TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Jenny Virolainen

Kongruenssista

Matematiikan, tilastotieteen ja filosofian laitos
Matematiikka
Lokakuu 2007

Tampereen yliopisto

Matematiikan, tilastotieteen ja filosofian laitos

VIROLAINEN, JENNY: Kongruensseista

Pro gradu -tutkielma, 47 s.

Matematiikka

Lokakuu 2007

Tiivistelmä

Tässä tutkielmassa perehdytään kongruensseihin, joka on lukuteorian yksi osa-alue. Tutkielman päälähteenä on käytetty Kenneth H. Rosenin kirjaa *Elementary Number Theory and its Applications*. Suurin osa määritelmistä ja lauseiden todistuksista löytyvät tästä lähdeteoksesta. Esimerkit ovat lähdeteoksen harjoitustehtäviä, jotka ovat tutkielman tekijän ratkaisemia. Lukijalta edellytetään kokonaisluvun käsitteen muistamista, sekä kokonaislukuihin liittyvien peruslaskutoimitusten hallitsemista.

Luvussa 1 käsitellään lukuteorian perusasioita, kuten jaollisuus, alkuluvut ja suurin yhteinen tekijä. Tässä luvussa esitetään tärkeimmät määritelmät ja lauseet, joita tarvitaan luvussa 2. Luvussa 2 käsitellään kongruenssia. Aluksi esitetään tärkeimmät tulokset, joita tarvitaan myöhemmin. Sen jälkeen käsittelemme lineaarista kongruenssia, kiinalaista jäännöslausetta sekä lineaarisia kongruenssiryhmiä. Luvussa 3 käsitellään kongruenssien sovelluksia. Tässä alaluvussa esittelemme ikikalenterin, kuningatarpulman sekä turnausaikataulun.

Sisältö

Johdanto

Lukuteoriassa tutkitaan kokonaislukuja. Kokonaisluvut näyttävät ja tuntuvat yksinkertaisilta, mutta matka yksinkertaisista havainnoista vaikeasti ratkaistaviin ongelmiin on lyhyempi kuin millään muulla matematiikan alueella. Yksinkertaisia havaintoja pystyy tekemään jopa pieni lapsi, joka haluaa jakaa saamansa suklaapatukat. Hän huomaa suklaapatukoita laskiessaan, että kuusi suklaapatukkaa voi kokonaisena jakaa tasan kahden, kolmen tai jopa kuuden kaverin kanssa. Hän on löytänyt jaollisuuden käsitteen. Hän myös huomaa, että seitsemää suklaapatukkaa ei voi jakaa tasan kuin seitsemän kaverin kanssa. Hän on löytänyt alkuluvut. Lukuteorian perusasioiden avulla pystytään siis laskemaan myös käytännön asioita, yksinkertaisista haasteellisimpaan ja hyvinkin monimutkaisiin tilanteisiin. Yksi mielenkiintoinen tehtävä on laskea, miten voidaan punnita yhden gramman paino, kun käytettävissä ovat punnukset, joiden painot ovat 19 grammaa ja 15 grammaa.

" Matematiikka on tieteiden kuningatar ja
lukuteoria on matematiikan kuningatar. "
-Karl Friedrich Gauss-

Kongruenssit otti ensimmäisenä käyttöön Karl Friedrich Gauss (1777-1855), jonka kirja *Disquisitiones Arithmeticae*, vuonna 1801, oli huima askel lukuteorian ja algebran kehityksessä. Tässä tutkielmassa perehdytään kongruensseihin, joka on lukuteorian yksi osa-alue. Lukijalta edellytetään kokonaisluvun käsitteen muistamista, sekä kokonaislukuihin liittyvien peruslaskutoimitusten hallitsemista. Luvussa 1 käsitellään lukuteorian perusasioita. Alaluku 1.1. käsittelee jaollisuutta. Alaluvussa 1.2. esitellään alkuluvut sekä aritmetiikan peruslause. Tässä alaluvussa esitetään myös kaksi lausetta, joita kukaan ei ole vielä pystynyt todistamaan. Alaluku 1.3. käsittelee suurinta yhteistä tekijää. Jakoalgoritmia sekä Eukleideen algoritmia, jotka esitellään alaluvussa 1.4., käytetään paljon kongruenssien ratkaisemisessa. Lineaarinen Diofantoksen yhtälö esitellään luvussa 1.5. Lineaarinen Diofantoksen yhtälöä käytetään myös paljon kongruenssien ratkaisemisessa.

Luvussa 2 käsitellään kongruenssia. Alaluku 2.1. on johdatusta kongruenssiin. Siinä esitetään tärkeimmät tulokset, joita tarvitaan myöhemmin. Alaluvussa 2.2. käsitellään lineaarista kongruenssia, eli kongruenssiyhtälöä, joka on muotoa $ax \equiv b \pmod{m}$, sekä sen ratkaisemista. Kiinalaisella jäännöslauseella, luvussa 2.3., voidaan ratkaista kongruenssiryhmiä, missä kongruenssit on muotoa $x \equiv a \pmod{m}$. Alaluvussa 2.4. käsitellään lineaarisia kongruenssiryhmiä, missä kongruenssit sisältävät kaksi muuttujaa.

Luvussa 3 käsitellään kongruenssien sovelluksia. Alaluvussa 3.1. esittelemme ikikalenterin. Alaluku 3.2. esittelee kuningatarpulman, mikä on osaltaan johdantoa alaluvussa 3.3. olevaan turnausaikatauluun.

Tutkielma seuraa tiiviisti Kenneth H. Rosenin kirjaa *Elementary Number Nheory and its Applications*. Muita lähdekirjoja ovat David M. Burtonin *Elementary Number Nheory* ja Thomas Koshyn *Elementary Number Theory with Applications*.

1 Lukuteorian peruskäsitteitä

1.1 Jaollisuus

Määritelmä 1.1.1. Olkoot a ja b kokonaislukuja ja olkoon a nollasta eroava. Luku a *jakaa* luvun b, eli luku a on luvun b *tekijä*, jos on olemassa sellainen kokonaisluku c, että

$$b = ac.$$

Merkintä. Jos luku a jakaa luvun b, eli jos luku a on luvun b tekijä, niin merkitään

$$a \mid b.$$

Muussa tapauksessa merkitään

$$a \nmid b.$$

Esimerkki 1.1.1. Luku 4 on luvun 8 tekijä, sillä $8 = 4 \cdot 2$. Siten $4 \mid 8$. Toisaalta, luku 3 ei ole luvun 8 tekijä, eli $3 \nmid 8$, sillä ei olemassa kokonaislukua c siten, että $8 = 3 \cdot c$.

Esimerkki 1.1.2. Luvun 8 kaikki tekijät ovat ± 1, ± 2, ± 4 ja ± 8.

Lause 1.1.1. *Olkoot a, b, c ja d kokonaislukuja. Tällöin*

(1) *jos $a \mid b$ ja $a \mid c$, niin $a \mid (b + c)$,*

(2) *jos $a \mid b$ ja $a \mid c$, niin $a \mid (b - c)$ ja*

(3) *jos $a \mid b$, niin $a \mid bd$.*

Todistus. (Vrt. [3, s. 71].)

(1) Oletetaan, että $a \mid b$ ja $a \mid c$. Tällöin on olemassa sellaiset kokonaisluvut e ja f, että $b = ae$ ja $c = af$. Siten

$$b + c = ae + af = a(e + f),$$

joten määritelmän perusteella $a \mid (b + c)$.

(2) Vastaavasti kuin kohta (1).

(3) Oletetaan, että $a \mid b$. Tällöin on olemassa sellainen kokonaisluku g, että $b = ag$. Siten

$$bd = (ag)d = a(dg),$$

joten määritelmän perusteella $a \mid bd$.

□

Lause 1.1.2. *Olkoot a, b, c ja d positiivisia kokonaislukuja. Tällöin*

(1) *jos $a \mid b$ ja $b \mid c$, niin $a \mid c$,*

(2) *jos $a \mid b$ ja $c \mid d$, niin $ac \mid bd$ ja*

(3) *jos $a \mid b$ ja $a \mid c$, niin $a \mid (bx + cy)$, kaikilla kokonaisluvuilla x ja y.*

Todistus. (Vrt. [1, s. 21].)

(1) Oletetaan, että $a \mid b$ ja $b \mid c$. Tällöin on olemassa sellaiset kokonaisluvut e ja f, että $b = ae$ ja $c = bf$. Siten

$$c = bf = (ae)f = a(ef),$$

joten määritelmän perusteella $a \mid c$.

(2) Oletetaan, että $a \mid b$ ja $c \mid d$. Tällöin on olemassa sellaiset kokonaisluvut g ja h, että $b = ag$ ja $d = ch$. Siten

$$bd = (ag)(ch) = (ac)(gh),$$

joten määritelmän perusteella $ac \mid bd$.

(3) Oletetaan, että $a \mid b$ ja $a \mid c$. Tällöin on olemassa sellaiset kokonaisluvut i ja j, että $b = ai$ ja $c = aj$. Siten

$$bx + cy = aix + ajy = a(xi + yj).$$

Koska $xi + yj$ on kokonaisluku, niin määritelmän perusteella $a \mid (bx + cy)$.

□

Esimerkki 1.1.3. Todistettava, että jos $a \mid b$ ja $a \nmid c$, niin $a \nmid (b + c)$.

Ratkaisu. Oletetaan, että $a \mid b$ ja $a \nmid c$. Tehdään vastaoletus, että $a \mid (b + c)$. Tällöin lauseen 1.1 mukaan $a \mid (b + c) - b$, eli $a \mid c$, mikä on ristiriidassa oletuksen kanssa. Siis jos $a \mid b$ ja $a \nmid c$, niin $a \nmid (b + c)$.

1.2 Alkuluvut

Määritelmä 1.2.1. Alkuluku on lukua 1 suurempi kokonaisluku, joka on jaollinen vain itsellään ja luvulla 1.

Esimerkki 1.2.1. Kymmenen ensimmäistä alkulukua ovat 1, 2, 3, 5, 7, 11, 13, 17, 19 ja 23.

Ennen tietokoneiden aikaa suurin tunnettu alkuluku oli vuonna 1876 löydetty 39-numeroinen luku $2^{127} - 1$. Tähän mennessä suurimman tunnetun alkuluvun, $2^{32\ 582\ 657} - 1$, löysivät Central Missouri State Universityn ryhmä 4.9.2006. Siinä on 9 808 358 numeroa ja se on 44. *Mersennen alkuluku.* [5] Mersennen alkuluvut ovat muotoa $2^p - 1$, missä p on alkuluku.

Määritelmä 1.2.2. Lukua 1 suurempi kokonaisluku, joka ei ole alkuluku on *yhdistetty* luku.

Aritmetiikan peruslauseen todistuksessa tarvitsemme joitakin apulauseita, joten esitämme ne ennen aritmetiikan peruslauseen esittämistä. Näiden apulauseiden todistukset kuitenkin sivuutetaan.

Apulause 1.2.1. *Olkoot a ja b kokonaislukuja ja olkoon p alkuluku. Silloin, jos $p \mid ab$, niin $p \mid a$ ja $p \mid b$.*

Todistus. (Ks. [1, s. 41].) Sivuutetaan.

Apulause 1.2.2. *Olkoot $a_1, a_2, \ldots, a_n$ kokonaislukuja ja olkoon p alkuluku. Silloin, jos*

$$p \mid a_1 a_2 \cdots a_n,$$

niin on olemassa sellainen a_i, missä $i = 1, 2, \ldots, n$, että $p \mid a_i$.

Todistus. (Ks. [1, s. 41].) Sivuutetaan.

