv AP \text{ (mod } 26)$$

tapauksessa, kun $A \in M_{2,2}(\mathbf{Z})$ siten, että $\text{syt}(det\, A, 26) = 1$. Kertomalla puolittain käänteismatriisilla modulo 26 saadaan

$$\overline{A}C \equiv \overline{A}AP \text{ (mod } 26).$$

Toisaalta Lauseen 5.2.4 mukaan

$$\overline{A}A \equiv I \text{ (mod } 26),$$

joten

$$\overline{A}AP \equiv IP \equiv P \text{ (mod } 26).$$

Matriisikongruenssin transitiivisuuden nojalla

$$\overline{A}C \equiv P \ (\text{mod}\, 26). \quad \text{(Dekryptausmuunnos)}$$

Siis selvätekstin lohko

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$$

saadaan kryptotekstin lohkosta

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix}$$

muunnoksen

$$P \equiv \overline{A}C \text{ (mod 26)}$$

avulla ottaen huomioon sen, että $0 \leq P_i \leq 25$, $i = 1, 2$. Käänteismuunnoksen määrääminen edellyttää siis matriisin

$$\overline{A} = (\overline{detA})\ adjA \text{ (mod 26)}$$

laskemista.

Esimerkki Tarkastellaan dekryptausta aiemman esimerkin

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \equiv \begin{pmatrix} 5\ 17 \\ 4\ 15 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \text{ (mod 26)}$$

tapauksessa. Nyt $det\ A = 5 \cdot 15 - 4 \cdot 17 = 7$ ja $\overline{det\ A} = 15$, sillä $15 \cdot 7 - 1 = 104 = 4 \cdot 26$. Adjungoiduksi matriisiksi saadaan

$$adj\ A = \begin{pmatrix} 15 & -17 \\ -4 & 5 \end{pmatrix},$$

joten

$$\overline{A} = \overline{detA}\ adjA = 15 \begin{pmatrix} 15 & -17 \\ -4 & 5 \end{pmatrix} = \begin{pmatrix} 225 & -255 \\ -60 & 75 \end{pmatrix} \equiv \begin{pmatrix} 17 & 5 \\ 18 & 23 \end{pmatrix} \text{ (mod 26).}$$

Siis dekryptausmuunnos on muotoa

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \equiv \begin{pmatrix} 17 & 5 \\ 18 & 23 \end{pmatrix} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \ (\mathrm{mod}\, 26)$$

eli yhtälöparina

$$\begin{cases} P_1 \equiv 17C_1 + 5C_2 \text{ (mod 26)} \\ P_2 \equiv 18C_1 + 23C_2 \text{ (mod 26)} \end{cases},$$

missä $0 \leq P_1 \leq 25$ ja $0 \leq P_2 \leq 25$. (Tässä tarvitaan matriisien kertolaskun määritelmää!)

Dekryptataan malliksi kaksi ensimmäistä lohkoa

$$\begin{pmatrix} 6 \\ 25 \end{pmatrix} \quad \text{ja} \quad \begin{pmatrix} 18 \\ 2 \end{pmatrix}.$$

Ensimmäisessä tapauksessa saadaan

$$\begin{aligned} P_1 &\equiv 17 \cdot 6 + 5 \cdot 25 \quad \equiv 227 \quad \equiv 19 \text{ (mod 26)}, \\ P_2 &\equiv 18 \cdot 6 + 23 \cdot 25 \quad \equiv 683 \quad \equiv 7 \text{ (mod 26)}. \end{aligned}$$

Jälkimmäisessä tapauksessa

$$\begin{aligned} P_1 &\equiv 17 \cdot 18 + 5 \cdot 2 \quad = 316 \quad \equiv 4 \text{ (mod 26)}, \\ P_2 &\equiv 18 \cdot 18 + 23 \cdot 2 \quad = 370 \quad \equiv 6 \text{ (mod 26)}. \end{aligned}$$

Huomautus Edellä esitetty yleistyy ilman ongelmia dimensioon $n \geq 2$. Hillin n-dimensionaalinen krytausmuunnos voidaan murtaa, jos tunnetaan n kpl kryptotekstilohkoja ja niitä vastaavat n selvätekstilohkoa.

5.3 Pohlig-Hellman exponenttisalakirjoitus

Pohlig ja Hellman esittelivät 1978 ns. *eksponenttisalakirjoitusmenetelmän*. Metodin lähtökohtana on lohkominen, mutta lohkon koko määrätään seuraavasti:

Liitetään kuhunkin kirjaimeen 2-numeroinen luku kirjoittamalla alkuun tarvittaessa nolla, siis esim. $A = 00,\ B = 01, \ldots$.

Valitaan alkuluku $p > 25$ ja luku $e \in \mathbf{N}$ siten, että $\text{syt}(e, p-1) = 1$. Selvätekstin kirjaimia vastaavat 2-numeroiset luvut ryhmitellään $2m$-numeroisiin lohkoihin, missä $m \in \mathbf{N}$ on suurin luku, jolle jokainen lohko $< p$. Siis esimerkiksi

$$\begin{array}{lll} 25 < & p & < 2525 \quad \Rightarrow m = 1 \text{ (lohkossa 1 kirjain)} \\ 2525 < & p & < 252525 \quad \Rightarrow m = 2 \text{ (lohkossa 2 kirjainta)} \\ 252525 < & p & < 25252525 \quad \Rightarrow m = 3 \text{ (lohkossa 3 kirjainta).} \end{array}$$

Kukin selvätekstin lohko ($2m$-numeroinen luku) kryptataan muunnoksella

$$C \equiv P^e \ (\mathrm{mod}\, p), \quad 0 \leq C < P. \quad (\text{Kryptausmuunnos})$$

Esimerkki Olkoon $p = 2633$ ja olkoon $e = 29$, jolloin $\text{syt}(e, p-1) = 1$. Nyt $m = 2$, ts. lohkot ovat 4-numeroisia. Kryptataan teksti THIS IS AN EXAMPLE (loppuun lisätään kirjaimia X tarpeen mukaan):

$$\begin{array}{cccccccc} TH & IS & IS & AN & EX & AM & PL & EX \\ 1907 & 0818 & 0818 & 0013 & 0423 & 0012 & 1511 & 0423 \end{array}$$

$$\downarrow \quad C \equiv P^{29} \text{ (mod 2633)}, \ 0 \leq C < 2633 \quad \downarrow$$

$$\begin{array}{cccccccc} 2199 & 1745 & 1745 & 1206 & 2437 & 2425 & 1729 & 2437 \end{array}$$

Esimerkiksi $1907^{29} \equiv 2199$ (mod 2633).

Miten dekryptaus suoritetaan?

Lause 5.3.1 Olkoon $p > 25$ alkuluku ja $e \in \mathbf{N}$ siten, että $\text{syt}(e, p-1) = 1$. Tällöin eksponentiaalisella muunnoksella

$$C \equiv P^e \ (\mathrm{mod}\, p), \quad 0 \leq C < p,$$

tuotettu kryptoteksti saadaan dekryptattua muunnoksella

$$P \equiv C^d \ (\mathrm{mod}\, p), \quad 0 \leq P < p,$$

missä d on luvun e käänteisluku modulo $p-1$.

Todistus. Olkoon $d = \overline{e}$ modulo $p-1$. Tällöin $de \equiv 1 \ (\mathrm{mod}\, p-1)$ eli $de = 1 + k(p-1)$ jollekin $k \in \mathbf{N}$. Jos

$$C \equiv P^e \ (\mathrm{mod}\, p),$$

niin

$$C^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{1+k(p-1)} \equiv P(P^{p-1})^k \equiv P \ (\mathrm{mod}\, p),$$

sillä Fermat'n pienen lauseen mukaan $P^{p-1} \equiv 1 \pmod{p}$. Huomaa, että $p \nmid P$ oletuksen $P < p$ seurauksena, koska voidaan olettaa, että $P > 0$ (Tapaus $P = 0$ triviaali). $\square$

Esimerkki Määrätään dekryptausmuunnos edellisen esimerkin tilanteessa. Siis $p = 2633$ ja $e = 29$. Nyt kongruenssin

$$29d \equiv 1 \,(\bmod 2632), \quad 0 \leq d \leq 2632,$$

ratkaisuksi saadaan $d = 2269$. Siis dekryptausmuunnos on

$$P \equiv C^{2269} \,(\bmod 2633).$$

Suorittamalla dekryptaus saadaan

$$\begin{array}{cccccccc} 2199 & 1745 & 1745 & 1206 & 2437 & 2425 & 1729 & 2437 \\ \downarrow & P \equiv C^{2269} \text{ (mod 2633)}, \ 0 \leq P < 2633 & & & & & & \downarrow \\ 1907 & 0818 & 0818 & 0013 & 0423 & 0012 & 1511 & 0423 \end{array}$$

Huomautus Luku e on ns. *kryptausavain*. Jos e ja p tunnetaan, kryptaus ja dekryptaus onnistuvat "nopeasti"suurillakin luvuilla, sillä modulaarisen potenssiinkorotuksen suorittamiseksi on olemassa tehokkaita algoritmeja. Ilman avainta e dekryptaaminen ei onnistu vaikka luku p olisi tiedossa.

5.4 RSA-salakirjoitus

Rivest, **S**hamir ja **A**dleman kehittivät 70-luvun lopulla eksponenttisalakirjoituksesta version, jossa kryptausavain voi olla julkisesti tiedossa ilman, että dekryptaus onnistuu.

Olkoon $n = pq$, missä p ja q ovat (käytännössä hyvin suuria) alkulukuja. Valitaan $e \in \mathbf{N}$ siten, että $\text{syt}(e, \phi(n)) = 1$.

Kuten edellä, selvätekstin kirjaimet korvataan 2-numeroisilla luvuilla ja ryhmitellään lohkoihin siten, että ehto $P < n$ pätee kaikille selvätekstilohkoille P. Nyt kryptausmuunnos on muotoa

$$C \equiv P^e \,(\bmod n), \quad 0 \leq C < n.$$

Lause 5.4.1 Olkoot p ja q erilliset alkuluvut ja $n = pq$. Olkoon $e \in \mathbf{N}$ siten, että $\text{syt}(e, \phi(n)) = 1$. Tällöin kryptausmuunnoksella

$$C \equiv P^e \,(\bmod n), \quad 0 \leq C < n$$

tuotettu kryptoteksti saadaan dekryptattua muunnoksella

$$P \equiv C^d \,(\bmod n), \quad 0 \leq P < n,$$

missä d on luvun e käänteisluku modulo $\phi(n)$.

