Algebra 8op

Syksy 2008

Sisältö

Merkinnät

Kurssilla käytetään tavanomaisia logiikan merkintöjä

$p \vee q$	tai (ainakin yksi)
$p \wedge q$	ja (kaikki)
$p \Rightarrow q$	seuraa
$p \Leftrightarrow q$	yhtäpitävää
$\exists x$	on olemassa alkio x
$\forall x$	kaikilla alkioilla x

sekä joukko-opillisia merkintöjä

$\emptyset$ tai $\{\,\}$	tyhjä joukko (ei alkioita)
$x \in A$	joukon alkio, kuuluu joukkoon
$x \notin A$	ei joukon alkio, ei kuulu joukkoon
$A \subseteq B$	osajoukko, inkluusio
$A \subset B$	aito osajoukko
$A \cup B$, $\cup_{i=1}^{n} A_i$, $\cup_{i=1}^{\infty} A_i$, $\cup_{i \in I} A_i$	joukkojen yhdisteitä
$A \cap B$, $\cap_{i=1}^{n} A_i$, $\cap_{i=1}^{\infty} A_i$, $\cap_{i \in I} A_i$	joukkojen leikkauksia
$E \setminus A = \overline{A}$	komplementti
$A \setminus B = A \cap \overline{B}$	erotus

Isot kirjaimet A, B, C, ... edustavat tällä kurssilla yleensä joukkoja, pienet kirjaimet ovat yleensä alkioita tai funktioita.

Merkinnällä $X := \textit{lauseke}$ asetetaan symbolille X arvo *lauseke*.

Lukujoukoista käytetään merkintöjä:

$\mathbb{N} = \{1, 2, 3, \ldots\}$	luonnolliset luvut
$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$	ei-negatiiviset kokonaisluvut
$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$	kokonaisluvut
$k\mathbb{Z} = \{\ldots, -3k, -2k, -k, 0, k, 2k, 3k, \ldots\}$	k-monikerrat
$\mathbb{Z}_k = \{0, 1, 2, 3, \ldots, k-1\}$	kokonaisluvut modulo k
$\mathbb{Q} = \{\, \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N} \,\}$	rationaaliluvut
$\mathbb{R}$	reaaliluvut
$\mathbb{C} = \{\, x + iy \mid x, y \in \mathbb{R} \,\}$	kompleksiluvut
A_+	aidosti positiivinen osa

1. Lukuteorian alkeita

Seuraavassa tutkitaan kokonaislukujen joukkoa $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$. Kokonaislukujen yhteenlaskun $+$, kertolaskun $\cdot$ ja järjestyksen $\leq$ "perusominaisuudet"oletetaan tunnetuiksi. Myös seuraavaa aksioomaa pidetään tunnettuna:

Aksiooma 1.1. *Jokaisessa epätyhjässä ei-negatiivisten kokonaislukujen osajoukossa on pienin luku.*

1.1. Jaollisuus

Kokonaisluku b on jaollinen kokonaisluvulla a, jos on olemassa $k \in \mathbb{Z}$, s.e. $b = ka$.

Määritelmä 1.2. Olkoot $a, b \in \mathbb{Z}$. Tällöin a on luvun b *tekijä*, jos $b = ka$ jollekin $k \in \mathbb{Z}$.

Voidaan sanoa myös, että a *jakaa* b:n, b on *jaollinen* luvulla a tai b on a:n *monikerta*. Merkintä tälle on $a \mid b$. Vastaavasti merkitään $a \nmid b$, jos a ei ole b:n tekijä.

Siis esimerkiksi $2 \mid 6$, $3 \mid 9$, mutta $4 \nmid 22$.