Apulause 1.2.3. *Olkoot $p, p_1, p_2, \ldots, p_n$ alkulukuja. Silloin, jos*

$$p \mid p_1 p_2 \cdots p_n,$$

niin on olemassa sellainen p_i, missä $i = 1, 2, \ldots, n$, että $p = p_i$.

Todistus. (Ks. [1, s. 41].) Sivuutetaan.

Lause 1.2.1 (Aritmetiikan peruslause)**.** *Jokainen lukua 1 suurempi kokonaisluku voidaan esittää alkulukujen tulona. Tämä tulo on yksikäsitteinen tekijöiden järjestystä lukuun ottamatta.*

Todistus. (Vrt. [4, s. 90].) Todistetaan ensin alkutekijähajotelman olemassaolo.

Olkoon a kokonaisluku. Jos a on alkuluku, asia on selvä. Olkoon siis a yhdistetty luku. Tällöin a voidaan kirjoittaa muodossa

$$a = p_1 a_1,$$

missä p_1 on pienin mahdollinen alkuluku ja $1 < a_1 < a$. Mikäli luku a_1 on alkuluku, lause on todistettu. Olkoon siis luku a_1 yhdistetty luku. Tällöin a_1 voidaan kirjoittaa muodossa

$$a_1 = p_2 a_2,$$

missä p_2 on pienin mahdollinen alkuluku ja $1 < a_2 < a_1$. Mikäli luku a_2 on alkuluku, lause on todistettu. Jatkamalla luvun a_2 hajottamista edelleen, saadaan lopulta luvulle a alkutekijähajotelma

$$a = p_1 p_2 \cdots p_k,$$

missä $p_1, p_2, \ldots, p_k$ ovat alkulukuja.

Todistetaan vielä alkutekijähajotelman yksikäsitteisyys. Tehdään vastaoletus, että luvulle a on kaksi esitystä

$$a = p_1 p_2 \cdots p_k \quad \text{ja} \quad a = q_1 q_2 \cdots q_l,$$

missä $p_1, p_2, \ldots, p_k$ ja $q_1, q_2, \ldots, q_l$ ovat alkulukuja. Tällöin $p_1 \mid q_1 q_2 \cdots q_l$, joten p_1 jakaa jonkin luvuista $q_1, q_2, \ldots, q_l$. Oletetaan, että $p_1 \mid q_1$. Koska molemmat luvut ovat alkulukuja on oltava $p_1 = q_1$. Jatkamalla samalla tavalla, saadaan lopulta

$$p_2 = q_2, \ldots p_k = q_l \quad \text{missä } k = l,$$

eli $p_1 p_2 \cdots p_k$ ja $q_1 q_2 \cdots q_l$ ovat identtiset. □

Apulause 1.2.4. *Jokaisella lukua 1 suuremmalla kokonaisluvulla on alkulukutekijä.*

Todistus. (Vrt. [3, s. 100].) Sivuutetaan. □

Lause 1.2.2. *Alkulukuja on ääretön määrä.*

Todistus. (Vrt. [4, s. 65].) Tehdään vastaoletus, että on olemassa äärellinen määrä alkulukuja. Olkoot nämä alkuluvut $p_1, p_2, \ldots, p_n$. Olkoon N kokonaisluku siten, että $N = p_1 p_2 \cdots p_n + 1$. Koska luku $N > 1$, niin apulauseen 1.2.4 perusteella kokonaisluvulla N on lukua 1 suurempi alkulukutekijä. Olkoon tämä alkuluku p_i, missä $i = 1, 2, \ldots, n$. Koska p_i on kokonaisluvun N tekijä, niin $p_i \div N$. Edelleen $p_i \div p_1 p_2 \cdots p_n$, joten lauseen 1.1.2. perusteella $p_i \div (N - p_1 p_2 \cdots p_n) = 1$, mikä on mahdotonta, koska $p_i > 1$.

Siis vastaoletus on väärin ja väite oikein, joten alkulukuja on ääretön määrä. □

Lukuteoriassa on vielä ratkaisematta monia yksinkertaiselta näyttäviä alkulukuihin liittyviä ongelmia. Todistusta odottaa muun muassa *Goldbachin väittämä* ja *väittämä alkulukuparien lukumäärästä.*

Lause 1.2.3 (Goldbachin väittämä)**.** *Jokainen lukua* 2 *suurempi parillinen luku voidaan esittää kahden alkuluvun summana.*

Esimerkki 1.2.2. Luku 36 voidaan kirjoittaa alkulukujen 23 ja 13 summana, ts. $36 = 23 + 13$. Myöskin luku 98 voidaan kirjoittaa alkulukujen summana, sillä $98 = 61 + 37$.

Lause 1.2.4 (Väittämä alkulukuparien lukumäärästä)**.** *On olemassa ääretömän monta alkulukuparia, eli äärettömän monta paria sellaisia alkulukuja, joiden erotus on kaksi.*

Esimerkki 1.2.3. Viisi ensimmäistä alkulukuparia on 3 ja 5, 5 ja 7, 11 ja 13, 17 ja 19 sekä 29 ja 31.

1.3 Suurin yhteinen tekijä

Esimerkki 1.3.1. Luvun 12 kaikki tekijät ovat ± 1, ± 2, ± 3, ± 4, ± 6 ja ± 12 ja luvun 6 kaikki tekijät ovat ± 1, ± 2, ± 3 ja ± 6. Lukujen 12 ja 6 yhteiset tekijät ovat siis ± 1, ± 2, ± 3 ja ± 6, joista suurin on 6.

Määritelmä 1.3.1. Olkoot a ja b kokonaislukuja, joista ainakin toinen on nollasta eroava. *Suurin yhteinen tekijä* c on suurin positiivinen kokonaisluku, joka jakaa sekä luvun a, että luvun b.

Merkintä. Suurinta yhteistä tekijää merkitään

$$syt(a, b) = c,$$

tai lyhyesti

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

Esimerkki 1.3.2. Lukujen 10 ja 18 yhteiset tekijät ovat ± 1 ja ± 2. Siten $(10, 18) = 2$.

Huomautus. Jos luvuista a ja b ainakin toinen on nollasta eroava, niin suurin yhteinen tekijä on aina olemassa ja se on yksikäsitteinen.

Jos molemmat luvuista a ja b ovat nollia, suurin yhteinen tekijä on nolla, ts. $(0, 0) = 0$.

Määritelmä 1.3.2. Olkoot a ja b kokonaislukuja. Silloin lukujen a ja b suurin yhteinen tekijä c voidaan esittää lineaarikombinaationa muodossa

$$(a, b) = ax + by,$$

eli

$$c = ax + by,$$

missä x ja y ovat kokonaislukuja.

Määritelmä 1.3.3. Kokonaislukuja a ja b kutsutaan *suhteellisiksi alkuluvuiksi*, jos

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

Määritelmä 1.3.4. Kokonaislukuja $a_1, a_2, \ldots, a_n$ kutsutaan *pareittain suhteellisiksi alkuluvuiksi*, jos jokaiselle parille (a_i, a_j), missä $i = 1, 2, \ldots, n$ ja $j = 1, 2, \ldots, n$, on voimassa

$$(a_i, a_j) = 1.$$

Apulause 1.3.1. *Olkoot a ja b kokonaislukuja, joista ainakin toinen on nollasta eroava. Silloin luvut a ja b ovat suhteellisia alkulukuja, jos ja vain jos*

$$1 = ax + by,$$

missä x ja y ovat kokonaislukuja.

Todistus. (Ks. [1, s. 23].) Sivuutetaan. □

Lause 1.3.1. *Olkoot a, b ja c kokonaislukuja siten, että $(a, b) = c$. Silloin*

$$(\frac{a}{c}, \frac{b}{c}) = 1.$$

Todistus. (Vrt. [4, s. 75].) Luvut $\frac{a}{c}$ ja $\frac{b}{c}$ ovat kokonaislukuja, sillä $(a, b) = c$ ja siten $c \mid a$ ja $c \mid b$.

Koska $(a, b) = c$, niin on olemassa kokonaisluvut x ja y, että $c = ax + by$. Jakamalla molemmat puolet luvulla c, saadaan

$$1 = \frac{a}{c}x + \frac{b}{c}y.$$

Koska luvut $\frac{a}{c}$ ja $\frac{b}{c}$ ovat kokonaislukuja, niin $\frac{a}{c}$ ja $\frac{b}{c}$ ovat suhteellisia alkulukuja. □

1.4 Jakoalgoritmi

Menetelmä, jolla voidaan aina määrittää kahden luvun suurin yhteinen tekijä, perustuu seuraavaan lauseeseen.

Lause 1.4.1 (**Jakoalgoritmi**). *Olkoon a kokonaisluku ja olkoon b positiivinen kokonaisluku. Silloin on olemassa sellaiset yksikäsitteiset luvut q ja r, että*

$$a = bq + r, \quad \textit{missä} \quad 0 \leq r < b.$$

Huomautus. Yhtälössä $a = bq + r$ lukua a sanotaan *jaettavaksi*, lukua b *jakajaksi*, lukua q *osamääräksi* ja lukua r *jakojäännökseksi*.

Todistus. (Vrt. [3, s. 18].) Todistetaan ensin lukujen q ja r olemassaolo. Olkoon S joukko siten, että

$$S = \{a - bx | x \in \mathbb{Z} \text{ ja } a - bn \geq 0\}.$$

Osoitetaan, että joukko S on epätyhjä. Riittää siis osoittaa, että yhtälö $a - bx$ on epänegatiivinen. Koska kokonaisluku $b \geq 1$, niin $|a|\, b \geq |a|$ ja siten

$$a - (-|a|)b = a + |a|\, b \geq a + |a| \geq 0.$$

Valitaan $x = -|a|$, jolloin $a - bx \in S$. Koska joukko on *hyvin järjestetty*, eli jokaisessa epätyhjässä joukossa positiivisia kokonaislukuja on olemassa pienin epänegatiivinen alkio, niin on olemassa pienin epänegatiivinen alkio r. Siten

$$r = a - bq.$$

Osoitetaan nyt, että $r < b$. Tehdään vastaoletus, että $r \geq b$. Siten

$$a - b(q + 1) = (a - qb) - b = r - b \geq 0,$$

eli $a - b(q+1) \in S$. Mutta, koska $a - b(q+1) = r - q < r$, niin r ei ole joukon S pienin alkio. Siis vastaoletus on väärin ja siis $r < b$.

Todistetaan vielä lukujen q ja r yksikäsitteisyys. Oletetaan, että

$$a = bq + r \quad \text{ja} \quad a = bq' + r',$$

missä $0 \leq r < b$ ja $0 \leq r' < b$. Tällöin

$$0 = (bq + r) - (bq' + r') = b(q - q') + (r - r'),$$

eli

$$b(q - q') = r - r'.$$

Näin ollen $b \mid (r' - r)$. Koska $0 \leq r < b$ ja $0 \leq r' < b$, niin $-b < r' - r < b$, eli $|r' - r| < b$. Siis $r = r'$. Lisäksi, koska $b \neq 0$, niin $q = q'$. Näin olemme todistaneet lukujen q ja r yksikäsitteisyyden. □

Suurin yhteinen tekijä on helppo löytää, kun tutkitaan pieniä kokonaislukuja. Suurien kokonaislukujen ollessa kyseessä, yhteisen tekijän löytämiseksi voidaan käyttää esimerkiksi *Eukleideen algoritmia*.

Eukleideen algoritmia sovellettaessa luku a jaetaan luvulla b. Jos jako ei mene tasan, jaetaan luku b jakojäännöksellä. Jos tämäkään jakolasku ei mene tasan, jaetaan taas tämän jakolaskun jakaja jakojäännöksellä. Näin jatketaan, kunnes saadaan jakolasku, joka menee tasan. Tasan menevän jakolaskun jakaja, eli viimeinen nollasta eroava jakojäännös, on lukujen a ja b suurin yhteinen tekijä.