Todistus. Käänteisluvun määritelmästä seuraa, että $ed = 1 + k\phi(n)$ jollekin $k \in \mathbf{N}$. Oletetaan, että $C \equiv P^e \pmod{n}$ ja jaetaan tarkastelu kahteen osaan seuraavasti:

1° Tapaus $\text{syt}(P, n) = 1$: Eulerin lauseen mukaan

$$P^{\phi(n)} \equiv 1 \pmod{n},$$

joten

$$C^d \equiv (P^e)^d \equiv P^{de} \equiv p^{1+k\phi(n)} \equiv P(P^{\phi(n)})^k \equiv P \pmod{n}.$$

2° Tapaus $\text{syt}(P, n) > 1$. Tällöin luvulla P on alkutekijänä p tai q. Olkoon esimerkiksi $p \mid P$. Koska $P < n$, on $P = pi$, missä $1 \leq i \leq q-1$. Näin ollen $q \nmid P$, joten Fermat'n pienen lauseen nojalla

$$P^{q-1} \equiv 1 \pmod{q}.$$

Eulerin funktiolle ϕ pätee $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$, joten

$$P^{\phi(n)} \equiv P^{(p-1)(q-1)} \equiv (P^{q-1})^{p-1} \equiv 1 \pmod{q}.$$

Koska $C \equiv P^e \pmod{q}$, saadaan

$$C^d \equiv P \pmod{q} \tag{20}$$

kuten tapauksessa 1°. Toisaalta $C \equiv P^e \pmod{p}$, joten

$$C^d \equiv P^{ed} = (pi)^{ed} \equiv 0 \equiv pi \equiv P \pmod{p}. \tag{21}$$

Yhdistämällä (20) ja (21) saadaan Lemman 3.3.5 nojalla

$$C^d \equiv P \pmod{n}.$$

□

Huomautus (a) Oletetaan, että RSA:n kryptokoodia tutkiva kryptanalyytikko löytää kryptatun luvun C, joka ei ole suhteellinen alkuluku moduloluvun n kanssa. Tällöin kryptanalyytikko pystyy faktoroimaan luvun n laskemalla Euklideen algoritmilla luvun $\text{syt}(C, n)$, joka on p tai q. Kuinka todennäköistä on, että tällainen luku löytyy?

Lukuja $C \in \{\, 0, 1, \ldots, n-1 \,\}$, jotka ovat suhteellisia alkulukuja luvun $n = pq$ kanssa, on

$$\phi(n) = (p-1)(q-1)$$

kappaletta. Siis vaaditun ehdon toteuttavia lukuja on

$$n - \phi(n) = pq - (p-1)(q-1) = pq - pq + p + q - 1 = p + q - 1$$

kappaletta. Näiden osuus luvuista $0, 1, \ldots, n-1$ on likimäärin

$$\frac{p+q+1}{pq} \approx \frac{p+q}{pq} = \frac{1}{q} + \frac{1}{p}.$$

Tyypillisesti vaaditaan, että luvut p ja q ovat molemmat suurempia kuin 10^{100}? Tällöin kysytty todennäköisyys on korkeintaan $2 \cdot 10^{-100}$.

(b) RSA:ssa luvun d ratkaiseminen edellyttää $\phi(n)$:n tuntemista. Huomaa, että $\phi(n)$:n selville saaminen on yhtä helppoa/vaikeaa kuin on luvun n faktoroiminen:
1° Jos $n = pq$ tunnetaan, $\phi(n) = (p-1)(q-1)$.
2° Jos $\phi(n)$ tunnetaan, p ja q saadaan yhtälöparista

$$\begin{cases} p+q = n - \phi(n) + 1 \\ p-q = \sqrt{(p+q)^2 - 4n}. \end{cases}$$

Näistä ylempi saadaan $\phi(n)$:n multiplikatiivisuusehdosta

$$\phi(n) = (p-1)(q-1) = pq - p - q + 1$$

ja alempi on trivialiteetti

$$(p-q)^2 = (p+q)^2 - 4pq$$

Esimerkiksi jos tiedetään, että $\phi(n) = 2436$ ja $n = 2537$, niin n:n kanoninen esitys saadaan yhtälöistä

$$\begin{aligned} p+q &= 2537 - 2436 + 1 = 102 \\ p-q &= \sqrt{102^2 - 4 \cdot 2537} = \sqrt{256} = 16. \end{aligned}$$

Laskemalla puolittain yhteen $2p = 118$ eli $p = 59$ ja sijoittamalla saadaan $q = 43$.

Esimerkki Olkoot $p = 43$, $q = 59$, jolloin $n = 43 \cdot 59 = 2537$ ja

$$\phi(n) = (43-1)(59-1) = 2436.$$

Nyt $2525 < n < 252525$, joten kukin lohko sisältää kaksi kirjainta. Tulkitaan koodi

$$0095 \quad 1648 \quad 1410 \quad 1299 \quad 1084\ ,$$

kun tiedetään että kryptaukseen on käytetty avainta $e = 13$. Koska luvut ovat pieniä, dekryptausavain pystytään ratkaisemaan yhtälöstä

$$ed \equiv 1 \ (\mathrm{mod}\, \phi(n))$$

eli yhtälöstä

$$13d \equiv 1 \ (\mathrm{mod}\, 2436).$$

Ratkaisuksi saadaan $d = 937$. Siis dekryptausmuunnos on

$$P \equiv C^{937} \ (\mathrm{mod}\, 2537), \quad 0 \leq P < 2537.$$

Laskemalla kutakin lukua C vastaavat selvätekstin lohkot P saadaan

$$\begin{aligned} 95^{937} &\equiv 1520 \ (\mathrm{mod}\ 2537) \Rightarrow \quad PU \\ 1648^{937} &\equiv 111 \ (\mathrm{mod}\ 2537) \Rightarrow \quad BL \\ 1410^{937} &\equiv 802 \ (\mathrm{mod}\ 2537) \Rightarrow \quad IC \\ 1299^{937} &\equiv 1004 \ (\mathrm{mod}\ 2537) \Rightarrow \quad KE \\ 1084^{937} &\equiv 2423 \ (\mathrm{mod}\ 2537) \Rightarrow \quad YX \end{aligned}$$

Siis salattu viesti on muotoa PUBLICKEY(X).

Esimerkki on *olennaisella tavalla harhaanjohtava; RSA:n käyttökelpoisuus perustuu nimenomaan siihen, että d:tä ei saada selville e:stä, kun käytetyt luvut ovat tarpeeksi suuria!*

Huomautus RSA on esimerkki ns. *julkinen avain (public key)-salakirjoitusmenetelmästä*. Tälle luonteenomainen piirre on se, että kryptausavaimen (tässä lukupari n, e), tunteminen ei johda dekryptausavaimen tuntemiseen (tässä lukupari n, d), jos p ja q ovat riittävän suuria. RSA:n julkisuus perustuu siihen, että alkulukutestaus on huomattavasti nopeammin toteuttavissa kuin faktorointi (=kanonisen esityksen etsiminen). Käytännössä kryptausavain voi olla monilla tahoilla yhteinen kunhan kullakin on oma dekryptausavaimensa, ks. Rosen, ss. 261–264.

6 Primitiivijuuret

6.1 Perusominaisuudet

Kertaluku Olkoon $m \in \mathbf{N}$ ja olkoon $a \in \mathbf{Z}$ siten, että $\text{syt}(a, m) = 1$. Eulerin lauseen mukaan

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

Siis joukko

$$A = \{\, k \in \mathbf{N} : a^k \equiv 1 \ (\mathrm{mod}\, m)\}$$

on epätyhjä. Joukon A pienintä alkiota sanotaan *luvun a kertaluvuksi modulo m*, ja sille käytetään merkintää $ord_m a$. Siis

$$ord_m a = \min\{\, k \in \mathbf{N} \mid a^k \equiv 1 \ (\mathrm{mod}\, m)\,\}.$$

Esimerkki Esimerkiksi $ord_7 2 = 3$, sillä

$$2^1 \equiv 2 \ (\mathrm{mod}\, 7), \quad 2^2 \equiv 4 \ (\mathrm{mod}\, 7), \quad 2^3 \equiv 8 \equiv 1 \ (\mathrm{mod}\, 7).$$

Vastaavasti $ord_7 6 = 2$, sillä $6^2 \equiv 36 \equiv 1 \ (\mathrm{mod}\, 7)$.

Lemma 6.1.1 Olkoon $m \in \mathbf{N}$ ja $a \in \mathbf{Z}$ siten, että $\text{syt}(a, m) = 1$. Tällöin $x \in \mathbf{N}$ toteuttaa ehdon $a^x \equiv 1 \ (\mathrm{mod}\, m)$ jos ja vain jos $ord_m a \mid x$.

Todistus. Jos $ord_m a \mid x$, niin $x = k \cdot ord_m a$ jollekin $k \in \mathbf{N}$. Näin ollen

$$a^x = a^{k \cdot ord_m a} = (a^{ord_m a})^k \equiv 1^k \equiv 1 \ (\mathrm{mod}\, m).$$

Olkoon kääntäen $a^x \equiv 1 \ (\mathrm{mod}\, m)$. Jakoyhtälön mukaan

$$x = q \cdot ord_m a + r, \quad 0 \leq r < ord_m a.$$

Saadaan

$$a^x = a^{q \cdot ord_m a + r} = (a^{ord_m a})^q a^r \equiv a^r \ (\mathrm{mod}\, m).$$

Siis $a^r \equiv 1 \ (\mathrm{mod}\, m)$. Mutta $0 \leq r < ord_m a$, joten kertaluvun määritelmän nojalla $r = 0$. Siis $ord_m a \mid x$. $\square$

Seuraus 6.1.2 Olkoon $m \in \mathbf{N}$ ja $a \in \mathbf{Z}$ siten, että $\text{syt}(a, m) = 1$. Tällöin $ord_m a \mid \phi(m)$.

Todistus. Väite seuraa Eulerin lauseesta ja Lemmasta 6.1.1. □

Esimerkki Määrätään $ord_{11}5$. Nyt $\phi(11) = 10$, jonka positiiviset tekijät ovat 1, 2, 5 ja 10. Nämä ovat ainoat ehdokkaat luvuksi $ord_{11}5$. Tutkimalla potenssit 2 ja 5 todetaan

$$5^2 \equiv 3 \ (\mathrm{mod}\, 11) \quad \text{ja} \quad 5^5 \equiv 3 \cdot 3 \cdot 5 = 45 \equiv 1 \ (\mathrm{mod}\, 11).$$

Näin ollen $ord_{11}5 = 5$.

Määritelmä 6.1.3 Olkoon $m \in \mathbf{N}$ ja $a \in \mathbf{Z}$ siten, että $\text{syt}(a, m) = 1$. Tällöin a on ***primitiivijuuri modulo*** m, jos

$$ord_m a = \phi(m).$$

Sopimus Jatkossa puhuttaessa kertaluvusta $ord_m a$ tai primitiivijuuresta a modulo m oletetaan automaattisesti, että ehto $\text{syt}(a, m) = 1$ on voimassa.

Huomautus Ehdosta $a^k \equiv 1 \ (\mathrm{mod}\, m)$, $k \in \mathbf{N}$, seuraa ehto $\text{syt}(a, m) = 1$. Jos nimittäin $a^k \equiv 1 \ (\mathrm{mod}\, m)$, niin $a^k - 1 = ml$ eli $a \cdot a^{k-1} - ml = 1$. Väite pätee Seurauksen 2.1.4 nojalla.