Jaollisuudella on mm. seuraavat ominaisuudet:

Lemma 1.3. *Olkoot $a, b, c, d \in \mathbb{Z}$. Tällöin:*

1. $a \mid 0$, $1 \mid a$, $-1 \mid a$, $a \mid a$, $-a \mid a$.
2. *Jos* $a \mid b$ *ja* $c \mid d$, *niin* $ac \mid bd$.
3. *Jos* $a \mid b$ *ja* $b \mid c$, *niin* $a \mid c$.
4. $a \mid 1 \iff a = 1$ *tai* $a = -1$.
5. $a \mid b$ *ja* $b \mid a \iff a = b$ *tai* $a = -b$.
6. *Jos* $a \mid b$ *ja* $b \neq 0$, *niin* $|a| \leq |b|$.
7. *Jos* $a \mid b_i$ *kaikilla* $i = 1, \ldots, n$, *niin*

$$a \mid b_1 c_1 + \ldots + b_n c_n$$

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

Todistus. Todistetaan pari kohtaa malliksi, loput jätetään harjoitustehtäviksi.

Kohta 2: Koska $a \mid b$ ja $c \mid d$, on olemassa luvut k_1, $k_2 \in \mathbb{Z}$ siten, että $b = k_1 a$ ja $d = k_2 c$. Silloin

$$bd = (k_1 a)(k_2 c) = (k_1 k_2)(ac),$$

eli $ac \mid bd$.

Kohta 6: Koska $a \mid b$, on olemassa $k \in \mathbb{Z}$ siten, että $b = ka$. Koska $b \neq 0$, on myös $k \neq 0$. Siis $|k| \geq 1$, joten

$$|b| = |ka| \geq |a|.$$

□

Huomautus. Lemman 1.3 kohdan 6 mukaan $|a| \leq |b|$. Tämä on yhtäpitävä epäyhtälön $-|b| \leq |a| \leq |b|$ kanssa. Siis jokaisella nollasta poikkeavalla kokonaisluvulla on vain äärellinen määrä tekijöitä.

Tehtävä. Etsi lukujen 9, 13, 20 ja 64 tekijät.

Yksinkertainen menetelmä sen ratkaisemiseksi, onko annettu kokonaisluku b jaollinen toisella kokonaisluvulla a, on jaon suorittaminen jakokulmassa eli jakoalgoritmi.

Kokonaislukujen jakoyhtälö. Esimerkiksi osamäärän

$$\frac{4509}{31} = 145\,\frac{14}{31}$$

kokonaisosa on 145 ja jakojäännös 14, mikä voidaan ilmaista myös muodossa

$$4509 = 31 \cdot 145 + 14.$$

Huomautus. Jos vaadimme vain, että a, $b \in \mathbb{Z}$ ja $b > 0$, niin muotoa

$$a = bq + r$$

olevia esityksiä on äärettömän paljon. Esimerkiksi jos $a = 64$ ja $b = 5$, niin

$$\begin{aligned} 64 &= 5 \cdot 1 + 59, \\ 64 &= 5 \cdot 10 + 14, \\ 64 &= 5 \cdot 20 - 36, \\ 64 &= 5 \cdot 11 + 9, \\ 64 &= 5 \cdot 12 + 4. \end{aligned}$$

Näistä viimeinen on sellainen, että $0 \leq r < 5$.

Lause 1.4 (Jakoyhtälö). *Olkoot a, $b \in \mathbb{Z}$, $b > 0$. Tällöin on olemassa yksikäsitteiset luvut q, $r \in \mathbb{Z}$ siten, että*

$$a = bq + r \quad \textit{ja} \quad 0 \leq r < b. \tag{1.1}$$

Luku r on jakoyhtälön mukainen pienin ei-negatiivinen (jako)jäännös.

Todistus. Tutkitaan kaikkia mahdollisia ei-negatiivisia lukuja $r = a - bq$, ja etsitään niistä pienin.