Lause 1.4.2 (**Eukleideen algoritmi**). *Olkoot a ja b positiivisia kokonaislukuja siten, että $b \nmid a$. Silloin voidaan kirjoittaa*

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < b \\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \\
r_2 &= r_3 q_4 + r_4, \quad 0 < r_4 < r_3 \\
&\vdots \\
r_{k-2} &= r_{k-1} q_k + r_k, \quad 0 < r_k < r_{k-1} \\
r_{k-1} &= r_k q_{k+1},
\end{aligned}$$

missä r_k on lukujen a ja b suurin yhteinen tekijä, ts. $(a, b) = r_k$.

Todistus. (Ks. [1, s. 81].)

Esimerkki 1.4.1. Määritettävä lukujen 8752 ja 768 suurin yhteinen tekijä.

Ratkaisu. Koska luvut ovat suuria ja luku $768 \nmid 8752$, niin käytetään Eukleideen algoritmia suurimman yhteisen tekijän selvittämiseksi. Saadaan

$$\begin{aligned} 8752 &= 768 \cdot 11 + 304 \\ 768 &= 304 \cdot 2 + 160 \\ 304 &= 160 \cdot 1 + 144 \\ 160 &= 144 \cdot 1 + 16 \\ 144 &= 16 \cdot 9 + 0. \end{aligned}$$

Tasan menneen jakolaskun jakaja, eli viimeinen nollasta eroava jakojäännös, on luku 16, joten $(8752, 768) = 16$.

1.5 Lineaarinen Diofantoksen yhtälö

Määritelmä 1.5.1. Olkoot a, b ja c ovat kokonaislukuja. Yhtälöä

$$ax + by = c \tag{1.5.1}$$

sanotaan *kahden muuttujan lineaariseksi Diofantoksen yhtälöksi.*

Seuraavaa lausetta voidaan käyttää lineaarisen Diofantoksen yhtälön ratkaisemisessa. Ennen lauseen esittämistä, esitetään se ennen lauseen esittämistä. Apulauseen todistus kuitenkin sivuutetaan.

Apulause 1.5.1. *Olkoot a, b ja c ovat kokonaislukuja. Silloin, jos $a \mid bc$ ja $(a, b) = 1$, niin $a \mid c$.*

Todistus. (Ks. [4, s. 120].) Sivuutetaan. □

Lause 1.5.1. *Olkoot a ja b kokonaislukuja ja olkoon $(a, b) = d$. Diofantoksen yhtälö $ax + by = c$ on ratkeava, jos ja vain jos $d \mid c$.*

Jos yhtälö $ax + by = c$ on ratkeava, niin yhtälön kaikki ratkaisut ovat

$$\begin{cases} x &= x_0 + \left(\frac{b}{d}\right) n, \\ y &= y_0 - \left(\frac{a}{d}\right) n, \end{cases} \tag{1.5.2}$$

missä n on kokonaisluku ja pari $(x_0,\, y_0)$ on yksi ratkaisu.

Todistus. (Vrt. [4, s. 113].) Olkoot a, b ja c ovat kokonaislukuja ja olkoon $(a, b) = d$. Oletetaan, että x ja y ovat kokonaislukuja siten, että $ax + by = c$. Koska $(a, b) = d$, niin $d \mid a$ ja $d \mid b$, joten lauseen 1.1.2 mukaan $d \mid (ax + by)$, eli $d \mid c$.

Oletetaan sitten, että $d \mid c$. Lauseen 1.4.2 mukaan on olemassa sellaiset kokonaisluvut s ja t, että

$$d = as + bt.$$

Koska $d \mid c$, niin on olemassa kokonaisluku e siten, että

$$c = de.$$

Näin ollen

$$c = de = (as + bt)e = a(se) + b(te),$$

missä $x = se$ ja $y = te$, joten $ax + by = c$. Siis yhtälö $ax + by = c$ on ratkeava.

Olkoot sitten $x = x_0 + \left(\frac{b}{d}\right) n$ ja $y = y_0 - \left(\frac{a}{d}\right) n$, missä n on kokonaisluku. Pari (x, y) on ratkaisu, sillä

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

Todistetaan vielä, että näin saadaan kaikki ratkaisut. Olkoot x ja y kokonaislukuja, joille $ax + by = c$. Koska

$$ax_0 + by_0 = c,$$

niin sijoittamalla tämä yhtälöön (1.5.1) saadaan, että

$$ax + by = ax_0 + by_0.$$

Siten

$$a(x - x_0) = b(y_0 - y). \tag{1.5.3}$$

Jaetaan nyt molemmat puolet luvulla d, jolloin saadaan

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

Edelleen lauseen 1.3.2 ja apulauseen 1.5.1 perusteella

$$\frac{a}{d} \mid (y_0 - y).$$

Siten on olemassa kokonaisluku n, että

$$\left(\frac{a}{d}\right) n = y_0 - y,$$

eli

$$y = y_0 - \left(\frac{a}{d}\right) n.$$

Sijoittamalla tämä yhtälöön (1.5.3) saadaan

$$a(x - x_0) = b\left(\frac{a}{d}\right) n,$$

joten

$$x = x_0 + \left(\frac{b}{d}\right) n.$$

Näin lause on todistettu. □

Esimerkki 1.5.1. Etsitään lineaarisen Diofantoksen yhtälön $2x + 5y = 11$ kaikki ratkaisut.

Koska $(2, 5) = 1$ ja $1 \mid 11$, niin yhtälö $2x + 5y = 11$ on ratkeava. Yksittäinen ratkaisu $(x_0, y_0) = (-2, 3)$ löydetään keksimällä. Käytetään lausetta 1.4.1 kaikkien ratkaisujen löytämiseksi.

Sijoitetaan pari $(x_0, y_0) = (-2, 3)$ yhtälöön (1.5.2), jolloin saadaan

$$\begin{cases} x &= -2 + \left(\frac{5}{1}\right) n, \\ y &= 3 - \left(\frac{2}{1}\right) n, \end{cases}$$

joten

$$\begin{cases} x &= -2 + 5n, \\ y &= 3 - 2n. \end{cases}$$

Esimerkki 1.5.2. Etsitään Diofantoksen yhtälön $21x + 14y = 147$ kaikki ratkaisut.

Käytetään Eukleideen algoritmia lukujen 21 ja 14 suurimman yhteisen tekijän selvittämiseksi. Saadaan

$$21 = 14 \cdot 1 + 7,$$
$$14 = 7 \cdot 2 + 0.$$

Siis $(21, 14) = 7$. Koska $7 \mid 147$, niin yhtälö on ratkeava.

Etsitään yksittäinen ratkaisu käyttämällä uudestaan Eukleideen algoritmia. Saadaan

$$7 = 21 - 14 \cdot 1.$$

Kerrotaan yhtälö puolittain luvulla $\frac{147}{(21,14)} = \frac{147}{7} = 21$, saadaan

$$147 = 21 \cdot 21 + 14 \cdot (-21).$$

Siis yksittäinen ratkaisu $(x_0, y_0) = (21, -21)$. Siten kaikki ratkaisut ovat

$$\begin{cases} x &= 21 + \left(\frac{14}{7}\right) n, \\ y &= -21 - \left(\frac{21}{7}\right) n, \end{cases}$$

ja edelleen

$$\begin{cases} x &= 21 + 2n, \\ y &= -21 - 3n. \end{cases}$$

2 Kongruenssi

Kongruenssin käsitteen esitteli ensimmäisenä saksalainen, yksi kaikkien aikojen suurimmista matemaatikoista, Carl Friedrich Gauss (1777-1855) vuonna 1801 julkaisemassaan teoksessa *Disquisitiones Arithmeticae*.

Gauss nimitettiin 1807 vain 30-vuotiaana kuulun Göttingenin yliopiston tähtitieteen professoriksi ja observatorion johtajaksi. Hänen kerrotaan nukkuneen elämänsä viimeisten 27 vuoden aikana vain kerran muualla kuin rakkaassa observatoriossaan.

Gaussin aivot ovat yhä tallella Göttingenin yliopiston fysiologian laitoksella. [6]

2.1 Johdatus kongruenssiin

Määritelmä 2.1.1. Olkoon m positiivinen kokonaisluku. Sanotaan, että luku a on *kongruentti* luvun b kanssa *modulo* m, jos

$$m \mid (a - b).$$

Merkintä. Jos luku a on kongruentti luvun b kanssa modulo m, niin merkitään

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

Jos $m \nmid (a - b)$, niin luku a ei ole kongruentti luvun b kanssa modulo m. Silloin merkitään

$$a \not\equiv b \pmod{m}.$$

Esimerkki 2.1.1. Koska $4 \mid (11 - 3) = 8$, niin $11 \equiv 3 \pmod{4}$. Toisaalta $4 \nmid (11 - (-3)) = 14$, joten $11 \not\equiv -3 \pmod{4}$.

Lause 2.1.1. *Olkoot a ja b ovat kokonaislukuja. Silloin $a \equiv b \pmod{m}$, jos ja vain jos on olemassa sellainen kokonaisluku k, että*

$$a = b + km.$$

Todistus. (Vrt. [4, s. 120].) Jos $a \equiv b \pmod{m}$, niin $m \mid (a-b)$. Tällöin on olemassa kokonaisluku k siten, että $km = a - b$ ja edelleen $a = b + km$.

Toisaalta, jos on olemassa kokonaisluku k siten, että $a = b + km$, niin $km = a - b$. Täten $m \mid (a-b)$ ja edelleen $a \equiv b \pmod{m}$. □

Esimerkki 2.1.2. Koska $15 = 7 + 2 \cdot 4$, niin $15 \equiv 7 \pmod{4}$.

Huomautus. Kongruenssin määritelmästä seuraa suoraan, että

$$a \equiv 0 \pmod{m},$$

jos ja vain jos $a = km$, missä k on kokonaisluku.

Esimerkki 2.1.3. Koska $7 \mid (252 - 0) = 252$, niin $252 \equiv 0 \pmod{7}$.

Lause 2.1.2. *Olkoot a, b ja c kokonaislukuja ja olkoon m positiivinen kokonaisluku. Silloin*

(1) *(Refleksiivisyys)* $a \equiv a \pmod{m}$,

(2) *(Symmetrisyys) jos* $a \equiv b \pmod{m}$, *niin* $b \equiv a \pmod{m}$ *ja*

(3) *(Transitiivisuus) jos* $a \equiv b \pmod{m}$ *ja* $b \equiv c \pmod{m}$, *niin* $a \equiv c \pmod{m}$.

Todistus. (Vrt. [4, s. 121].)

(1) Koska $m \mid (a - a) = 0$, niin $a \equiv a \pmod{m}$.

(2) Oletetaan, että $a \equiv b \pmod{m}$. Silloin $m \mid (a - b)$, joten on olemassa kokonaisluku k siten, että $km = a - b$. Siten $(-k)m = b - a$, joten $m \mid (b - a)$. Siis $b \equiv a \pmod{m}$.

(3) Oletetaan, että $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$. Silloin $m \mid (a-b)$ ja $m \mid (b-c)$, joten on olemassa kokonaisluvut k ja l siten, että $km = a-b$ ja $lm = b - c$, eli $a = km + b$ ja $c = b - lm$. Siis

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

joten $m \mid (a - c)$ ja edelleen $a \equiv c \pmod{m}$.