Huomautus 6.1.4 Olkoon $a \equiv b \ (\mathrm{mod}\, m)$. Tällöin $ord_m a = ord_m b$ olettaen, että kertaluku on olemassa (harjoitustehtävä).

Esimerkki Luvulla $m \in \mathbf{N}$ ei välttämättä ole primitiivijuurta. Esimerkiksi luvulla 8 ei ole, sillä ehdokkaat primitiivijuuriksi luvuista $1, \ldots, 7$ ovat 3, 5 ja 7. Näille pätee

$$ord_8 1 = 1, \quad ord_8 3 = ord_8 5 = ord_8 7 = 2 < 4 = \phi(8),$$

sillä

$$3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \ (\mathrm{mod}\, 8).$$

Lemma 6.1.5 Olkoon r primitiivijuuri modulo m. Tällöin joukko

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

on redusoitu jäännössysteemi modulo m.

Todistus. Huomaa, että $\text{syt}(r^i, m) = 1$ kaikilla $i \in \mathbf{N}$, sillä r^i:n alkutekijäjoukko on sama kuin r:n alkutekijäjoukko ja toisaalta $\text{syt}(r, m) = 1$. Riittää osoittaa, että

$$r^i \not\equiv r^j \ (\mathrm{mod}\, m)$$

aina kun $i, j \in \{1, \ldots, \phi(m)\}$, $i \neq j$. Tätä varten oletetaan vastoin väitettä, että

$$r^i \equiv r^j \ (\mathrm{mod}\, m),$$

missä $i > j$ ja $i, j \in \{1, \ldots, \phi(m)\}$. Tällöin

$$r^j \equiv r^i = r^j r^{i-j} \ (\mathrm{mod}\, m).$$

Mutta $\text{syt}(r^j, m) = 1$, joten supistussäännön seurauksena

$$r^{i-j} \equiv 1 \,(\bmod m).$$

Tämä on ristiriidassa ehdon $ord_m r = \phi(m)$ kanssa, sillä $1 \leq i - j < \phi(m)$. $\square$

Esimerkki (a) Luvulla 7 on primitiivijuuri 3. Nimittäin $\phi(7) = 6$, joten kertalukuehdokkaat ovat 2, 3 ja 6. Saadaan

$$3^2 \equiv 2 \,(\bmod 7), \quad 3^3 \equiv 6 \,(\bmod 7),$$

joten $ord_7 3 = 6 = \phi(7)$. Myös 5 on primitiivijuuri modulo 3.

(b) Tarkastellaan Lemman 6.1.5 väitettä primitiivijuurten 3 ja 5 (modulo 7) tapauksessa. Nyt $\phi(7) = 6$ ja

$$\begin{array}{lll} 3^1 \equiv 3 \,(\bmod 7), & 3^2 \equiv 2 \,(\bmod 7), & 3^3 \equiv 6 \,(\bmod 7), \\ 3^4 \equiv 4 \,(\bmod 7), & 3^5 \equiv 5 \,(\bmod 7), & 3^6 \equiv 1 \,(\bmod 7). \end{array}$$

Toisaalta

$$\begin{array}{lll} 5^1 \equiv 5 \,(\bmod 7), & 5^2 \equiv 4 \,(\bmod 7), & 5^3 \equiv 6 \,(\bmod 7), \\ 5^4 \equiv 2 \,(\bmod 7), & 5^5 \equiv 3 \,(\bmod 7), & 5^6 \equiv 1 \,(\bmod 7). \end{array}$$

Huomaa, että

$$3^{\frac{\phi(7)}{2}} \equiv -1 \,(\bmod 7) \quad \text{ja} \quad 5^{\frac{\phi(7)}{2}} \equiv -1 \,(\bmod 7).$$

Seuraus 6.1.6 Oletetaan, että luvulla $m \in \mathbf{N}$ on primitiivijuuri r. Tällöin

$$r^{\frac{\phi(m)}{2}} \equiv -1 \,(\bmod m).$$

Todistus. Harjoitustehtävä. $\square$

Kuinka monta primitiivijuurta luvulla m on, jos niitä on olemassa?

Jos $k \in \mathbf{N}$ ja $ord_m a$ on määritelty, niin

$$(a^k)^{ord_m a} = (a^{ord_m a})^k \equiv 1 \,(\bmod m).$$

Siis on selvää, että

$$ord_m a^k \leq ord_m a.$$

Mikä on tarkka tulos?

Lause 6.1.7 Olkoot $m, k \in \mathbf{N}$ ja $a \in \mathbf{Z}$ siten, että $\text{syt}(a, m) = 1$. Tällöin

$$ord_m a^k = \frac{ord_m a}{\text{syt}(ord_m a, k)}.$$

Erityisesti $ord_m a^k \mid ord_m a$.

Todistus. Olkoot $s = ord_m a^k$, $t = ord_m a$ ja $u = \text{syt}(t, k)$. Valitaan $t_1, k_1 \in \mathbf{N}$ siten, että $t = ut_1$ ja $k = uk_1$. On osoitettava, että $s = t_1$. Koska

$$(a^k)^{t_1} = (a^{uk_1})^{\frac{t}{u}} = a^{k_1 t} = (a^t)^{k_1} \equiv 1 \,(\bmod m),$$

niin Lemman 6.1.1 nojalla $s \mid t_1$. Toisaalta

$$a^{ks} \equiv (a^k)^s \equiv 1 \ (\mathrm{mod}\, m),$$

joten $t \mid ks$ (Lemma 6.1.1). Siis $ut_1 \mid uk_1 s$ eli $t_1 \mid k_1 s$. Lemman 3.1.6 nojalla

$$\text{syt}(t_1, k_1) = \text{ syt}(\frac{t}{u}, \frac{k}{u}) = 1,$$

joten Lemman 2.1.8 mukaan $t_1 \mid s$. Näin ollen $s = t_1$ eli

$$ord_m a^k = s = t_1 = \frac{t}{u} = \frac{ord_m a}{\text{syt}(ord_m a, k)}.$$

□

Esimerkki Edellä on todettu, että $ord_7 2 = 3$. Lauseen 6.1.7 nojalla

$$ord_7 64 = ord_7 2^6 = \frac{3}{\text{syt}(3,6)} = 1$$

ja

$$ord_7 128 = ord_7 2^7 = \frac{3}{\text{syt}(3,7)} = 3.$$

Seuraus 6.1.8 Olkoon r primitiivijuuri modulo m ja olkoon $k \in \mathbf{N}$. Tällöin r^k on primitiivijuuri modulo m jos ja vain jos $\text{syt}(k, \phi(m)) = 1$.

Todistus. Lauseen 6.1.7 mukaan

$$ord_m r^k = \frac{ord_m r}{\text{syt}(k, ord_m r)} = \frac{\phi(m)}{\text{syt}(k, \phi(m))}.$$

Siis $ord_m r^k = \phi(m)$ jos ja vain jos $\text{syt}(k, \phi(m)) = 1$. □

Esimerkki Seurauksen 6.1.8 avulla voidaan etsiä kaikki primitiivijuuret. Olkoon esimerkiksi $m = 11$. Tällöin 2 on eräs primitiivijuuri modulo 11, sillä 2,5, ja 10 ainoat kertalukuehdokkaat,

$$2^2 \equiv 4 \ (\mathrm{mod}\, 11) \quad \text{ja} \quad 2^5 \equiv 10 \ (\mathrm{mod}\, 11).$$

Lemman 6.1.5 mukaan joukko

$$\{\, 2, 2^2, \ldots, 2^{10} \,\}$$

on redusoitu jäännössysteemi modulo 11, joten se sisältää kaikki primitiivijuuriehdokkaat modulo 11. Seurauksen 6.1.8 mukaan

$$2, 2^2, 2^7, 2^9$$

ovat primitiivijuuria modulo 11 eikä muita ole, so. muista jäännösluokista modulo 11 ei löydy primitiivijuuria.

Lause 6.1.9 Jos luvulla $m \in \mathbf{N}$ on primitiivijuuri, sillä on täsmälleen $\phi(\phi(m))$ ei-kongruenttia primitiivijuurta modulo m.

Todistus. Olkoon r primitiivijuuri modulo m. Lemman 6.1.5 mukaan joukko

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

sisältää kaikki primitiivijuuriehdokkaat. Seurauksen 6.1.8 nojalla luku r^i, $i = 1, \ldots, \phi(m)$, on primitiivijuuri modulo m jos ja vain jos $\text{syt}(i, \phi(m)) = 1$. Tällaisia lukuja i on $\phi(\phi(m))$ kappaletta. □

Primitiivijuurten olemassaolosta voidaan todistaa (Rosen, ss. 290-296):

Lause 6.1.10 Luvulla $m > 1$ on primitiivijuuri jos ja vain jos

$$m \in \{ 2, 4, p^t, 2p^t \},$$

missä p on pariton alkuluku ja $t \in \mathbf{N}$.

Huomautus 6.1.11 Luvut, joilla on primitiivijuuri, käyttäytyvät eräissä suhteissa kuten alkuluvut. Esimerkiksi, jos luvulla $m \in \mathbf{N}$ on primitiivijuuri, niin

$$x^2 \equiv 1 \pmod{m} \iff x \equiv \pm 1 \pmod{m}.$$

Todetaan implikaatio vasemmalta oikealle (käänteinen triviaali). Oletetaan, että r on primitiivijuuri modulo m ja olkoon $x^2 \equiv 1 \pmod{m}$. Tällöin $\text{syt}(x, m) = 1$. Koska joukko

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

on redusoitu jäännössysteemi modulo m (Lemma 6.1.5), niin

$$r^i \equiv x \pmod{m}$$

jollakin $i = 0, 1, \ldots, \phi(m) - 1$. Tämä seuraa siitä, että x:n jakojäännös modulo m on jokin lukujen $1, r, \ldots, r^{\phi(m)-1}$ jakojäännöksistä modulo m Lemman 4.1.7 ja Huomautuksen 4.1.8 nojalla. Näin ollen

$$r^{2i} \equiv x^2 \equiv 1 \pmod{m},$$

joten $\phi(m) \mid 2i$ (Lemma 6.1.1). Siis $2i = k\phi(m)$ eli $i = k\frac{\phi(m)}{2}$. Seurauksen 6.1.6 nojalla

$$x \equiv r^i = r^{k\frac{\phi(m)}{2}} = (r^{\frac{\phi(m)}{2}})^k \equiv (-1)^k \equiv \pm 1 \pmod{m}.$$

6.2 Primitiivijuurten sovellutuksia

Lucasin alkulukutesti

Seuraava Lucasin alkulukutesti on lähtökohtana ns. Lucas-Lehmer-testissä, jota on menestyksellä käytetty suurten Mersenne-lukujen alkulukutestaukseen.

Lause 6.2.1 Olkoon $m > 1$. Jos on olemassa $x \in \mathbf{Z}$ siten, että

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

ja

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

kaikille luvun $m - 1$ alkutekijöille q, niin m on alkuluku.

Todistus. Koska $x^{m-1} \equiv 1 \pmod{m}$ ja $m-1 \geq 1$, niin $ord_m x \mid m-1$ Lemman 6.1.1 nojalla. Osoitetaan, että $ord_m x = m-1$. Tätä varten, oletetaan vastoin väitettä, että $ord_m x < m-1$. Tällöin $m-1 = k \cdot ord_m x$ jollekin $k \geq 2$. Olkoon q luvun k alkutekijä. Nyt q on luvun $m-1$ alkutekijä ja

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

On päädytty ristiriitaan lauseen oletusten kanssa, joten

$$m-1 = ord_m x \leq \phi(m) \leq m-1.$$

Siis $\phi(m) = m-1$ eli m on alkuluku. $\square$

Huomautus (a) Lauseessa 6.2.1 x on välttämättä primitiivijuuri modulo m, sillä $ord_m x = \phi(m)$. Lause 6.2.1 ei sellaisenaan sovellu yleiseksi alkulukutestiksi, sillä se edellyttää luvun $m-1$ alkutekijöiden tuntemista. Tietyissa erikoistapauksissa, joissa luvun $m-1$ alkutekijät tunnetaan, lauseesta saadaan käyttökelpoinen alkulukutesti. Tällaisia tapauksia ovat mm. Fermat'n luvut $F_n = 2^{2^n} + 1$.

(b) Lucas todisti vuonna 1876, että Mersenne-luku

$$M_{127} = 2^{127} - 1$$

on alkuluku. Tämä pysyi suurimpana tunnettuna alkulukuna aina vuoteen 1951 saakka ja jäänee historiaan suurimpana käsin laskien löydettynä alkulukuna.

Pseudosatunnaisluvut

Mm. tietokonesimulaatioita varten on tarpeen kyetä tuottamaan "satunnaislukuja"tietokoneella. Seuraava lineaarisen kongruenssin metodi on paljon käytetty:

Valitaan $m \in \mathbf{N}$ ja $a, c, x_0 \in \mathbf{Z}$ siten, että $2 \leq a < m$, $0 \leq c < m$ ja $0 \leq x_0 < m$. Konstruoidaan *pseudosatunnaislukujono* (x_i) rekursiivisesti ehdosta

$$x_{i+1} \equiv a x_i + c \pmod{m}, \quad 0 \leq x_{i+1} < m,$$

missä $i = 0, 1, \ldots$. Luku x_0 on *syöte*. Jos $c = 0$, puhutaan *puhtaasti multiplikatiivisesta metodista*.

Esimerkki 6.2.2 (a) Olkoon $m = 12$, $a = 3$, $c = 4$ ja $x_0 = 5$. Tällöin

$$\begin{aligned} x_1 &\equiv 3 \cdot 5 + 4 \equiv 7 \pmod{12}, \\ x_2 &\equiv 3 \cdot 7 + 4 \equiv 1 \pmod{12}, \\ x_3 &\equiv 3 \cdot 1 + 4 \equiv 7 \pmod{12}, \\ x_4 &\equiv 1 \pmod{12}. \end{aligned}$$

Lukujonoksi saadaan $5, 7, 1, 7, 1, \ldots$. Tämän tyyppinen jono ei ole hyvä, koska siinä esiintyy lyhyt sykli!

(b) Olkoon $m = 9$, $a = 7$, $c = 4$ ja $x_0 = 3$. Tällöin

$$\begin{aligned}
x_1 &\equiv 7 \cdot 3 + 4 \equiv 7 \,(\mathrm{mod}\, 9),\\
x_2 &\equiv 7 \cdot 7 + 4 \equiv 8 \,(\mathrm{mod}\, 9),\\
x_3 &\equiv 7 \cdot 8 + 4 \equiv 6 \,(\mathrm{mod}\, 9),\\
x_4 &\equiv 7 \cdot 6 + 4 \equiv 1 \,(\mathrm{mod}\, 9),\\
x_5 &\equiv 7 \cdot 1 + 4 \equiv 2 \,(\mathrm{mod}\, 9),\\
x_6 &\equiv 7 \cdot 2 + 4 \equiv 0 \,(\mathrm{mod}\, 9),\\
x_7 &\equiv 7 \cdot 0 + 4 \equiv 4 \,(\mathrm{mod}\, 9),\\
x_8 &\equiv 7 \cdot 4 + 4 \equiv 5 \,(\mathrm{mod}\, 9),\\
x_9 &\equiv 7 \cdot 5 + 4 \equiv 3 \,(\mathrm{mod}\, 9).
\end{aligned}$$

Tässä tapauksessa sykli on pisin mahdollinen eli kaikki mahdolliset jakojäännökset käydään läpi.

Sopimus Lineaarisen kongruenssin metodissa *jakson pituus* tarkoittaa peräkkäisten lukujen maksimaalista lukumäärää ilman toistoa, kun syötettä ei lasketa.

Metodin toimivuuden kannalta jakson pituuden tulee olla riittävän suuri. Välttämätön ehto tälle on se, että modululoku on riittävän suuri.

Lemma 6.2.3 Lineaarisen kongruenssin metodilla konstruoitava lukujono (x_i) saadaan ehdosta

$$x_i \equiv a^i x_0 + c\left(\frac{a^i - 1}{a - 1}\right) \,(\mathrm{mod}\, m), \quad 0 \leq x_i < m.$$

Todistus. Induktiotodistus (harjoitustehtävä). □

Puhtaasti mutliplikatiivinen metodi Tarkastellaan lähemmin puhtaasti multiplikatiivista metodia

$$x_i \equiv a^i x_0 \,(\mathrm{mod}\, m).$$

Jos nyt l on jakson pituus, niin $l = j - i$, missä

$$x_j \equiv a^j x_0 \equiv a^i x_0 \equiv x_i \,(\mathrm{mod}\, m)$$

ja luvut $x_i, x_{i-1}, \ldots, x_{j-1}$ ovat pareittein ei-kongruentteja modulo m. Jos $\mathrm{syt}(x_0, m) = 1$ ja $\mathrm{syt}(a, m) = 1$, niin supistussäännön nojalla ehdosta

$$a^j x_0 \equiv a^i x_0 \,(\mathrm{mod}\, m)$$

seuraa, että

$$a^{j-i} x_0 \equiv x_0 \,(\mathrm{mod}\, m).$$

Tästä saadaan edelleen

$$a^{j-i} \equiv 1 \,(\mathrm{mod}\, m).$$

Siis

$$a^l \equiv 1 \,(\mathrm{mod}\, m).$$

Lemman 6.1.1 mukaan $ord_m a \mid l$. Jos erityisesti a on primitiivijuuri modulo m ja m on alkuluku, niin $ord_m a = \phi(m) = m - 1$. Tällöin välttämättä $l = m - 1$, mikä on optimaalinen tilanne.

Käytännössä on oltava takeet siitä ettei Esimerkin 6.2.2 (a) tilanne voi esiintyä. Puhtaasti multiplikatiivisessa metodissa modulolukuna käytetään mm. Mersenne-alkulukua

$$M_{31} = 2^{31} - 1 = 2147483647$$

ja sen sopivaa primitiivijuurta kertoimena a. Primitiivijuuren käyttö takaa sen, että jakson pituus on maksimaalinen.

Lemma 6.2.4 Luku 7 on luvun M_{31} primitiivijuuri.

Todistus. Riittää osoittaa, että

$$7^{\frac{M_{31}-1}{q}} \not\equiv 1 \pmod{M_{31}} \tag{22}$$

kaikille luvun $M_{31} - 1$ alkutekijöille, ks. harjoitustehtävä. Luvun $M_{31} - 1$ kanoninen esitys on

$$M_{31} - 1 = 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331.$$

Nyt kongruenssiehto (22) voidaan todeta tietokoneella kaikille $q \in \{2, 3, 7, 11, 31, 151, 331\}$. Esimerkiksi

$$7^{\frac{M_{31}-1}{2}} \equiv 1661280733 \pmod{M_{31}}.$$

□

Esimerkki Konstruoidaan malliksi lukuja x_i metodilla käyttäen kertoimena lukua 7 ja modulolukuna lukua M_{31}. Siis

$$x_{i+1} \equiv 7x_i \pmod{M_{31}}, \quad 0 \leq x_{i+1} < M_{31}.$$

Lisäksi valitaan syöte $x_0 = 2$. Nyt jonon ensimmäiset luvut ovat

$$x_1 = 2 \cdot 7,\ x_2 = 2 \cdot 7^2,\ x_3 = 2 \cdot 7^3, \ldots, x_{10} = 2 \cdot 7^{10} = 564950498.$$

Koska modululoku on verrattain suuri, ongelmana on se, että 10 ensimmäistä lukua saadaan suoraan rekursiokaavasta ilman jakojäännöksen ottamista. Tämän ongelman poistamiseksi korvataan primitiivijuuri 7 riittävän suurella toisella primitiivijuurella. Seurauksen 6.1.8 mukaan 7^k on primitiivijuuri jos ja vain jos $\text{syt}(k, M_{31} - 1) = 1$. Esimerkiksi voidaan valita $k = 5$ tai $k = 13$, jolloin

$$7^5 = 16807, \quad 7^{13} \equiv 252246292 \pmod{M_{31}}.$$

Konstruoidaan malliksi lukuja x_i metodilla

$$x_{i+1} \equiv 16807x_i \pmod{M_{31}}, \quad 0 \leq x_{i+1} < M_{31},$$

kun $x_0 = 2$. Nyt jonon alkupään luvuiksi saadaan

$$\begin{aligned}
x_1 &\equiv 2 \cdot 16807 \equiv 33614 \pmod{M_{31}},\\
x_2 &\equiv 2 \cdot 16807^2 \equiv 564950498 \pmod{M_{31}},\\
x_3 &\equiv 2 \cdot 16807^3 \equiv 1097816499 \pmod{M_{31}},\\
x_4 &\equiv 2 \cdot 16807^4 \equiv 1969887316 \pmod{M_{31}},\\
x_5 &\equiv 2 \cdot 16807^5 \equiv 140734213 \pmod{M_{31}}.
\end{aligned}$$

Tässä jo x_3 saadaan jakojäännöksenä.

6.3 Lagrangen lause

Olkoon f kokonaislukukertoiminen polynomi ja $m \in \mathbf{N}$. Tällöin $x_0 \in \mathbf{Z}$ on polynomin f *juuri modulo* m, jos

$$f(x_0) \equiv 0 \ (\mathrm{mod}\, m).$$

Olkoon $a \equiv b \ (\mathrm{mod}\, m)$. Tällöin a on polynomin f juuri modulo m jos ja vain jos b on polynomin f juuri modulo m. Jos nimittäin

$$f(x) := a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

ja $a \equiv b \ (\mathrm{mod}\, m)$, niin $a_i a^i \equiv a_i b^i \ (\mathrm{mod}\, m)$ kaikilla $i = 0, 1, \ldots, n$, mistä edelleen seuraa, että

$$f(a) \equiv f(b) \ (\mathrm{mod}\, m).$$

Jos nyt $f(a) \equiv 0 \ (\mathrm{mod}\, m)$, niin transitiivisuuden nojalla $f(b) \equiv 0 \ (\mathrm{mod}\, m)$ ja kääntäen ehdosta $f(b) \equiv 0 \ (\mathrm{mod}\, m)$ seuraa ehto $f(a) \equiv 0 \ (\mathrm{mod}\, m)$.