□

Esimerkki 2.1.4. Olkoot a ja b kokonaislukuja ja olkoot c ja m positiivisia kokonaislukuja. Osoitettava, että jos $a \equiv b \pmod{m}$, niin $ac \equiv bc \pmod{mc}$. ([4, s. 120, teht. 9]).

Ratkaisu. Koska $a \equiv b \pmod{m}$, niin on olemassa kokonaisluku k siten, että $a = b + km$. Siten $ac = (b + km)c = bc + k(mc)$. Siis lauseen 2.1.1 mukaan $ac \equiv bc \pmod{mc}$.

Määritelmä 2.1.2. *Jäännösluokka modulo m* sisältää kaikki ne kokonaisluvut, jotka ovat keskenään kongruentteja modulo m.

Esimerkki 2.1.5. Jäännösluokat modulo 5 ovat

$$\{\cdots \equiv -10 \equiv -5 \equiv 0 \equiv 5 \equiv 10 \equiv \cdots\}$$
$$\{\cdots \equiv -9 \equiv -4 \equiv 1 \equiv 6 \equiv 11 \equiv \cdots\}$$
$$\{\cdots \equiv -8 \equiv -3 \equiv 2 \equiv 7 \equiv 12 \equiv \cdots\}$$
$$\{\cdots \equiv -7 \equiv -2 \equiv 3 \equiv 8 \equiv 13 \equiv \cdots\}$$
$$\{\cdots \equiv -6 \equiv -1 \equiv 4 \equiv 9 \equiv 14 \equiv \cdots\}.$$

Lause 2.1.3. *Olkoon a, b ja c kokonaislukuja ja m positiivinen kokonaisluku. Jos $a \equiv b \pmod{m}$, niin*

(1) $a + c \equiv b + c \pmod{m}$,

(2) $a - c \equiv b - c \pmod{m}$ *ja*

(3) $ac \equiv bc \pmod{m}$.

Todistus. (Vrt. [4, s. 122].) Olkoon a, b ja c kokonaislukuja ja m positiivinen kokonaisluku. Oletetaan, että $a \equiv b \pmod{m}$, joten $m \mid (a - b)$.

(1) Kirjoitetaan $(a - b)$ muodossa

$$a - b = (a + c) - (b + c),$$

missä on lisätty ja vähennetty luku c. Siis $m \mid ((a + c) - (b + c))$, joten $a + c \equiv b + c \pmod{m}$.

(2) Vastaavasti, kuin kohta (1).

(3) Koska $m \mid (a-b)$, niin $m \mid c(a-b) = ac - bc$. Siis $m \mid (ac - bc)$, joten $ac \equiv bc \pmod{m}$.

□

Esimerkki 2.1.6. Olkoot $a = 15$, $b = 11$, $c = 7$ ja $m = 4$. Tällöin $15 \equiv 11 \pmod{4}$ ja lauseen 2.1.3 mukaan pitää paikkansa, että $15 - 7 \equiv 11 - 7 \pmod{4}$, eli $8 \equiv 4 \pmod{4}$.

Lause 2.1.4. *Olkoot a, b ja c kokonaislukuja ja m positiivinen kokonaisluku. Jos $ac \equiv bc \pmod{m}$ ja $(c, m) = d$, niin*

$$a \equiv b \pmod{\left(\frac{m}{d}\right)}.$$

Todistus. (Vrt. [4, s. 121].) Oletetaan, että $ac \equiv bc \pmod{m}$ ja $(c, m) = d$. Silloin

$$m \mid (ac - bc) = c(a - b).$$

Koska $(c, m) = d$, niin molemmat puolet voidaan jakaa luvulla d, jolloin saadaan

$$\left(\frac{m}{d}\right) \mid \left(\frac{c}{d}\right)(a - b).$$

Edelleen lauseen 1.3.2 ja apulauseen 1.5.1 mukaan

$$\left(\frac{m}{d}\right) \mid (a - b).$$

Siis $a \equiv b \pmod{\left(\frac{m}{d}\right)}$. □

Esimerkki 2.1.7. Kongruenssi $60 \equiv 24 \pmod{18}$ voidaan kirjoittaa muodossa $5 \cdot 12 \equiv 2 \cdot 12 \pmod{18}$. Näin ollen $(12, 18) = 6$, joten edellisen lauseen perusteella $5 \equiv 2 \pmod{\frac{18}{6}}$, eli $5 \equiv 2 \pmod{3}$.

Lause 2.1.5. *Olkoot a, b ja c kokonaislukuja ja olkoon m positiivinen kokonaisluku. Jos $ac \equiv bc \pmod{m}$ ja $(c, m) = 1$, niin $a \equiv b \pmod{m}$.*

Todistus. Oletetaan, että $ac \equiv bc \pmod{m}$ ja $(c, m) = 1$. Silloin

$$m \mid (ac - bc) = c(a - b).$$

Koska $(c, m) = 1$, niin

$$m \mid (a - b).$$

Siis $a \equiv b \pmod{m}$. □

Huomautus. Edellisen lauseen ehto $(c, m) = 1$ on välttämätön. Esimerkiksi kongruenssi $28 \equiv 7 \pmod{3}$ voidaan kirjoittaa muodossa $4 \cdot 7 \equiv 1 \cdot 7 \pmod{3}$, missä $(7, 3) = 1$. Täten saadaan $4 \equiv 1 \pmod{3}$, mikä pitää paikkansa.

Kongruenssi $28 \equiv 7 \pmod{7}$ voidaan myös kirjoittaa muodossa $4 \cdot 7 \equiv 1 \cdot 7 \pmod{7}$. Jos jättää huomioimatta suurimman yhteisen tekijän, niin saadaan, että $4 \equiv 1 \pmod{7}$, mikä ei pidä paikkansa. Tämä johtuu siitä, että $(7, 7) = 7 \neq 1$.

Lause 2.1.6. *Olkoot a, b, c ja d kokonaislukuja ja olkoon m positiivinen kokonaisluku. Jos $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$, niin*

(1) $a + c \equiv b + d \pmod{m}$,

(2) $a - c \equiv b - d \pmod{m}$ *ja*

(3) $ac \equiv bd \pmod{m}$.

Todistus. (Vrt. [4, s. 123].) Oletetaan, että $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$, joten $m \mid (a - b)$ ja $m \mid (c - d)$. On siis olemassa kokonaisluvut k ja l, että $km = a - b$ ja $lm = c - d$, eli $a = b + km$ ja $c = d + lm$.

(1) Tällöin

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

eli $m \mid ((a + c) - (b + d))$. Siis $a + c \equiv b + d \pmod{m}$.

(2) Vastaavasti kuin kohta (1).

(3) Tällöin

$$ac = (b + km)(d + lm) = bd + (bl + dk + kml)m,$$

eli $m \mid (ac - bd)$. Siis $ac \equiv bd \pmod{m}$.

□

Esimerkki 2.1.8. Jos $7 \equiv 3 \pmod{4}$ ja $18 \equiv 2 \pmod{4}$, niin $7+18 \equiv 3+2 \pmod{4}$, eli $25 \equiv 5 \pmod{4}$. Lisäksi $7 \cdot 18 \equiv 3 \cdot 2 \pmod{4}$, eli $126 \equiv 6 \pmod{4}$.

Lause 2.1.7. *Olkoot a ja b kokonaislukuja ja olkoot k ja m positiivisia kokonaislukuja. Tällöin, jos $a \equiv b \pmod{m}$, niin $a^k \equiv b^k \pmod{m}$.*

Todistus. (Vrt. [4, s. 124].) Oletetaan, että $a \equiv b \pmod{m}$, joten $m \mid (a-b)$. Tällöin

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

joten $(a - b) \mid (a^k - b^k)$. Lauseesta 1.1.2 seuraa, että

$$m \mid (a^k - b^k).$$

Siten $a^k \equiv b^k \pmod{m}$. □

2.2 Lineaarinen kongruenssi

Määritelmä 2.2.1. Olkoot a ja b kokonaislukuja ja olkoon m positiivinen kokonaisluku. Kongruenssia, joka on muotoa

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

missä x on tuntematon kokonaisluku, sanotaan *yhden muuttujan lineaarikongruenssiksi.*

Lause 2.2.1. *Olkoot a ja b kokonaislukuja ja olkoon m positiivinen kokonaisluku. Olkoon lisäksi $(a, m) = d$. Kongruenssi $ax \equiv b \pmod{m}$ on ratkeava, jos*

$$d \mid b.$$

Mikäli kongruenssi $ax \equiv b \pmod{m}$ *on ratkeava, sen yleinen ratkaisu on muotoa*

$$x \equiv x_0 \pmod{\left(\frac{m}{d}\right)},$$

missä x_0 *on yksi ratkaisu.*

Todistus. (Vrt. [4, s. 131].) Oletetaan, että $(a, m) = d$ ja $d \mid b$. Kokonaisluku x on kongruenssin $ax \equiv b \pmod{m}$ ratkaisu, jos ja vain jos on olemassa kokonaisluku y siten, että

$$ax - my = b.$$

Yhtälö $ax - my = b$ on kahden muuttujan Diofantoksen yhtälö, joka on ratkeava, sillä $d \mid b$.

Koska yhtälö $ax - my = b$ on ratkeava, sen ratkaisut ovat muotoa

$$\begin{cases} x &= x_0 + \left(\frac{m}{d}\right) t, \\ y &= y_0 - \left(\frac{a}{d}\right) t, \end{cases}$$

missä $t = 0, 1, 2, \ldots, (d-1)$ ja pari (x_0, y_0) on yhtälön $ax - my = b$ yksi ratkaisu. Siis luvun x arvot,

$$x = x_0 + \left(\frac{m}{d}\right) t,$$

ovat kongruenssin $ax \equiv b \pmod{m}$ ratkaisut, joten kongruenssi $x \equiv x_0 \pmod{\left(\frac{m}{d}\right)}$ on voimassa.

□

Esimerkki 2.2.1. Etsitään kongruenssin $19x \equiv 30 \pmod{40}$ kaikki ratkaisut. Koska $(19, 40) = 1$ ja $1 \mid 30$, niin yhtälö on ratkeava ja sillä on täsmälleen yksi ratkaisu modulo 40. Löytääksemme tämän ratkaisun, ratkaistaan lineaarinen diofantoksen yhtälö $19x - 40y = 30$ Eukleideen algoritmin avulla. Saadaan

$$\begin{aligned} 40 &= 19 \cdot 2 + 2, \\ 19 &= 2 \cdot 9 + 1, \\ 2 &= 1 \cdot 2. \end{aligned}$$

Käyttämällä Eukleideen algoritmia uudelleen, saadaan yksi ratkaisupari (x_0, y_0). Siis

$$\begin{aligned} 1 &= 19 - 2 \cdot 9 \\ &= 19 - (40 - 19 \cdot 2) \cdot 9 \\ &= 19 \cdot 19 - 40 \cdot 9. \end{aligned}$$

Kertomalla yhtälö puolittain luvulla $\frac{30}{(19,40)} = 30$, saadaan

$$30 = 19 \cdot 570 - 40 \cdot 270,$$

missä $(x_0, y_0) = (570, 270)$. Siis kongruenssin $19x \equiv 30 \pmod{40}$ yleinen ratkaisu on muotoa

$$x \equiv 570 \pmod{40},$$

eli

$$x \equiv 10 \pmod{40}.$$

Huomautus. Jos $(a, m) = d$, niin kongruenssilla $ax \equiv b \pmod{m}$ on d kappaletta erisuuria ratkaisuja modulo m.

Mikäli $(a, m) = 1$, niin kongruenssilla $ax \equiv b \pmod{m}$ on täsmälleen yksi ratkaisu modulo m.