Sopimus Puhuttaessa juurien lukumäärästä modulo m tarkoitetaan pareittain ei-kongruenttien juurien lukumäärää.

Lause 6.3.1 (Lagrangen lause) Olkoon p alkuluku ja olkoon

$$f(x) := a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

polynomi, jolle $a_i \in \mathbf{Z}$ ja $p \nmid a_n$, ts. $a_n \not\equiv 0 \ (\mathrm{mod}\, p)$. Tällöin polynomilla f on korkeintaan n juurta modulo p.

Todistus. Todistetaan väite induktiolla asteen n suhteen:

1° Olkoon $f(x) = a_1 x + a_0$, missä $p \nmid a_1$. Nyt $x \in \mathbf{Z}$ on juuri modulo p täsmälleen silloin kun $a_1 x \equiv -a_0 \ (\mathrm{mod}\, p)$. Tällä yhtälöllä on yksikäsitteinen ratkaisu Lauseen 3.2.3 nojalla, sillä $\mathrm{syt}(a_1, p) = 1$.

2° Oletetaan, että väite pätee kaikille astetta $n-1$ oleville polynomeille, $n \geq 2$. Olkoon f astetta n oleva polynomi, jolle $p \nmid a_n$. Tehdään antiteesi eli oletetaan, että f:llä on $n+1$ juurta modulo p. Olkoon nämä juuret $c_0, c_1, \ldots, c_n$, ts. $f(c_k) \equiv 0 \ (\mathrm{mod}\, p)$ kaikilla $i = 0, 1, \ldots n$. Tällöin

$$\begin{aligned} f(x) - f(c_0) &= a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0) \\ &= a_n(x - c_0)(x^{n-1} + x^{n-2}c_0 + \cdots + xc_0^{n-2} + c_0^{n-1}) + \cdots \\ &+ a_{n-1}(x - c_0)(x^{n-2} + x_{n-3}c_0 + \cdots + xc_0^{n-3} + c_0^{n-2}) + \cdots \\ &+ a_2(x - c_0)(x + c_0) + a_1(x - c_0) = (x - c_0)g(x), \end{aligned}$$

missä g on astetta $n-1$ oleva polynomi, jonka korkeimman potenssin kerroin on a_n. Riittää osoittaa, että $c_1, \ldots, c_n$ ovat polynomin g juuria modulo p, koska tämä on ristiriidassa induktio-oletuksen kanssa. Jos $k \in \{1, \ldots, n\}$, niin

$$f(c_k) \equiv 0 \equiv f(c_0) \ (\mathrm{mod}\, p),$$

joten

$$0 \equiv f(c_k) - f(c_0) = (c_k - c_0)g(c_k) \ (\mathrm{mod}\, p).$$

Nyt Lemman 2.3.2 seurauksena $g(c_k) \equiv 0 \pmod p$, sillä antiteesin mukaan $c_k - c_0 \not\equiv 0 \pmod p$ eli syt$(c_k - c_0, p) = 1$. $\square$

Esimerkki (a) Olkoon $p > 2$ alkuluku. Tällöin kongruenssilla

$$2x^2 \equiv 1 \pmod p$$

on korkeintaan kaksi ratkaisua modulo p Lagrangen lauseen nojalla. Jos $p = 3$, ratkaisuja ei ole, sillä $0, 1, 2$ eivät ole ratkaisuja. Jos $p = 7$, niin $x = \pm 2$ ovat kaksi eri ratkaisua modulo 7.

(b) Kongruenssilla $x^2 \equiv x \pmod 6$ on neljä ratkaisua $x = 0, 1, 3, 4$. Nyt moduloluku ei ole alkuluku.

Huomautus Mitä tiedämme tähän mennessä juurten lukumäärästä?

(a) Luvun 2 metodein voidaan päätellä, että kongruenssilla

$$x^2 \equiv 1 \pmod{p^k}$$

on täsmälleen kaksi ratkaisua $x \equiv \pm 1 \pmod{p^k}$, jos p on alkuluku ja $k \in \mathbf{N}$ siten, että $p^k \neq 2$.

(b) Eulerin lause sanoo, että kongruenssilla

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

on täsmälleen $\phi(m)$ ratkaisua modulo m.

Eulerin lauseen antamaa tietoa voidaan parantaa Lagrangen lauseen avulla seuraavasti:

Seuraus 6.3.2 Olkoon p alkuluku ja olkoon $d \in \mathbf{N}$, $d \mid p - 1$. Tällöin kongruenssilla

$$x^d \equiv 1 \pmod p$$

on täsmälleen d ratkaisua modulo p.

Todistus. Olkoon $p - 1 = de$. Tällöin

$$x^{p-1} - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1) =: (x^d - 1)g(x).$$

Nyt Fermat'n pienen lauseen perusteella polynomilla $x^{p-1} - 1$ on $p-1$ juurta $1, \ldots, p-1$ modulo p. Lisäksi jokainen näistä juurista on joko polynomin $x^d - 1$ juuri modulo p tai polynomin g juuri modulo p Lemman 2.3.2 seurauksena. Jos nimittäin $p \mid x^{p-1} - 1$ ja esimerkiksi $p \nmid g(x)$, niin Lemman 2.3.2 mukaan $p \mid x^d - 1$.

Lagrangen lauseen nojalla g:llä on korkeintaan $d(e-1) = de - d = p - d - 1$ juurta modulo p. Näin ollen polynomilla $x^d - 1$ on vähintään $p - 1 - (p - d - 1) = d$ juurta modulo p. Toisaalta Lagrangen lause kertoo sen, että polynomilla $x^d - 1$ on korkeintaan d juurta modulo p. Väite seuraa. $\square$

Lause 6.3.3 Olkoon p alkuluku ja olkoon $d \in \mathbf{N}$, $d \mid p - 1$. Tällöin on olemassa täsmälleen $\phi(d)$ ei-kongruenttia lukua, joiden kertaluku modulo p on d.

Todistus. Täsmällinen todistus sivuutetaan. Todistus yhdistää luvun 6.1 avaintulokset, Seurauksen 6.3.2 ja Eulerin funktion multiplikatiivisuudesta seuraavan ominaisuuden

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

ks. Rosen, ss. 286–287. □

Seuraus 6.3.4 Jokaisella alkuluvulla on primitiivijuuri.

Todistus. Olkoon p alkuluku. Jos $d := p - 1 = \phi(p)$, niin Lauseen 6.3.3 mukaan on olemassa täsmälleen $\phi(\phi(p))$ ei-kongruenttia lukua, joiden kertaluku modulo p on $\phi(p)$. Kyseiset luvut ovat primitiivijuuria. □

7 Neliönjäännökset

7.1 Perusominaisuudet

Esimerkki Yhtälöllä

$$x^2 \equiv 1 \pmod{m}$$

on aina ratkaisu $x \equiv \pm 1 \pmod{m}$. Mitä esimerkiksi yhtälön $x^2 \equiv 2 \pmod{m}$ ratkaisuista voidaan sanoa?

Määritelmä 7.1.1 Olkoon $m \in \mathbf{N}$. Tällöin $a \in \mathbf{Z}$ on luvun $x \in \mathbf{Z}$ *neliönjäännös modulo* m (tai lyhyesti neliönjäännös modulo m), jos $\text{syt}(a, m) = 1$ ja

$$x^2 \equiv a \pmod{m}.$$

Huomautus Ehto $\text{syt}(a, m) = 1$ *ei ole välttämätön* edellytys ehdon

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

toteutumiselle jollekin $x \in \mathbf{Z}$. Esimerkiksi $4^2 \equiv 2 \pmod{14}$ vaikka $\text{syt}(2, 14) = 2 > 1$.

Esimerkki Olkoon $m = 11$. Nyt

$$\begin{aligned}
1^2 &\equiv 10^2 \equiv 1 \pmod{11}, \\
3^2 &\equiv 8^2 \equiv 9 \pmod{11}, \\
6^2 &\equiv 5^2 \equiv 3 \pmod{11}, \\
2^2 &\equiv 9^2 \equiv 4 \pmod{11}, \\
4^2 &\equiv 7^2 \equiv 5 \pmod{11},
\end{aligned}$$

joten neliönjäännöksiä modulo 11 ovat 1,3,4,5 ja 9. Luonnollisesti kaikki neliönjäännökset löydetään tutkimalla luvut $x \in \{1, \ldots, m-1\}$.

Lemma 7.1.2 Olkoon $p > 2$ alkuluku ja olkoon $a \in \mathbf{Z}$ siten, että $p \nmid a$. Tällöin joko a ei ole neliönjäännös modulo p tai on olemassa täsmälleen kaksi ei-kongruenttia lukua modulo p, joiden neliönjäännös a on.

Todistus. Oletetaan, että a on luvun x_0 neliönjäännös modulo p, ts.

$$x_0^2 \equiv a \pmod{p}.$$

Tällöin $(-x_0)^2 \equiv a \pmod{p}$. Lisäksi $x_0 \not\equiv -x_0 \pmod{p}$, sillä jos $x_0 \equiv -x_0 \pmod{p}$, niin $p \mid 2x_0$ ja ehdosta syt$(2, p) = 1$ seuraa, että $p \mid x_0$. Tällöin $x_0 \equiv 0 \pmod{p}$ eli $x_0^2 \equiv 0 \pmod{p}$, mistä edelleen seuraa $a \equiv 0 \pmod{p}$. Tämä on ristiriidassa oletuksen $p \nmid a$ kanssa. Siis on olemassa vähintään kaksi ei-kongruenttia lukua modulo p, joiden neliönjäännös a on.

Olkoon lopuksi $x_1 \in \mathbf{Z}$ mielivaltainen siten, että

$$x_1^2 \equiv a \pmod{p}. \tag{23}$$

Tällöin

$$x_0^2 \equiv a \equiv x_1^2 \pmod{p},$$

joten $p \mid x_0^2 - x_1^2$. Siis $p \mid (x_0 - x_1)(x_0 + x_1)$ ja koska p on alkuluku, niin $p \mid x_0 - x_1$ tai $p \mid x_0 + x_1$. Siis $x_0 \equiv x_1 \pmod{p}$ tai $-x_0 \equiv x_1 \pmod{p}$. Jokainen kongruenssin (23) ratkaisu x_1 on siis joko x_0:n tai $-x_0$:n määräämästä kongruenssiluokasta. □

Lause 7.1.3 Olkoon $p > 2$ alkuluku. Tällöin on olemassa täsmälleen $\frac{p-1}{2}$ ei-kongruenttia neliönjäännöstä modulo p.

Todistus. Luku 0 ei kelpaa neliönjäännökseksi, sillä syt$(0, p) = p > 1$. Jos määrätään neliön x^2 jakojäännös a modulo p kullakin $x = 1, \ldots, p-1$, ts.