Huomautus. Kongruenssilla $ax \equiv 1 \pmod{m}$ on ratkaisu, jos ja vain jos $(a, m) = 1$. Jos ratkaisu on olemassa, niin kaikki ratkaisut ovat kongruentteja modulo m.

Määritelmä 2.2.2. Olkoon a kokonaisluku ja m positiivinen kokonaisluku siten, että $(a, m) = 1$. Kongruenssin $ax \equiv 1 \pmod{m}$ ratkaisua kutsutaan luvun a käänteisluvuksi modulo m.

Merkintä. Luvun a käänteisluku modulo m on $\bar{a}$.

Huomautus. Mikäli luku $\bar{a}$ on luvun a on käänteisluku modulo m, niin $a\bar{a} \equiv 1 \pmod{m}$.

Esimerkki 2.2.2. Etsitään luvun 7 käänteisluku modulo 17. Pitää siis etsiä ratkaisu kongruenssille $7x \equiv 1 \pmod{17}$. Koska $(7, 17) = 1$ ja $1 \mid 1$, niin on olemassa yksikäsitteinen ratkaisu modulo 17. Helposti keksimme ratkaisun $x = 5$. Siten kaikki kokonaisluvut, jotka ovat kongruentteja luvun 5 kanssa modulo 17, ovat luvun 7 käänteislukuja modulo 17.

Lause 2.2.2. *Olkoon a positiivinen kokonaisluku ja olkoon p alkuluku. Luku a on itsensä käänteisluku modulo p, jos ja vain jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$.*

Todistus. (Ks. [4, s. 133].) Sivuutetaan. □

2.3 Kiinalainen jäännöslause

Lause 2.3.1. *Olkoot $m_1, m_2, \ldots, m_r$ pareittain suhteellisia alkulukuja. Silloin kongruenssiryhmällä*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

on yksikäsitteinen ratkaisu modulo $M = m_1 m_2 \cdots m_r$.

Todistus. (Vrt. [4, s. 136].) Konstruoidaan ensin ratkaisu ja todistetaan sitten ratkaisun yksikäsitteisyys. Olkoon $M = m_1 m_2 \cdots m_r$. Silloin

$$M_k = \frac{M}{m_k} = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r,$$

missä $k = 1, 2, \ldots, r$. Koska $m_1, m_2, \ldots, m_r$ ovat pareittain suhteellisia alkulukuja, niin määritelmän (1.3.4) perusteella $(M_k, m_k) = 1$. Siis luvulla M_k on käänteisluku y_k modulo m_k siten, että

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Todistetaan nyt, että

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_r M_r y_r.$$

Täytyy siis todistaa, että $x \equiv a_k \pmod{m_k}$.

Koska $m_k \mid M_j$, kun $j \neq k$, niin $M_j \equiv 0 \pmod{m_k}$. Koska $M_k y_k \equiv 1 \pmod{m_k}$, niin

$$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}.$$

Siis x on kongruenssiryhmän ratkaisu.

Todistetaan sitten, että ratkaisu on yksikäsitteinen modulo M. Tehdään vastaoletus, että ratkaisuja on kaksi kappaletta. Olkoot x_0 ja x_1 kongruenssiryhmän ratkaisut. Silloin jokaista lukua k kohti

$$x_0 \equiv x_1 \equiv a_k \pmod{m_k},$$

joten $m_k \mid (x_0 - x_1)$. Siten $M \mid (x_0 - x_1)$, eli $x_0 \equiv x_1 \pmod{m_k}$, joten $x_0 = x_1$. Siis ratkaisu on yksikäsitteinen modulo M. □

Esimerkki 2.3.1. Ratkaistaan kongruenssiryhmä

$$\begin{aligned} x &\equiv 3 \pmod{4}, \\ x &\equiv 5 \pmod{9}, \\ x &\equiv 10 \pmod{35}. \end{aligned}$$

Koska luvut $4, 9$ ja 35 ovat pareittain suhteellisia alkulukuja, niin kiinalaisen jäännöslauseen mukaan kongruenssiryhmällä on yksikäsitteinen ratkaisu modulo $M = 4 \cdot 9 \cdot 35 = 1260$. Silloin

$$M_1 = \frac{1260}{4} = 315 \quad , \quad M_2 = \frac{1260}{9} = 140 \quad \text{ja} \quad M_3 = \frac{1260}{35} = 36.$$

Ratkaistaan nyt lukujen M_k käänteisluvut y_k modulo m_k. Luvun M_1 käänteisalkion y_1 saamme selville, kun ratkaistaan kongruenssi $315 y_1 \equiv 1 \pmod{4}$ muuttamalla se ensin lineaariseksi Diofantoksen yhtälöksi $315 y_1 - 4 y_2 = 1$ ja ratkaisemalla se Eukleideen algoritmin avulla. Saadaan

$$y_1 \equiv 3 \pmod{4}.$$

Vastaavasti luku y_2 saadaan selville ratkaisemalla kongruenssi $140 y_2 \equiv 1 \pmod{9}$, josta saadaan

$$y_2 \equiv 2 \pmod{9}.$$

Lopuksi luku y_3 saadaan ratkaisemalla kongruenssi $36y_3 \equiv 1 \pmod{35}$, josta saadaan

$$y_3 \equiv 1 \pmod{35}.$$

Siis

$$\begin{aligned} x &\equiv 3 \cdot 315 \cdot 3 + 5 \cdot 140 \cdot 2 + 10 \cdot 36 \cdot 1 \\ &\equiv 4595 \equiv 815 \pmod{1260}. \end{aligned}$$

Luku x toteuttaa kongruenssiryhmän, koska $815 \equiv 3 \pmod 4$, $815 \equiv 5 \pmod 9$ ja $815 \equiv 10 \pmod{35}$.

Esimerkki 2.3.2. Ratkaistaan kongruenssiryhmä

$$\begin{aligned} x &\equiv 1 \pmod 2, \\ x &\equiv 2 \pmod 3, \\ x &\equiv 3 \pmod 5, \\ x &\equiv 4 \pmod 7, \\ x &\equiv 5 \pmod{11}. \end{aligned}$$

Koska luvut $2, 3, 5, 7$ ja 11 ovat pareittain suhteellisia alkulukuja, niin kiinalaisen jäännöslauseen mukaan kongruenssiryhmällä on yksikäsitteinen ratkaisu modulo $M = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$. Silloin

$$M_1 = \frac{2310}{2} = 1155 \quad , \quad M_2 = \frac{2310}{3} = 770 \quad , \quad M_3 = \frac{2310}{5} = 462,$$
$$M_4 = \frac{2310}{7} = 330 \quad \text{ja} \quad M_5 = \frac{2310}{11} = 210.$$

Ratkaistaan nyt lukujen M_k käänteisluvut y_k modulo m_k. Luvun y_1 saamme selville, kun ratkaistaan kongruenssi $1155y_1 \equiv 1 \pmod 2$, jolloin saadaan $y_1 \equiv 1 \pmod 2$. Vastaavasti luku y_2 saadaan selville ratkaisemalla kongruenssi $770y_2 \equiv 1 \pmod 3$, josta saadaan $y_2 \equiv 2 \pmod 3$. Samalla tavalla saadaan $y_3 \equiv 3 \pmod 5$, $y_4 \equiv 1 \pmod 7$ ja $y_5 \equiv 1 \pmod{11}$. Siis

$$\begin{aligned} x &\equiv 1 \cdot 1155 \cdot 1 + 2 \cdot 770 \cdot 2 + 3 \cdot 462 \cdot 3 + 4 \cdot 330 \cdot 1 + 5 \cdot 210 \cdot 1 \\ &\equiv 10763 \equiv 1523 \pmod{2310}. \end{aligned}$$

2.4 Lineaariset kongruenssiryhmät

Lause 2.4.1. *Olkoot a, b, c, d, e ja f kokonaislukuja ja olkoon m positiivinen kokonaisluku. Jos $(\Delta, m) = 1$, missä $\Delta = ad - bc$, niin lineaarisella kongruenssiryhmällä*

$$\begin{aligned} ax + by &\equiv e \pmod{m}, \\ cx + dy &\equiv f \pmod{m} \end{aligned} \tag{2.4.1}$$

on yksikäsitteinen ratkaisu modulo m. Ratkaisu saadaan kongruensseista

$$\begin{aligned} x &\equiv \bar{\Delta}(de - bf) \pmod{m}, \\ y &\equiv \bar{\Delta}(af - ce) \pmod{m}, \end{aligned}$$

missä $\bar{\Delta}$ on luvun Δ käänteisluku modulo m.

Todistus. (Vrt. [4, s. 120].) Oletetaan, että $(\Delta, m) = 1$, missä $\Delta = ad - bc$. Kerrotaan ryhmän (2.4.1) ensimmäinen yhtälö luvulla d ja toinen luvulla b, jolloin saadaan

$$\begin{aligned} adx + bdy &\equiv de \pmod{m}, \\ bcx + bdy &\equiv bf \pmod{m}. \end{aligned}$$

Vähennetään sitten toinen kongruenssi ensimmäisestä, jolloin saadaan

$$(ad - bc)x \equiv de - bf \pmod{m}.$$

Koska $\Delta = ad - bc$, niin

$$\Delta x \equiv de - bf \pmod{m}.$$

Kerrotaan nyt edellisen kongruenssin molemmat puolet luvulla $\bar{\Delta}$, jolloin saadaan

$$x \equiv \bar{\Delta}(de - bf) \pmod{m}.$$

Vastaavasti, kerrotaan ryhmän (2.4.1) ensimmäinen yhtälö luvulla c ja toinen luvulla a, jolloin saadaan

$$\begin{aligned} acx + bcy &\equiv ce \pmod{m}, \\ acx + ady &\equiv af \pmod{m}. \end{aligned}$$

Vähennetään sitten ensimmäinen kongruenssi toisesta, jolloin saadaan

$$(ad - bc)y \equiv af - ce \pmod{m},$$

josta edelleen

$$\Delta y \equiv af - ce \pmod{m}.$$

Kerrotaan nyt edellisen kongruenssin molemmat puolet luvulla $\bar{\Delta}$, jolloin saadaan

$$y \equiv \bar{\Delta}(af - ce) \pmod{m}.$$

Siis, jos (x, y) on lineaarisen kongruenssiryhmän ratkaisu, niin

$$\begin{aligned} x &\equiv \bar{\Delta}(de - bf) \pmod{m}, \\ y &\equiv \bar{\Delta}(af - ce) \pmod{m}. \end{aligned}$$

Voimme helposti osoittaa, että mikä tahansa pari (x, y) on ratkaisu. Kun $x \equiv \bar{\Delta}(de - bf) \pmod{m}$ ja $y \equiv \bar{\Delta}(af - ce) \pmod{m}$, niin

$$\begin{aligned} ax + by &\equiv a\bar{\Delta}(de - bf) + b\bar{\Delta}(af - ce) \pmod{m}, \\ &\equiv \bar{\Delta}(ade - abf + abf - bce) \pmod{m}, \\ &\equiv \bar{\Delta}(ad - bc)e \pmod{m}, \\ &\equiv \bar{\Delta}\Delta e \pmod{m}, \\ &\equiv e \pmod{m} \end{aligned}$$

ja

$$\begin{aligned} cx + dy &\equiv c\bar{\Delta}(de - bf) + d\bar{\Delta}(af - ce) \pmod{m}, \\ &\equiv \bar{\Delta}(cde - bcf + adf - cde) \pmod{m}, \\ &\equiv \bar{\Delta}(ad - bc)f \pmod{m}, \\ &\equiv \bar{\Delta}\Delta f \pmod{m}, \\ &\equiv f \pmod{m}. \end{aligned}$$

□

Esimerkki 2.4.1. Ratkaistaan lineaarinen kongruenssiryhmä

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

Ratkaistaan ensin luku x. Kerrotaan ensimmäinen kongruenssi luvulla 1 ja toinen kongruenssi luvulla 2. Saadaan

$$\begin{aligned} x + 2y &\equiv 1 \pmod 5, \\ 4x + 2y &\equiv 2 \pmod 5. \end{aligned}$$

Vähennetään nyt toinen kongruenssi ensimmäisestä, jolloin saadaan

$$-3x \equiv -1 \pmod 5.$$

Kun kerrotaan kongruenssi puolittain luvulla -2, saadaan

$$6x \equiv 2 \pmod 5,$$

ja edelleen

$$x \equiv 2 \pmod 5.$$

Ratkaistaan sitten luku y. Kerrotaan nyt ensimmäinen kongruenssi luvulla 2 ja toinen kongruenssi luvulla 1. Saadaan

$$\begin{aligned} 2x + 4y &\equiv 2 \pmod 5, \\ 2x + y &\equiv 1 \pmod 5. \end{aligned}$$

Vähennetään nyt ensimmäinen kongruenssi toisesta, jolloin saadaan

$$-3y \equiv -1 \pmod 5.$$

Kun kerrotaan kongruenssi puolittain luvulla -2, saadaan

$$6y \equiv 2 \pmod 5,$$

ja edelleen

$$y \equiv 2 \pmod 5.$$

Tarkistetaan vielä, että pari (x, y) toteuttaa alkuperäisen kongruenssiryhmän. Siis, kun $x \equiv 2 \pmod 5$ ja $y \equiv 2 \pmod 5$, niin

$$\begin{aligned} x + 2y &\equiv 1 \cdot 2 + 2 \cdot 2 = 6 \equiv 1 \pmod 5, \\ 2x + y &\equiv 2 \cdot 2 + 1 \cdot 2 = 6 \equiv 1 \pmod 5. \end{aligned}$$

Siis kongruenssiryhmä toteutuu.

3 Kongruenssin sovelluksia

3.1 Ikikalenteri

Tämä alaluku seuraa tiiviisti Kenneth H. Rosenin kirjaa *Elementary Number Theory and its Applications*.

Ikikalenterin avulla voimme laskea minkä tahansa päivän ja vuoden viikonpäivän. Ensin kuitenkin käymme läpi hieman historiaa.

Varhaisissa egyptiläisissä kalentereissa vuoteen kuului 360 päivää ja vuodessa oli 12 kuukautta. Noin 4230 eKr. siirryttiin puhtaaseen aurinkokalenteriin, jossa vuosi oli 365-päiväinen. Viisi lisäpäivää lisättiin 12. kuukauden loppuun, siten kukin kuukausi sisälsi 30 päivää. Vuosi oli kuitenkin neljännesvuorokauden liian lyhyt, joten neljän vuoden kuluttua virhettä oli yksi vuorokausi. Vuonna 238 eKr. otettiin käyttöön neljän vuoden välein lisättävä karkauspäivä.

Roomalaisten ajanlaskussa vuosi oli ensin 303 vuorokautta pitkä ja siihen kuului 10 kuukautta. Vuosi alkoi maaliskuussa ja loppui joulukuussa. Neljä ensimmäistä kuukautta sai jumaliin viittaavan nimen: Martius, Aprilis, Maius ja Junius. Martius pyhitettiin sodan jumala Marsille, Aprilis lienee pyhitetty Venukselle, Maius nimettiin maan kasvillisuuden jumalattaren Majan mukaan ja Junius pyhitettiin Juppiterin puolisolle Junolle. Loput kuukaudet nimettiin järjestysnumeroilla Quintilis, Sextilis, September, October, November ja December. Seitsemännellä vuosisadalla eKr. vuoteen lisättiin tammikuu ja helmikuu. Tammikuu (Januarius) pyhitettiin Janukselle, kaiken alun ja lopun jumalalle ja Helmikuu (Februarius) on saanut nimensä puhdistus- ja uhrijuhlasta Februasta, jota vietettiin Februus-jumalan mukaan helmikuussa. Tammikuussa oli 29 ja helmikuussa 28 päivää. Joka toinen vuosi oli karkauskuukausi helmikuussa, mutta sen käyttö oli kuitenkin usein varsin mielivaltaista ja ajanlasku meni sekaisin.

Julius Caesar 46 eKr. uudisti kalenteria siten, että vuoden pituudeksi määrättiin 365.25 päivää. Täten joka neljäs vuosi sisälsi 366 päivää ja muut 365 päivää. Karkauspäivä sijoitettiin 24. päiväksi helmikuuta, koska aiempi

karkauskuukausi oli helmikuun 23. päivän jälkeinen aika. Juliaanista kalenteria sovellettiin tammikuun ensimmäisestä vuodesta 45 eKr. lähtien. Lisäksi uudenvuodenpäivä, joka aiemmin oli 1.3., siirrettiin 1. päivälle tammikuuta. Helmikuusta siirrettiin yksi päivä elokuuhun, syyskuusta yksi päivä lokakuuhun ja marraskuusta yksi päivä joulukuuhun. Tämä juliaaninen kalenteri säilyi Euroopassa yli 1600 vuotta. Koska tammikuu siirrettiin vuoden alkuun myöhemmin, syys-joulukuun nimet kulkevat kahta jäljessä niiden nykyisestä järjestysnumerosta.

Paavi Gregorius XIII sääti uuden kalenterin 1582. Hän muutti kalenterivuoden pituuden trooppista vuotta (365,2421897 vrk) paremmin vastaavaksi. Trooppinen vuosi on 11 minuuttia 14 sekuntia lyhyempi kuin 365,25 vrk. Siten se edistää juliaaniseen kalenteriin verrattuna vuorokauden 128 vuodessa. Ajanlaskussa puhutaan trooppisesta vuodesta eli ajasta, joka tarkalleen vastaa auringon täyttä kierrosta laskettuna kevätpäiväntasauspisteestä ja joka siten kiinteästi liittyy vuodenaikojen vaihteluun. Trooppista vuotta kutsutaan myös aurinkovuodeksi. Gregoriaaninen kalenteri määräsi, että karkausvuodet ovat jaollisia luvulla 4 sekä luvulla 400. Kuitenkaan vuodet, jotka ovat jaollisia luvulla 100, eivät ole karkausvuosia, vaikka ne olisivatkin jaollisia luvuilla 4 ja 400.

Gregoriaaninen kalenteri otettiin käyttöön aluksi vain roomalaiskatolisissa maissa. Ortodoksit ja luterilaiset vastustivat aluksi uudistusta. Gregoriaaninen kalenteri otettiin ensimmäisenä käyttöön Italiassa vuonna 1582, Suomessa se otettiin käyttöön vuonna 1753. Kaikkialla maailmassa käytössä oleva gregoriaaninen kalenteri on niin tarkka, että se eroaa aurinkovuodesta vain noin 25,92 sekuntia. Tämä eroavuus esiintyy, koska gregoriaaninen vuosi kestää noin 365,2425 päivää kun taas aurinkovuosi kestää noin 365,242216 päivää. Tuloksena on kolmen päivän virhe joka 10 000. vuosi.

Nyt voidaan alkaa määrittelemään kaavaa, jolla voidaan laskea minkä tahansa vuoden, minkä tahansa kuukauden ja minkä tahansa päivän viikonpäivä gregoriaanisen kalenterin mukaan. Koska viikossa on seitsemän päivää, käytämme laskuissa kongruenssia modulo 7. Olkoon W viikonpäivä siten,

että

sunnuntai = 0,
maanantai = 1,
tiistai = 2,
keskiviikko = 3,
torstai = 4,
perjantai = 5,
lauantai = 6.

Ensimmäinen karkausvuosi osui vuoteen 1600, joten käytetään vuoden 1600 maaliskuun ensimmäistä päivää laskukaavan pohjana. Huomaa, että uusi vuosi alkaa 1. maaliskuuta. Esimerkiksi maaliskuu vuonna 2007 oli vuoden ensimmäinen kuukausi ja helmikuu vuonna 2007 oli vuoden 2006 viimeinen kuukausi.

Olkoon m = kuukausi siten, että

Tammikuu = 11,
Helmikuu = 12,
Maaliskuu = 1,
Huhtikuu = 2,
Toukokuu = 3,
Kesäkuu = 4,
Heinäkuu = 5,
Elokuu = 6,
Syyskuu = 7,
Lokakuu = 8,
Marraskuu = 9,
Joulukuu = 10.

Olkoon lisäksi N vuosiluku siten, että $N = 100C + Y$, missä

C = vuosisata, ja
Y = vuosisadan ylimenevät vuodet, missä $0 < Y \leq 100$.

Esimerkki 3.1.1. Päivämäärästä 31.12.2007 saamme, että $k = 31$, $m = 10$, $N = 2007$, $C = 20$ ja $Y = 7$.

Huomautus. Mikäli N on tammi- tai helmikuu, niin vuosiluvuksi N merkitään edellinen vuosi.

Esimerkki 3.1.2. Loppiaisesta 6. tammikuuta vuonna 1980 saamme $k = 5$, $m = 11$, $N = 1979$, $C = 19$ ja $Y = 79$.

Olkoon d_N viikonpäivä maaliskuun ensimmäisenä päivänä vuonna N. Oletamme, että d_{1600} on tunnettu ja se on vuoden 1600 maaliskuun ensimmäinen päivä. Mikäli N ei ole karkausvuosi, vuodessa on 365 päivää. Näin ollen päivien 1. maaliskuuta vuonna $N-1$ ja 1. maaliskuuta vuonna N välillä on 365 päivää. Koska $365 \equiv 1 \pmod 7$, niin

$$d_N \equiv d_{N-1} + 1 \pmod 7.$$

Jos vuosi N on karkausvuosi, vuodessa on 366 päivää. Näin ollen 1. maaliskuuta vuonna $N-1$ ja 1. maaliskuuta vuonna N välillä on 366 päivää. Koska $366 \equiv 2 \pmod 7$, niin

$$d_N \equiv d_{N-1} + 2 \pmod 7.$$

Jotta pystymme löytämään viikonpäivän d_N, meidän täytyy tietää karkausvuosien lukumäärä vuosien 1600 ja N välillä. Olkoon karkausvuosien lukumäärä x. Huomaa, että luku x ei sisällä vuotta 1600, mutta sisältää vuoden N. Jakoalgoritmin perusteella vuosien 1600 ja N välillä on luvuilla 4, 100 ja 400 jaollisia vuosia vastaavasti

$$\left\lfloor \frac{N-1600}{4} \right\rfloor, \left\lfloor \frac{N-1600}{100} \right\rfloor \text{ ja } \left\lfloor \frac{N-1600}{400} \right\rfloor$$

kappaletta. Siten karkausvuosien lukumäärä saadaan vähentämällä toisistaan ne vuodet, jotka ovat jaollisia luvulla 4 ja 100, sekä lisäämällä ne vuodet, jotka ovat jaollisia luvulla 400. Lisäksi käytämme ominaisuutta, että $\lfloor x - a \rfloor =$

$\lfloor x \rfloor - a$, kunhan a on kokonaisluku, jolloin saadaan

$$\begin{aligned} x &= \lfloor (N-1600)/4 \rfloor - \lfloor (N-1600)/100 \rfloor + \lfloor (N-1600)/400 \rfloor \\ &= \lfloor N/4 \rfloor - 400 - \lfloor N/100 \rfloor + 16 + \lfloor N/400 \rfloor - 4 \\ &= \lfloor N/4 \rfloor - \lfloor N/100 \rfloor + \lfloor N/400 \rfloor - 388. \end{aligned}$$

Esimerkki 3.1.3. Laskemme nyt kuinka monta karkausvuotta on vuosien 1600 ja 2007 välissä. Sijoitetaan luku $N = 2007$ yhtälöön $x = \lfloor N/4 \rfloor - \lfloor N/100 \rfloor + \lfloor N/400 \rfloor - 388$, jolloin saadaan

$$\begin{aligned} x &= \lfloor 2007/4 \rfloor - \lfloor 2007/100 \rfloor + \lfloor 2007/400 \rfloor - 388 \\ &= 501 - 20 + 5 - 388 = 98. \end{aligned}$$

Nyt, koska $N = 100C + Y$, niin sijoittamalla tämä yhtälöön, saadaan

$$\begin{aligned} x &= \lfloor (100C+Y)/4 \rfloor - \lfloor (100C+Y)/100 \rfloor + \lfloor (100C+Y)/400 \rfloor - 388 \\ &= 25C + \lfloor Y/4 \rfloor - C - \lfloor Y/100 \rfloor + \lfloor C/4 \rfloor + \lfloor Y/400 \rfloor - 388 \\ &= 24C + \lfloor C/4 \rfloor + \lfloor Y/4 \rfloor - 388 \\ &\equiv 3C + \lfloor C/4 \rfloor + \lfloor Y/4 \rfloor - 3 \pmod 7. \end{aligned}$$

Huomaa, että $\lfloor Y/100 \rfloor = 0$ ja $\lfloor Y/400 \rfloor = 0$, koska $0 \leq Y < 100$.