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

niin Lemman 7.1.2 nojalla myös $p - x$ toteuttaa ehdon $(p-x)^2 \equiv a \pmod{p}$ ja muita ratkaisuja ei ole joukossa $\{1, \ldots, p-1\}$. Koska tarkasteltavia neliöitä on $p - 1$ kpl, saadaan $\frac{p-1}{2}$ ei-kongruenttia lukua modulo p jakojäännökseksi a. □

Määritelmä 7.1.4 Olkoon $p > 2$ alkuluku ja $a \in \mathbf{Z}$ siten, että $p \nmid a$. Tällöin *Legendren symboli* $\left[\frac{a}{p}\right]$ määritellään asettamalla

$$\left[\frac{a}{p}\right] = \begin{cases} 1, & \text{jos a on neliönjäännös modulo } p \\ -1, & \text{jos a ei ole neliönjäännös modulo } p \end{cases}$$

Esimerkki Esimerkiksi pätee

$$\left[\frac{4}{5}\right] = 1 = \left[\frac{1}{5}\right], \ \left[\frac{2}{5}\right] = \left[\frac{3}{5}\right] = -1,$$

sillä

$$1^2 \equiv 1 \pmod{5}, \ 2^2 \equiv 4 \pmod{5}, \ 3^2 \equiv 4 \pmod{5}, \ 4^2 \equiv 1 \pmod{5}.$$

Lause 7.1.5 (Eulerin kriteeri) Olkoon $p > 2$ alkuluku ja olkoon $a \in \mathbf{Z}$ siten, että $p \nmid a$. Tällöin

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

Todistus. Oletetaan ensin, että $\left[\frac{a}{p}\right] = 1$, ts. on olemassa $x_0 \in \mathbf{Z}$ siten, että $x_0^2 \equiv a \pmod{p}$. Fermat'n pienen lauseen nojalla

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 = \left[\frac{a}{p}\right] \pmod{p}.$$

Huomaa, että $p \nmid x_0$, ts. Fermat'n pientä lausetta voidaan soveltaa. Jos nimittäin $p \mid x_0$, niin $x_0 \equiv 0 \pmod{p}$ ja edelleen $a \equiv x_0^2 \equiv 0 \pmod{p}$. Siis $p \mid a$, mikä on ristiriita.

Oletetaan, että $\left[\frac{a}{p}\right] = -1$, ts. kongruenssilla $x^2 \equiv a \pmod{p}$ ei ole ratkaisua. Tiedetään, että jokaisella $1 \leq i \leq p-1$ on olemassa yksikäsitteinen ratkaisu kongruenssille

$$ix \equiv a \pmod{p}. \tag{24}$$

Olkoon j yhtälön (24) ratkaisun x jakojäännös modulo p. Nyt $1 \leq j \leq p-1$, sillä jos $j = 0$, niin $a \equiv 0 \pmod{p}$ eli $p \mid a$. Lisäksi, koska kongruenssilla $x^2 \equiv a \pmod{p}$ ei ole ratkaisuja, niin $i \neq j$ kaikilla $i = 1, \ldots, p-1$. Näin ollen luvut $1, \ldots, p-1$ voidaan ryhmitellä $\frac{p-1}{2}$:een pariin, joiden tulot ovat kongruentteja a:n kanssa modulo p. Kertomalla kaikki tulot keskenään saadaan

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

Wilsonin lauseen (Lause 3.4.2) mukaan

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

joten kongruenssi

$$a^{\frac{p-1}{2}} \equiv -1 \equiv \left[\frac{a}{p}\right]$$

pätee myös tässä tapauksessa. □

Esimerkki (a) Olkoon $p = 23$ ja $a = 5$. Koska

$$5^{\frac{23-1}{2}} = 5^{11} \equiv -1 \pmod{23},$$

niin Eulerin kriteerin mukaan kongruenssilla $x^2 \equiv 5 \pmod{23}$ ei ole ratkaisua.

(b) Olkoon r primitiivijuuri modulo p, missä $p > 2$ on alkuluku. Tällöin Seurauksen 6.1.6 nojalla

$$r^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

joten Eulerin kriteeristä nähdään, että kongruenssilla $x^2 \equiv r \pmod{p}$ ei ole ratkaisua.

Huomautus Eulerin kriteeri on käytännön laskujen kannalta hyödyllinen, koska se muuttaa kysymyksen neliönjäännöksen olemassaolosta modulaariseksi potenssiin korotukseksi.

Lemma 7.1.6 Olkoon $p > 2$ alkuluku ja olkoot $a, b \in \mathbf{Z}$ siten, että $p \nmid a$ ja $p \nmid b$. Tällöin

(i) $\left[\frac{a}{p}\right] = \left[\frac{b}{p}\right]$ aina kun $a \equiv b \pmod{p}$;

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

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

Todistus. Kohta (iii) on triviaali, sillä $(\pm a)^2 \equiv a^2 \pmod p$.

(i) Olkoon $a \equiv b \pmod p$. Tällöin transitiivisuuden ja symmetrisyyden seurauksena

$$x^2 \equiv a \pmod p \iff x^2 \equiv b \pmod p,$$

joten väite seuraa helposti.

(ii) Harjoitustehtävä. □

Esimerkki 7.1.7 (a) Eulerin kriteeristä seuraa, että alkuluvulla $p > 2$ on neliönjäännöksenä -1 jos ja vain jos $p \equiv 1 \pmod 4$ (harjoitustehtävä).

(b) Oletetaan, että $p \equiv 1 \pmod 4$ ja a on neliönjäännös modulo p. Tällöin myös $-a$ on neliönjäännös modulo p, sillä kohdan (a) sekä Lemman 7.1.6 kohdan (ii) nojalla voidaan kirjoittaa

$$\left[\frac{-a}{p}\right] = \left[\frac{-1}{p}\right]\left[\frac{a}{p}\right] = 1^2 = 1.$$

Vastaavasti tapauksessa $p \equiv 3 \pmod 4$ oletuksesta a on neliönjäännös modulo p seuraa

$$\left[\frac{-a}{p}\right] = \left[\frac{-1}{p}\right]\left[\frac{a}{p}\right] = -1 \cdot 1 = -1.$$

7.2 Elektroninen kolikonheitto

Esimerkki 7.2.1 Oletetaan, että $p \equiv 3 \pmod 4$ ja että $\left[\frac{a}{p}\right] = 1$. Tällöin

$$\frac{p+1}{4} = \frac{4k+3+1}{4} = k+1 \in \mathbf{N}$$

ja kongruenssin $x^2 \equiv a \pmod p$ ratkaisu saadaan seuraavasti: Eulerin kriteerin mukaan

$$a^{\frac{p-1}{2}} \equiv \left[\frac{a}{p}\right] = 1 \pmod p,$$

joten

$$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a \equiv a \pmod p.$$

Siis

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod p$$

ovat kongruenssin $x^2 \equiv a \pmod p$ ainoat ratkaisut (Lemma 7.1.2).

Lause 7.2.2 Olkoon $n = pq$, missä p ja q ovat erilliset parittomat alkuluvut. Jos $\text{syt}(a, n) = 1$, niin kongruenssilla

$$x^2 \equiv a \pmod n \tag{25}$$

on täsmälleen neljä ei-kongruenttia ratkaisua modulo n, mikäli yksi ratkaisu on olemassa.

Todistus. Oletetaan, että x_0 on kongruenssin (25) ratkaisu. Olkoot

$$\begin{aligned} x_0 &\equiv x_1 \pmod{p}, \quad 0 \leq x_1 \leq p, \\ x_0 &\equiv x_2 \pmod{q}, \quad 0 \leq x_2 \leq q, \end{aligned}$$

ts. x_1 ja x_2 ovat x_0:n jakojäännökset modulo p ja modulo q. Lemman 7.1.2 nojalla kongruenssilla

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

on täsmälleen kaksi ei-kongruenttia ratkaisua, koska x_0 on eräs ratkaisu. Nämä ratkaisut ovat $\pm x_1 \pmod{p}$. Vastaavasti kongruenssilla

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

on täsmälleen kaksi ei-kongruenttia ratkaisua, jotka ovat $\pm x_2 \pmod{q}$. Huomaa, että x on kongruenssin (25) ratkaisu jos ja vain jos x on yhtälöparin

$$\begin{cases} x^2 \equiv a \pmod{p} \\ x^2 \equiv a \pmod{q} \end{cases} \tag{26}$$

ratkaisu. Tässä implikaatio vasemmalta oikealle on triviaali ja käänteinen implikaatio pätee Lemman 3.3.5 nojalla.

Koska

$$x^2 \equiv a \pmod{p} \iff x \equiv \pm x_1 \pmod{p}$$

ja

$$x^2 \equiv a \pmod{q} \iff x \equiv \pm x_2 \pmod{q},$$

niin x on yhtälöparin (26) ratkaisu jos ja vain jos jokin seuraavista neljästä vaihtoehdosta toteutuu:

$$\text{(i)} \begin{cases} x \equiv x_1 \pmod{p} \\ x \equiv x_2 \pmod{q}, \end{cases}$$

$$\text{(ii)} \begin{cases} x \equiv x_1 \pmod{p} \\ x \equiv -x_2 \pmod{q}, \end{cases}$$

$$\text{(iii)} \begin{cases} x \equiv -x_1 \pmod{p} \\ x \equiv x_2 \pmod{q}, \end{cases}$$

$$\text{(iv)} \begin{cases} x \equiv -x_1 \pmod{p} \\ x \equiv -x_2 \pmod{q}. \end{cases}$$

Kiinalainen jäännöslause sanoo, että kullakin yhtälöparilla (i)-(iv) on täsmälleen yksi ratkaisu modulo n. Yhtälöparien (i)-(iv) ratkaisut ovat pareittain ei-kongruentit modulo n (harjoitustehtävä). $\square$

Esimerkki 7.2.3 Olkoon $n = 11021 = 103 \cdot 107$ ja tarkastellaan yhtälön

$$x^2 \equiv 860 \pmod{11021} \tag{27}$$

ratkaisuja. Nyt $p \equiv q \equiv 3 \pmod{4}$, joten kaikki neljä ratkaisua löydetään Esimerkin 7.2.1 ja Lauseen 7.2.2 keinoin: Ratkaistaan ensin kongruenssit

$$x^2 \equiv 860 \equiv 36 \pmod{103} \quad \text{ja} \quad x^2 \equiv 860 \equiv 4 \pmod{107}$$

Esimerkin 7.2.1 mukaisesti. Ensimmäisen yhtälön ratkaisuiksi saadaan

$$x \equiv \pm 36^{\frac{103+1}{4}} \equiv \pm 36^{26} \equiv \pm 6 \ (\mathrm{mod}\, 103)$$

ja toisen ratkaisuiksi saadaan

$$x \equiv \pm 4^{\frac{107+1}{4}} \equiv \pm 4^{27} \equiv \pm 2 \ (\mathrm{mod}\, 107).$$

Kongruenssin $x^2 \equiv 860 \ (\mathrm{mod}\, 11021)$ ratkaisut saadaan Kiinalaisen jäännöslauseen avulla ratkaisemalla yhtälöparit (i)-(iv):

$$\text{(i)} \begin{cases} x \equiv 6 \ (\mathrm{mod}\, 103) \\ x \equiv 2 \ (\mathrm{mod}\, 107), \end{cases}$$

$$\text{(ii)} \begin{cases} x \equiv 6 \ (\mathrm{mod}\, 103) \\ x \equiv -2 \ (\mathrm{mod}\, 107), \end{cases}$$

$$\text{(iii)} \begin{cases} x \equiv -6 \ (\mathrm{mod}\, 103) \\ x \equiv 2 \ (\mathrm{mod}\, 107), \end{cases}$$

$$\text{(iv)} \begin{cases} x \equiv -6 \ (\mathrm{mod}\, 103) \\ x \equiv -2 \ (\mathrm{mod}\, 107). \end{cases}$$

Ratkaisuiksi saadaan

$$x \equiv \pm 212 \ (\mathrm{mod}\, 11021) \quad \text{tai} \quad x \equiv \pm 109 \ (\mathrm{mod}\, 11021).$$

Huomaa, että jos x on (i):n ratkaisu, niin $-x$ on (iv):n ratkaisu. Vastaavasti, jos x on (ii):n ratkaisu, niin $-x$ on (iii):n ratkaisu. Riittää siis ratkaista esimerkiksi (i) ja (ii).