Määritellään nyt d_N. Lisätään vuoden 1600 maaliskuun ensimmäisen päivän viikonpäivään yksi päivä jokaista vuotta kohti alkaen vuodesta 1600, sekä yksi päivä jokaista karkausvuotta kohden alkaen vuodesta 1600. Toisin sanoen

$$\begin{aligned} d_N &\equiv d_{1600} + N - 1600 + x \\ &= d_{1600} + 100C + Y - 1600 + 3C + \lfloor C/4 \rfloor + \lfloor Y/4 \rfloor - 3 \\ &\equiv d_{1600} - 2C + Y + \lfloor C/4 \rfloor + \lfloor Y/4 \rfloor \pmod 7. \end{aligned} \tag{3.1.1}$$

Esimerkki 3.1.4. Maaliskuun ensimmäinen päivä vuonna 2007 oli torstai, joten $d_{2007} = 4$. Lisäksi saamme, että $C = 20$ ja $Y = 7$.

Edellisen esimerkin perusteella pystymme laskemaan vuoden 1600 maaliskuun ensimmäisen päivän viikonpäivän. Sijoittamalla luvut $C = 20$ ja $Y = 7$, saadaan

$$4 \equiv d_{1600} - 2 \cdot 20 + 7 + \lfloor 20/4 \rfloor + \lfloor 7/4 \rfloor \pmod 7.$$

Edelleen kongruenssin laskusääntöjen perusteella saamme

$$d_{1600} \equiv 3 \pmod 7,$$

joten vuoden 1600 maaliskuun ensimmäinen päivä oli keskiviikko. Sijoittamalla nyt luku $d_{1600} = 3$ kaavaan (3.1.1), saadaan

$$d_N \equiv 3 - 2C + Y + \lfloor C/4 \rfloor + \lfloor Y/4 \rfloor \pmod 7. \tag{3.1.2}$$

Kaavan (3.1.2) avulla voimme laskea minkä tahansa vuoden maaliskuun ensimmäisen päivän.

Esimerkki 3.1.5. Lasketaan maaliskuun ensimmäinen päivä vuonna 2008. Koska $C = 20$ ja $Y = 8$, niin saamme

$$\begin{aligned} d_{2008} &\equiv 3 - 2 \cdot 20 + 8 + \lfloor 20/4 \rfloor + \lfloor 8/4 \rfloor \pmod 7 \\ &\equiv 6 \pmod 7. \end{aligned}$$

Siis vuoden 2008 maaliskuun ensimmäinen päivä on lauantai.

Yleistetään kaava (3.1.2) siten, että voimme laskea viikonpäivän minkä tahansa vuoden, minkä tahansa kuukauden ensimmäiselle päivälle. Tätä yleistystä varten, meidän tarvitsee tietää päivien lukumäärä kuukauden ensimmäisestä päivästä seuraavan kuukauden ensimmäiseen päivään. Kuukausille, joissa on 30 päivää, pätee $30 \equiv 2 \pmod 7$ ja kuukausille, joissa on 31 päivää, pätee $31 \equiv 3 \pmod 7$. Siten kuukaudet, joissa on 30 päivää, edistää seuraavan kuukauden ensimmäistä viikonpäivää kahdella, vastaavasti kuukaudet, joissa on 31 päivää, edistää kolmella.

Esimerkki 3.1.6. Maaliskuun ensimmäinen päivä vuonna 2007 oli torstai ja, koska maaliskuussa on 31 päivää, niin huhtikuun ensimmäinen päivä vuonna 2007 oli $(4+3) \equiv 0 \pmod 7$, eli sunnuntai. Edelleen toukokuun ensimmäinen päivä vuonna 2007 oli $(0+2) \equiv 2 \pmod 7$, eli tiistai.

Nyt yksitoista kuukausittaista lisäystä ovat seuraavat

1. maaliskuuta - 1. huhtikuuta :	3,
1. huhtikuuta - 1. toukokuuta :	2,
1. toukokuuta - 1. kesäkuuta :	3,
1. kesäkuuta - 1. heinäkuuta :	2,
1. heinäkuuta - 1. elokuuta :	3,
1. elokuuta - 1. syyskuuta :	3,
1. syyskuuta - 1. lokakuuta :	2,
1. lokakuuta - 1. marraskuuta :	3,
1. marraskuuta - 1. joulukuuta :	2,
1. joulukuuta - 1. tammikuuta :	3,
1. tammikuuta - 1. helmikuuta :	3.

Muotoilemme nyt kaavan, joka antaa yllä olevat lisäykset. Koska 11:stä lisäyksestä saadaan yhteensä 29 päivää, niin saadaan keskimäärin $2,6$ lisäystä joka kuukaudelle. Tarvitsemme kuitenkin tarkan kuukausittaisen lisäyksen. Reverend Zeller löysi ensimmäisenä funktion $\lfloor 2,6m-0,2\rfloor - 2$, missä $m = 2, \cdots, 12$, mikä antaa edellä mainitut lisäykset. Funktion arvo on nolla, kun $m = 1$. Siten funktio $d_N + \lfloor 2,6m-0,2\rfloor - 2 \pmod 7$ antaa vuoden N, kuukauden m ensimmäisen päivän viikonpäivän. Siten vuoden N, kuukauden m ensimmäisen päivän viikonpäivä W' saadaan kaavan (3.1.2) avulla. Saadaan

$$\begin{aligned} W' &\equiv \lfloor 2,6m-0,2\rfloor - 2 + 3 - 2C + Y + \lfloor C/4\rfloor + \lfloor Y/4\rfloor \pmod 7 \\ &\equiv 1 + \lfloor 2,6m-0,2\rfloor - 2C + Y + \lfloor C/4\rfloor + \lfloor Y/4\rfloor \pmod 7. \end{aligned} \tag{3.1.3}$$

Jotta pystymme laskemaan minkä tahansa vuoden N, minkä tahansa kuukauden m ja minkä tahansa päivän k viikonpäivän W, muotoilemme kaavan (3.1.3) koskemaan päivää k. Saamme

$$W \equiv k + \lfloor 2,6m-0,2\rfloor - 2C + Y + \lfloor C/4\rfloor + \lfloor Y/4\rfloor \pmod 7. \tag{3.1.4}$$

Esimerkki 3.1.7. Etsitään esimerkissä 3.1.1. annetun päivämäärän viikonpäivä. Sijoitetaan arvot kaavaan (3.1.4), jolloin saamme

$$\begin{aligned} W &\equiv 31 + \lfloor 2,6\cdot 10-0,2\rfloor - 2\cdot 20 + 7 + \lfloor 20/4\rfloor + \lfloor 7/4\rfloor \pmod 7 \\ &\equiv 29 \pmod 7 \\ &\equiv 1 \pmod 7. \end{aligned}$$

Siis 31.12.2007 on maanantai.

3.2 Kuningatarpulma

Kuningatar arvoituksen tavoitteena on asettaa p kuningatarta p x p-kokoiselle shakkilaudalle siten, ettei yksikään kuningatar uhkaa toista kuningatarta. On huomattava, että arvoituksella ei ole ratkaisua, mikäli $p = 2$ tai $p = 3$.

Kehitellään kaava, jonka avulla voidaan asettaa p kuningatarta p x p -kokoiselle shakkilaudalle, missä p on kokonaislukua kolme suurempi alkuluku.

Jotta voimme esittää kaavan kuningatarpulman ratkaisemiseen, asetetaan kuningattaret paikoilleen rivi riviltä. Olkoon $f(i)$ kuningattaren i paikka sarakkeessa, missä $1 \leq i \leq p$. Silloin $f(i)$ voidaan määritellä rekursiivisesti.

Määritelmä 3.2.1. Määritellään $f(i)$ rekursiivisesti siten, että

$$\begin{aligned} &f(0) = 0, \\ &f(i) \equiv f(i-1) + \frac{p+1}{2} \pmod{p}, \quad 1 \leq i \leq p-1 \quad \text{ja} \\ &f(p) = p. \end{aligned}$$

Määritellään nyt funktio $f(i)$ täsmällisesti.

Määritelmä 3.2.2. Olkoon $f(i)$ kuningattaren i paikka. Silloin, jos $1 \leq i \leq p$, niin

$$f(i) \equiv \left(\frac{p+1}{2}\right) i \pmod{p}.$$

Nyt $f(i)$ on yhtälön $\frac{(p+1)i}{2}$ pienin jäännös modulo p, missä jäännös 0 on tulkitaan luvuksi p.

Esitämme ja todistamme seuraavaksi funktion f ominaisuuksia.

Lause 3.2.1. *Funktio f on injektiivinen.*

Todistus. (Vrt. [3, s. 268].) Oletetaan, että i ja j ovat pienimmät jäännökset modulo p siten, että

$$f(i) = f(j).$$

Silloin

$$\left(\frac{p+1}{2}\right) i \equiv \left(\frac{p+1}{2}\right) j \pmod{p}.$$

Koska p on alkuluku, niin $\left(\frac{p+1}{2}, p\right) = 1$, joten lauseen (2.1.4) perusteella

$$i \equiv j \pmod{p}.$$

Mutta, koska i ja j ovat pienimmät jäännökset modulo p, on oltava $i = j$. Siis f on injektiivinen. □

Lause (3.2.1) määrää sen, että jokaisella rivillä ja sarakkeella on vain yksi kuningatar, kuten alla oleva kuva osoittaa, kun $p = 5$.

i \ j	1	2	3	4	5
1	.	Q	.	.	.
2	.	.	.	Q	.
3	Q	.	.	.	.
4	.	.	Q	.	.
5	.	.	.	.	Q

Taulukko 1: Viisi kuningatarta 5 x 5 -kokoisella shakkilaudalla.

Lause 3.2.2. *Mitkään kaksi kuningatarta, jotka on asetettu p x p -kokoiselle shakkilaudalle funktion f määräämällä tavalla, eivät voi uhata toisiaan.*

Todistus. (Vrt. [3, s. 268].) Koska jokaisella rivillä ja sarakkeella voi olla vain yksi kuningatar, joten mitkään kaksi kuningatarta eivät voi uhata toisiaan riveittäin eikä sarakkeittain. Riittää siis osoittaa, etteivät kuningattaret uhkaa toisiaan myöskään diagonaalisti.

Jokaisella nousevalla diagonaalilla, rivin i ja sarakkeen j summa $i+j = k$, missä k on vakio ja $2 \leq k \leq 2p$. Meidän tarvitsee siis tutkia vain diagonaaleja, missä $3 \leq k \leq 2p-1$.

Oletetaan, että on olemassa kaksi kuningatarta, jotka ovat samalla nousevalla diagonaalilla. Olkoot näiden kuningattarien sijainnit (i_1, j_1) ja (i_2, j_2).

Silloin

$$f(i_1) \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p} \quad \text{ja} \quad f(i_2) \equiv \left(\frac{p+1}{2}\right) i_2 \pmod{p}.$$

Siten

$$j_1 \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p} \quad \text{ja} \quad j_2 \equiv \left(\frac{p+1}{2}\right) i_2 \pmod{p}, \tag{3.2.1}$$

missä $i_1 + j_1 = k = i_2 + j_2$. Nyt

$$i_1 + j_1 \equiv \left(\frac{p+3}{2}\right) i_1 \pmod{p},$$

eli

$$k \equiv \left(\frac{p+3}{2}\right) i_1 \pmod{p}.$$

Vastaavasti saadaan, että

$$k \equiv \left(\frac{p+3}{2}\right) i_2 \pmod{p},$$

joten

$$\left(\frac{p+3}{2}\right) i_1 \equiv \left(\frac{p+3}{2}\right) i_2 \pmod{p}.$$

Siis, koska $(p, \frac{p+3}{2}) = 1$, niin lauseen (2.1.4) perusteella

$$i_1 \equiv i_2 \pmod{p}.$$

Koska luvuilla i_1 ja j_1 on pienin jakojäännös modulo p, niin on oltava $i_1 = i_2$. Siten kongruenssien (3.2.1) perusteella $j_1 = j_2$. Siis millään nousevalla diagonaalilla ei ole kahta kuningatarta.

On vielä osoitettava, ettei millään laskevalla diagonaalilla ole kahta kuningatarta. Jokaisella laskevalla diagonaalilla, joilla rivin i ja sarakkeen j erotus $i - j = l$, missä l on vakio ja $1 - p \leq l \leq p - 1$. Voimme olettaa, että $l \neq 1 - p$ ja $l \neq p - 1$.

Oletetaan, että on olemassa kaksi kuningatarta, jotka ovat samalla laskevalla diagonaalilla. Olkoot näiden kuningattarien sijainnit (i_1, j_1) ja (i_2, j_2). Silloin

$$f(i_1) \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p} \quad \text{ja} \quad f(i_2) \equiv \left(\frac{p+1}{2}\right) i_2 \pmod{p}.$$

Siten

$$j_1 \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p} \quad \text{ja} \quad j_2 \equiv \left(\frac{p+1}{2}\right) i_2 \pmod{p}, \tag{3.2.2}$$

missä $i_1 - j_1 = l = i_2 - j_2$. Nyt

$$i_1 - j_1 \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p},$$

eli

$$l \equiv \left(\frac{p+1}{2}\right) i_1 \pmod{p}.$$

Vastaavasti

$$l \equiv \left(\frac{p+1}{2}\right) i_2 \pmod{p}.$$

Koska $(\frac{p+1}{2}, p) = 1$ ja luvuilla i_1 ja j_1 on pienin jakojäännös modulo p, niin $i_1 = i_2$. Siten kongruenssien (3.2.2) perusteella $j_1 = j_2$, joten yhdelläkään laskevalla diagonaalilla ei ole kahta kuningatarta.

Siis mitkään kaksi kuningatarta, jotka on asetettu p x p -kokoiselle shakkilaudalle funktion f määräämällä tavalla, eivät voi uhata toisiaan. □

Algoritmi. Sijoitetaan p kuningatarta p x p -kokoiselle shakkilaudalle. Kuningattaren paikka rivillä i sarakkeessa s_i, missä $i = 1, 2, \ldots, p$, saadaan kaavalla

$$s_i \equiv \frac{p+1}{2} + s_{i-1} \pmod{p},$$

missä $s_0 = 0$.

Esimerkki 3.2.1. Sijoitetaan 7 kuningatarta 7 x 7 -kokoiselle shakkilaudalle. Saadaan

$$\begin{aligned}
s_1 &\equiv \frac{7+1}{2} = 4 \equiv 4 \pmod{7}, & s_2 &\equiv \frac{7+1}{2} + 4 \equiv 1 \pmod{7}, \\
s_3 &\equiv \frac{7+1}{2} + 1 \equiv 5 \pmod{7}, & s_4 &\equiv \frac{7+1}{2} + 5 \equiv 2 \pmod{7}, \\
s_5 &\equiv \frac{7+1}{2} + 2 \equiv 6 \pmod{7}, & s_6 &\equiv \frac{7+1}{2} + 6 \equiv 3 \pmod{7}, \\
s_7 &\equiv \frac{7+1}{2} + 3 \equiv 7 \pmod{7}.
\end{aligned}$$

Sijoitetaan nyt kuningattaret shakkilaudalle alla olevan kuvan osoittamalla tavalla.

i \ j	1	2	3	4	5	6	7
1	.	.	.	Q	.	.	.
2	Q	.	.	.	.	.	.
3	.	.	.	.	Q	.	.
4	.	Q	.	.	.	.	.
5	.	.	.	.	.	Q	.
6	.	.	Q	.	.	.	.
7	.	.	.	.	.	.	Q

Taulukko 2: Seitsemän kuningatarta 7 x 7 -kokoisella shakkilaudalla.

3.3 Turnausaikataulu

Kongruenssia voidaan käyttää myös aikataulun laatimiseen sellaisissa turnauksissa, missä kaikki osallistujat pelaavat toisiaan vastaan. Osallistuja voi olla esim. yksilö tai joukkue. Tässä kappaleessa näytämme, kuinka tehdä turnausaikataulu, kun joukkueita on N kappaletta ja kaikki joukkueet pelaavat toisiaan vastaan.

Olkoon siis turnauksessa N joukkuetta. Jos luku N on pariton, niin jokaisella kierroksella yksi joukkue pitää taukoa, kuitenkaan yksikään joukkue ei pidä taukoa kuin yhden kerran. Jos taas luku N on parillinen, niin kaikki joukkueet pelaavat samaan aikaan ja tällöin pelejä on yhtä aikaa käynnissä parillinen määrä. Huomaa, että vaikka N olisi pariton, niin pelejä on yhtä aikaa käynnissä parillinen määrä.

Määritelmä 3.3.1. Olkoon N joukkueiden kokonaislukumäärä. Olkoot lisäksi i ja j joukkueita siten, että i ja j ovat eri joukkueita. Joukkueiden $1, 2, \ldots, N-1$ aikataulu voidaan laskea kaavalla

$$i + j \equiv k \pmod{N-1},$$

missä joukkue i pelaa joukkuetta j vastaan kierroksella k.

Joukkueiden N ja i välinen ottelu voidaan laskea kaavalla

$$2i \equiv k \pmod{N-1}.$$

Kierros	Joukkue					
	1	2	3	4	5	6
1	5	4	6	2	1	3
2	6	5	4	3	2	1
3	2	1	5	6	3	4
4	3	6	1	5	4	2
5	4	3	2	1	6	5

Taulukko 3: Turnausaikataulu viidelle joukkueelle.

Esimerkki 3.3.1. Olkoon joukkueiden kokonaislukumäärä kuusi, eli $N = 6$. Silloin joukkueiden 4 ja 5 välinen ottelu on kierroksella

$$4 + 5 = 9 \equiv 4 \pmod{5}.$$

Siis joukkueet 4 ja 5 kohtaavat kierroksella 3.

Joukkueet 3 ja 6 kohtaavat kierroksella

$$2 \cdot 3 = 6 \equiv 1 \pmod{5}.$$

Siis joukkueet 3 ja 6 kohtaavat ensimmäisellä kierroksella.

Kun joukkueita on kuusi, saadaan aikatauluksi seuraava taulukko.

Lause 3.3.1. *Jokainen joukkue pelaa toista joukkuetta vastaan täsmälleen kerran.*

Todistus. (Vrt. [4, s. 184].) Joukkue N pelaa joukkuetta i vastaan kierroksella k, missä $2i \equiv k \pmod{N-1}$. Nyt kongruenssi $2i \equiv k \pmod{N-1}$ on ratkeava, koska $(2, N-1) = 1$ ja $1 \mid k$. Tällöin ratkaisujen lukumäärä on täsmälleen $(2, N-1) = 1$ kappaletta. Siis joukkue N pelaa joukkuetta i vastaan täsmälleen kerran.

Tarkastellaan sitten joukkueita $1, 2, \ldots, N-1$. Tehdään vastaoletus, että joukkueet i ja j, missä $1 \leq i \leq N-1$, $1 \leq j \leq N-1$ ja $i \neq j$, pelaavat vastakkain kierroksilla k_1 ja k_2. Silloin

$$i + j \equiv k_1 \pmod{N-1} \quad \text{ja} \quad i + j \equiv k_2 \pmod{N-1}.$$

Edelleen

$$k_1 \equiv k_2 \pmod{N-1},$$

mikä on selvästi ristiriita, koska piti olla $k_1 \not\equiv k_2 \pmod{N-1}$. Siis joukkueet pelaavat keskenään täsmälleen kerran. □

Esimerkki 3.3.2. Olkoon joukkueiden kokonaislukumäärä seitsemän, eli $N = 7$. Koska joukkueita on pariton määrä, niin jokaisella kierroksella yksi joukkue on tauolla. Nyt joukkueiden 1 ja 2 välinen ottelu on kierroksella $1 + 2 \equiv 3 \pmod{6}$. Siis joukkueet 1 ja 2 kohtaavat kierroksella 3.

Joukkueet 1 ja 3 kohtaavat kierroksella $1+3 \equiv 4 \pmod{6}$. Siis joukkueet 1 ja 3 kohtaavat kierroksella 4.

Joukkueet 1 ja 6 kohtaavat kierroksella $2 \cdot 1 \equiv 2 \pmod{6}$. Siis joukkueet 1 ja 6 kohtaavat toisella kierroksella.

Kun kaikki ottelut on laskettu, voidaan muodostaa taulukko turnausaikataululle.

	Joukkue						
Kierros	1	2	3	4	5	6	7
1	7	6	5	tauko	3	2	1
2	tauko	7	6	5	4	3	2
3	2	1	7	6	tauko	4	3
4	3	tauko	1	7	6	5	4
5	4	3	2	1	7	tauko	5
6	5	4	tauko	2	1	7	6
7	6	5	4	3	2	1	tauko

Taulukko 4: Turnausaikataulu seitsemälle joukkueelle.

Lähdeteokset

[1] Burton, David M., *Elementary Number Theory*, 5th ed., The McGraw-Hill Companies, New York, 2005.

[2] Kangasaho Jukka, Mäkinen Jukka, Oikkonen Juha, Paasonen Johannes ja Salmela Maija, *Logiikka ja lukuteoria*, 1.-4. painos, WS Bookwell Oy, Porvoo, 2004.

[3] Koshy, Thomas, *Elementary number theory with applications*, A Harcourt Science and Technology Company, California, 2002.

[4] Rosen, Kenneth H., *Elementary number theory and its applications*, 3rd ed., Addison-Wesley Publishing Company, Reading, Massachusetts, 1993.

[5] Internet osoite http://fi.wikipedia.org/wiki/Alkuluku (28.9.2007).

[6] Aamulehti, Alkulukujen tekijöitä, 27.3.2007.
Internet osoite http://www.aamulehti.fi/teema/tiede/15642.shtml.