Lopuksi on vielä tarkistettava, että esimerkiksi $x = 212$ toteuttaa kongruenssin (27) ellei ratkaisujen olemassaoloa muuten tiedetä. Mutta

$$212^2 - 860 = 44944 - 860 = 44084 = 4 \cdot 11021,$$

joten ratkaisut on löydetty.

Esimerkki 7.2.4 Edellä esitetyllä tekniikalla voidaan toteuttaa ns. *elektroninen kolikonheitto*. Tämä nojaa pohjimmiltaan samaan kuin RSA -salakirjoitus; voidaan nopeasti löytää suuret alkuluvut p ja q siten, että tulon $n = pq$ faktorointi on käytännössä mahdotonta.

Henkilöt X ja Y voivat "heittää kolikkoa"sähköpostin välityksellä seuraavasti:

I. X valitsee alkuluvut p ja q siten, että $p \equiv q \equiv 3 \ (\mathrm{mod}\, 4)$ ja lähettää Y:lle luvun $n = pq$ (lukujen p ja q tulee olla niin suuria, että luvun n faktorointi ei onnistu).

II. Y valitsee luvun $2 \leq x_0 < n$, syt$(x_0, n) = 1$, ja lähettää X:lle luvun x_0^2 jakojäännöksen a modulo n. Ehdoista syt$(x_0, n) = 1$ ja $x_0^2 \equiv a \ (\mathrm{mod}\, n)$ seuraa, että syt$(a, n) = 1$.

III. X etsii kongruenssin $x^2 \equiv a \ (\mathrm{mod}\, n)$ neljä ei-kongruenttia ratkaisua ja lähettää yhden niistä Y:lle. Olkoon tämä ratkaisu x'. Olennaista on, että X ei saa selville lukua x_0 jos luvut p ja q

ovat riittävän suuria.

IV. Y määrää Euklideen algoritmilla luvun $d := \text{syt}(x_0 + x', n)$, joka on yksi vaihtoehdoista $1, n, p, q$. Kutakin kongruenssin $x^2 \equiv a \pmod n$ neljästä ratkaisusta vastaa luku d joukossa $\{ 1, n, p, q \}$. Esimerkiksi, jos $x' = -x_0$, niin $d = n$ triviaalisti. Toisaalta jos $x' = x_0$, niin $d = 1$, sillä jos $\text{syt}(2x_0, n) > 1$, niin $p \mid x_0$ tai $q \mid x_0$. Tällöin $x_0^2 \equiv 0 \pmod p$ tai $x_0^2 \equiv 0 \pmod q$, joten $a \equiv 0 \pmod p$ tai $a \equiv 0 \pmod q$. Ristiriita oletuksen $\text{syt}(a, n) = 1$ kanssa. Kaksi muuta vaihtoehtoa jätetään harjoitustehtäväksi.

V. Y voittaa kolikonheiton, jos Y kykenee faktoroimaan luvun n ($d = p$ tai $d = q$) ja häviää jos ei kykene faktoroimaan n:ää ($d = 1$ tai $d = n$). Kummankin vaihtoehdon todennäköisyys on $\frac{2}{4} = \frac{1}{2}$.

7.3 Resiprookkilaki

Lause 7.3.1 (Gaussin Lemma) Olkoon $p > 2$ alkuluku ja $a \in \mathbf{Z}$ siten, että $p \nmid a$. Olkoon $s \in \mathbf{N}$ luku, joka ilmoittaa kuinka moni lukujen $a, 2a, \ldots, (\frac{p-1}{2})a$ jakojäännöksistä modulo p on $> \frac{p}{2}$. Tällöin

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

Todistus. Tarkastellaan joukkoa

$$A = \{ a, 2a, \ldots, (\frac{p-1}{2})a \}.$$

Olkoot $u_1, \ldots, u_s$ ne A:n lukujen jakojäännökset modulo p, jotka ovat $> \frac{p}{2}$ ja olkoot $v_1, \ldots, v_t$ ne jäännökset modulo p, jotka ovat $< \frac{p}{2}$. Koska $\text{syt}(x, p) = 1$ kaikilla $x \in A$, on $u_i > 0$ ja $v_j > 0$. Koska A:n alkiot ovat pareittain ei-kongruentteja modulo p, voidaan helposti päätellä (harjoitustehtävä), että

$$\{ p - u_1, \ldots, p - u_s, v_1, \ldots, v_t \} = \{ 1, 2, \ldots, \frac{p-1}{2} \}.$$

Kertomalla joukkojen alkiot puolittain saadaan ehdon $p - u_i \equiv -u_i \pmod p$ nojalla

$$(\frac{p-1}{2})! = \prod_{i=1}^{s}(p - u_i)\prod_{j=1}^{t} v_j \equiv (-1)^s \prod_{i=1}^{s} u_i \prod_{j=1}^{t} v_j \equiv (-1)^s a^{\frac{p-1}{2}}(\frac{p-1}{2})! \pmod p.$$

Koska $\text{syt}(p, (\frac{p-1}{2})!) = 1$, supistussäännöstä seuraa, että

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

Kertomalla puolittain $(-1)^s$:llä saadaan

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

joten Eulerin kriteerin nojalla

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

Väite seuraa, koska $p > 2$. $\square$

Esimerkki Olkoon $p = 11$ ja $a = 2$. Nyt $\frac{p-1}{2} = 5$ ja

$$\begin{aligned} 1 \cdot 2 &\equiv 2 \,(\mathrm{mod}\, 11), \\ 2 \cdot 2 &\equiv 4 \,(\mathrm{mod}\, 11), \\ 3 \cdot 2 &\equiv 6 \,(\mathrm{mod}\, 11), \\ 4 \cdot 2 &\equiv 8 \,(\mathrm{mod}\, 11), \\ 5 \cdot 2 &\equiv 10 \,(\mathrm{mod}\, 11). \end{aligned}$$

Nyt $\frac{p}{2} = 5\frac{1}{2}$, joten $s = 3$. Gaussin lemman nojalla

$$\left[\frac{a}{p}\right] = (-1)^3 = -1.$$

Gaussin lemman avulla voidaan kätevästi määrätä ne alkuluvut p, joille 2 on neliönjäännös modulo p:

Seuraus 7.3.2 Olkoon $p > 2$ alkuluku. Tällöin

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

ts.

$$\left[\frac{2}{p}\right] = \begin{cases} 1, & \text{kun } p \equiv \pm 1 \,(\mathrm{mod}\, 8) \\ -1, & \text{kun } p \equiv \pm 3 \,(\mathrm{mod}\, 8). \end{cases}$$

Todistus. Koska luvut $1 \cdot 2, 2 \cdot 2, \ldots, (\frac{p-1}{2}) \cdot 2$ ovat kaikki $\leq p-1$, niin Gaussin lemman nojalla

$$\left[\frac{2}{p}\right] = (-1)^s,$$

missä $s \in \mathbf{N}$ ilmoittaa sen, kuinka moni luvuista $2j$, $j = 1, \ldots, \frac{p-1}{2}$, on $> \frac{p}{2}$. Nyt $2j \leq \frac{p}{2}$ jos ja vain jos $j \leq \frac{p}{4}$, joten

$$s = \frac{p-1}{2} - m(\frac{p}{4}),$$

missä funktio m määritellään yhtälöllä $m(x) := \max\{\, k \in \mathbf{N} \mid k \leq x \,\}$. Riittää osoittaa, että s on parillinen täsmälleen silloin kun $\frac{p^2-1}{8}$ on parillinen.

Olkoon esimerkiksi $p \equiv \pm 1 \,(\mathrm{mod}\, 8)$. Tällöin $p = 8k \pm 1$, joten

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k \equiv 0 \,(\mathrm{mod}\, 2)$$

eli $\frac{p^2-1}{8}$ on parillinen. Osoitetaan, että myös s on parillinen tapauksessa $p \equiv \pm 1 \,(\mathrm{mod}\, 8)$.

1° Jos $p \equiv 1 \,(\mathrm{mod}\, 8)$, niin $p = 8k + 1$ ja

$$s = \frac{p-1}{2} - m(\frac{p}{4}) = 4k - m(2k + \frac{1}{4}) = 4k - 2k = 2k \equiv 0 \,(\mathrm{mod}\, 2).$$

2° Jos $p \equiv -1 \pmod 8$, niin $p = 8k + 7$ ja

$$s = \frac{p-1}{2} - m(\frac{p}{4}) = 4k + 3 - m(2k + \frac{7}{4}) = 4k + 3 - (2k + 1) = 2k + 2 \equiv 0 \pmod 2.$$

Tapausta $p \equiv \pm 3 \pmod 8$ koskeva väite todetaan samantapaisella päättelyllä (harjoitustehtävä). $\square$

Esimerkki Seurauksen 7.3.2 nojalla $\left[\frac{2}{31}\right] = 1$, sillä $31 \equiv -1 \pmod 8$. Vastaavasti $\left[\frac{2}{29}\right] = -1$, sillä $29 \equiv -3 \pmod 8$. Lemman 7.1.6 (i) nojalla

$$\left[\frac{89}{13}\right] = \left[\frac{-2}{13}\right] = \left[\frac{-1}{13}\right]\left[\frac{2}{13}\right] = -1,$$

sillä $89 \equiv -2 \pmod{13}$, $\left[\frac{-1}{13}\right] = 1$ (Esimerkki 7.1.7) ja $\left[\frac{2}{13}\right] = -1$ (Seuraus 7.3.2).

Lause 7.3.3 (Neliönjäännösten resiprookkilaki) Olkoot p ja q erillisiä parittomia alkulukuja. Tällöin

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

Todistus sivuutetaan, ks. esim. Rosen, ss. 351–354. Resiprookkilaille on esitetty suunnaton määrä erilaisia todistuksia, mm. 1980-luvulla julkaistiin artikkeli, joka tekijän mukaan sisälsi 152:n resiprookkilain todistuksen. Euler keksi resiprookkilain väitteen muttei todistanut tulosta, Legendre formuloi väitteen modernilla tavalla ja esitti useita puutteellisia todistuksia. Gauss esitti ensimmäisen aukottoman todistuksen väitteelle ja myöhemmin seitsemän muuta todistusta.

Esimerkki 7.3.4 (a) Olkoot p ja q parittomia alkulukuja. Koska $\frac{p-1}{2}$ on parillinen jos ja vain jos $p \equiv 1 \pmod 4$, ja vastaava pätee luvulle q, niin

$$(\frac{p-1}{2})(\frac{q-1}{2}) \text{ on parillinen } \iff p \equiv 1 \pmod 4 \text{ tai } q \equiv 1 \pmod 4.$$

Tässä tapauksessa $[\frac{p}{q}]$ ja $[\frac{q}{p}]$ ovat samanmerkkiset resiprookkilain nojalla. Vastaavasti

$$(\frac{p-1}{2})(\frac{q-1}{2}) \text{ on pariton } \iff p \equiv q \equiv 3 \pmod 4.$$

Tässä tapauksessa $[\frac{p}{q}]$ ja $[\frac{q}{p}]$ ovat vastakkaismerkkiset.

(b) Kohdan (a) päättelyn avulla Legendren symboli on helppo laskea jos $\min(p, q)$ on "pieni". Olkoon esimerkiksi $p \equiv 2 \pmod 3$ ja $p \equiv 1 \pmod 4$. Tällöin

$$\left[\frac{3}{p}\right] = \left[\frac{p}{3}\right] = \left[\frac{2}{3}\right] = -1.$$

Jos p ja q ovat "samaa"suuruusluokkaa, resiprookkilaki ei välttämättä auta.

Fermat'n luvut

Fermat'n luvuiksi sanotaan lukuja

$$F_m = 2^{2^m} + 1,$$

missä $m \in \mathbf{N}$. Fermat totesi itse, että luvut

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

ovat alkulukuja ja esitti hypoteesin, että luvut F_m ovat kaikki alkulukuja.

Esimerkki Fermat'n luku $F_5 = 2^{2^5} + 1 = 4294967297$ ei ole alkuluku, sillä $641 \mid F_5$. Tämän totesi ensimmäisenä Euler. Väite saadaan esityksistä

$$641 = 5 \cdot 2^7 + 1 = 2^4 + 5^4$$

kirjoittamalla

$$\begin{aligned} F_5 &= 2^{2^5} + 1 = 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 = (641 - 5^4)2^{28} + 1 \\ &= 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 = 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\ &= 641(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 - 4). \end{aligned}$$

Fermat'n alkuluvut esiintyvät seuraavassa klassisessa tuloksessa, jonka Gauss todisti:

Lause Säännöllinen n-kulmio voidaan konstruoida pelkästään viivotinta ja harppia käyttäen jos ja vain jos

$$n \mid 2^a p_1 \cdots p_t,$$

missä $a = 0, 1, \ldots$ ja p_i:t ovat erillisiä Fermat'n alkulukuja.

Lause 7.3.5 (Pepinin testi) Fermat'n luku $F_m = 2^{2^m} + 1$ on alkuluku, jos ja vain jos

$$3^{\frac{F_m - 1}{2}} \equiv -1 \pmod{F_m}.$$

Todistus. Osoitetaan ensin induktiolla, että

$$F_m \equiv 2 \pmod 3 \tag{28}$$

kaikilla $m \in \mathbf{N}$. Tapaus $m = 1$ on triviaali, joten tehdään induktio-oletus $F_m \equiv 2 \pmod 3$, $m \in \mathbf{N}$. Siis $2^{2^m} \equiv 1 \pmod 3$ ja siten $2^{2^m} = 1 + 3k$ jollekin $k \in \mathbf{N}$. Näin ollen

$$2^{2^{m+1}} = 2^{2^m \cdot 2} = (2^{2^m})^2 = (1 + 3k)^2 = 1 + 3(2k + 3k^2),$$

joten

$$2^{2^{m+1}} \equiv 1 \pmod 3 \quad \text{eli} \quad F_{m+1} \equiv 2 \pmod 3.$$

Siis (28) pätee kaikilla $m \in \mathbf{N}$.

Oletetaan, että F_m on alkuluku. Tällöin resiprookkilaista saadaan

$$\left[\frac{3}{F_m}\right] = (-1)^{(\frac{F_m - 1}{2})(\frac{3-1}{2})} \left[\frac{F_m}{3}\right] = (-1)^{\frac{2^{2^m}}{2}} \left[\frac{F_m}{3}\right] = \left[\frac{F_m}{3}\right],$$

joten ehdon (28) ja Lemman 7.1.6 nojalla

$$\left[\frac{3}{F_m}\right] = \left[\frac{F_m}{3}\right] = \left[\frac{2}{3}\right] = -1.$$

Edelleen Eulerin kriteerin nojalla

$$3^{\frac{F_m-1}{2}} \equiv \left[\frac{3}{F_m}\right] = -1 \ (\mathrm{mod}\, F_m).$$

Käänteinen implikaatio harjoitustehtävä. $\square$

Huomautus Fermat epäonnistui hypoteesissaan pahimmalla mahdollisella tavalla. Lukujen F_0-F_4 lisäksi ei ole löydetty yhtään Fermat'n alkulukua. Luvut $n = 5, \ldots, 30$ on todettu yhdistetyiksi, ja yleisesti uskotaan ettei uusia Fermat'n alkulukuja enää löydy. Fermat'n luvut ovat silti teoreettisesti kiinnostavia johtuen niiden spesifistä luonteesta; Fermat'n lukujen tutkimus on mm. edistänyt faktorointimenetelmien kehittymistä.

Esimerkki 7.3.6 Jokaiselle Fermat'n luvun F_m alkutekijälle p pätee $ord_p 2 = 2^{m+1}$. Tämän toteamiseksi olkoon p luvun F_m alkutekijä (jolloin siis $m > 4$). Koska $2^{2^m} \equiv -1 \ (\mathrm{mod}\, F_m)$, niin

$$(2^{2^m})^2 = 2^{2^{m+1}} \equiv 1 \ (\mathrm{mod}\, F_m).$$

Erityisesti $2^{2^{m+1}} \equiv 1 \ (\mathrm{mod}\, p)$, joten $ord_p 2 \mid 2^{m+1}$ Lemman 6.1.1 nojalla. Toisaalta, jos vastoin väitettä $ord_p 2 = 2^k$ jollekin $k = 1, \ldots, m$, niin

$$2^{2^m} = (2^{2^k})^{2^{m-k}} \equiv 1^{2^{m-k}} \equiv 1 \ (\mathrm{mod}\, p).$$

Koska $p > 2$, tämä on ristiriidassa ehdon $2^{2^m} \equiv -1 \ (\mathrm{mod}\, F_m)$ kanssa, ja siten $ord_p 2 = 2^{m+1}$.

Lause 7.3.7 Jokainen Fermat'n luvun F_m alkutekijä p on muotoa $p = 2^{m+2}k + 1$.

Todistuksen idea. Voidaan osoittaa, että $[\frac{2}{p}] = 1$. Toisaalta Eulerin kriteerin mukaan

$$2^{\frac{p-1}{2}} \equiv \left[\frac{2}{p}\right] = 1 \ (\mathrm{mod}\, p),$$

joten $ord_p 2 = 2^{m+1} \mid \frac{p-1}{2}$. Näin ollen $\frac{p-1}{2} = k2^{m+1}$ eli $p = k2^{m+2} + 1$ jollekin $k \in \mathbf{N}$.

Esimerkki Tarkastellaan lukua $F_6 = 2^{2^6} + 1$ (20-numeroinen luku). Lauseen 7.3.7 mukaan jokainen F_6:n mahdollinen alkutekijä on muotoa $2^8 k + 1 = 256k + 1$. Näin ollen riittää kokeilla F_6:n jakamista ko. muotoa olevilla luvuilla, jotka eivät ylitä lukua $\sqrt{F_6}$. Osoittautuu, että arvolla $k = 1071$ saadaan alkutekijä, so.

$$274177 = 256 \cdot 1071 + 1$$

on luvun F_6 alkutekijä.

Modulaarisesta potenssiinkorotuksesta

Suurin osa kurssilla esitetyistä lukuteorian sovelluksista nojaa siihen, että modulaarinen potenssiinkorotus voidaan suorittaa tehokkaasti. Tarkastellaan lopuksi tätä.

Määrätään luvun 3^{644} jakojäännös modulo 217. Luvun 3^{644} kymmenjärjestelmäesitys sisältää yli 200 desimaalia, joten potenssiinkorotus ja jakolasku kymmenjärjestelmässä ei ole hyvä idea.

Luvun 644 binäärijärjestelmäesitys on

$$644 = (1010000100)_2 = 2^9 + 2^7 + 2^2 = 512 + 128 + 4.$$

Toisaalta modulaarisella neliöinnillä saadaan:

$$\begin{aligned}
3^1 &\equiv 3 \ (\mathrm{mod}\, 217) \\
3^2 &\equiv 9 \ (\mathrm{mod}\, 217) \\
3^4 &\equiv 9^2 \equiv 81 \ (\mathrm{mod}\, 217) \\
3^8 &\equiv 81^2 \equiv 51 \ (\mathrm{mod}\, 217) \\
3^{16} &\equiv 51^2 \equiv 214 \ (\mathrm{mod}\, 217) \\
3^{32} &\equiv 214^2 \equiv 9 \ (\mathrm{mod}\, 217) \\
3^{64} &\equiv 9^2 \equiv 81 \ (\mathrm{mod}\, 217).
\end{aligned}$$

Havaitaan, että neliöön korottaminen noudattaa tiettyä sykliä. Näin ollen voidaan kirjoittaa suoraan

$$3^{128} \equiv 51 \ (\mathrm{mod}\, 217), \quad 3^{256} \equiv 214 \ (\mathrm{mod}\, 217), \quad 3^{512} \equiv 9 \ (\mathrm{mod}\, 217).$$

Yhdistämällä tulokset saadaan

$$3^{644} = 3^{512} \cdot 3^{128} \cdot 3^4 \equiv 9 \cdot 51 \cdot 81 \equiv 72 \ (\mathrm{mod}\, 217).$$

Numeroesimerkin idea yleistyy välittömästi metodiksi, jolla modulaarinen potenssiin korotus

$$b^N \text{ (mod n)}$$

voidaan suorittaa. Metodi sisältää vaiheet (1)-(3):

(1) Etsitään luvun N esitys binäärijärjestelmässä $N = (a_k a_{k-1} \cdots a_0)_2$.

(2) Etsitään modulaarisella neliöinnillä jakojäännökset modulo n potensseille $b, b^2, \ldots, b^{2^k}$.

(3) Kerrotaan modulo n ne potenssit b^{2^i} keskenään, joiden kerroin a_i on 1.