Olemassaolo. Olkoon x kokonaisluku, ja olkoon S muotoa $a - bx$ olevien ei-negatiivisten kokonaislukujen joukko, eli

$$S = \{\, a - bx \mid x \in \mathbb{Z} \text{ ja } a - bx \in \mathbb{N}_0 \,\}.$$

Esimerkiksi äskeisessä tilanteessa meillä olisi joukko

$$S_{64} = \{\, 64 - 5x \mid x \in \mathbb{Z} \text{ ja } 64 - 5x \in \mathbb{N}_0\},$$

ja ainakin luvut 59, 14, 74 ja 4 kuuluvat joukkoon S_{64}, sillä $59 = 64-5\cdot 1$, $14 = 64-5\cdot 10$, $74 = 64 - 5\cdot(-2)$, $4 = 64 - 5\cdot 12$.

Vaihe 1. Osoitetaan aluksi, että joukko S ei koskaan voi olla tyhjä joukko.

1. Jos $a \geq 0$, niin silloin $a - b\cdot 0 = a \in S$.

2. Jos $a < 0$, niin silloin $a - b\cdot a = a(1-b) \in S$, koska sekä a että $1-b$ ovat ei-positiivisia. Siis $a - bx$ on ei-negatiivinen luvulle $x = a$.

Siten joukko S on epätyhjä ei-negatiivisten kokonaislukujen osajoukko. Järjestysaksioooman 1.1 mukaan joukossa S on pienin alkio. Olkoon r tämä pienin alkio. Koska $r \in S$, niin r on muotoa $r = a - bx$ jollekin $x \in \mathbb{Z}$; merkitään tätä $x = q$. Siis

$$r = a - bq \text{ tai } a = bq + r.$$

Koska $r \in S$, on $r \geq 0$.

Vaihe 2. Todistetaan toiseksi, että joukon S pienin alkio $r < b$.

Tehdään vastaoletus: $r \geq b$. Silloin luku $a - b(q+1) \in S$, sillä

$$a - b(q+1) = (a-bq) - b = r - b,$$

ja koska $r - b \geq 0$, on myös $a - b(q+1) \geq 0$. Mutta koska b on positiivinen, on $r - b < r$. Siispä

$$a - b(q+1) = r - b < r,$$

mikä osoittaisi, että $a - b(q+1)$ olisi pienempi kuin r. Mutta r oli joukon S pienin alkio, ja näin on saatu ristiriita. Siis on oltava $r < b$. Olemme todistaneet jakoyhtälöesityksen olemassaolon.

Yksikäsitteisyys. Osoitetaan, että esitys (1.1) on yksikäsitteinen, eli että q ja r ovat ainoat luvut, joille $a = bq + r$ ja $0 \leq r < b$.

Tämän todistamiseksi oletetaan, että olisi olemassa toiset luvut q_1 ja r_1, joille myös pätisi $a = bq_1 + r_1$, $0 \leq r_1 < b$.

Nyt joko $r \geq r_1$ tai $r < r_1$. Oletetaan, että $r \geq r_1$. Vähentämällä yhtälöt toisistaan saamme

$$\begin{array}{rcl} a & = & bq + r \\ a & = & bq_1 + r_1 \\ \hline 0 & = & bq - bq_1 + r - r_1 \end{array}$$

$$\begin{array}{rcl} bq_1 - bq & = & r - r_1 \\ b(q_1 - q) & = & r - r_1. \end{array}$$

Viimeisen yhtälön mukaan $r - r_1$ on luvun b monikerta. Mutta $b > 0$ ja $r - r_1 \geq 0$, joten $q_1 - q$ on välttämättä ei-negatiivinen kokonaisluku. Siispä $r - r_1$ on jokin luvuista $0b, 1b, 2b, 3b, 4b, \ldots$.

Mutta $0 \leq r_1 \leq r < b$, joten $0 \leq r - r_1 < b$. Näin ollen ainoa mahdollisuus on, että $r - r_1 = 0b = 0$. Siten $r = r_1$.

Lopuksi, koska $b(q_1 - q) = r - r_1 = 0$ ja $b > 0$, on myös $q_1 - q = 0$ eli $q_1 = q$.

Samanlainen päättely todistaa yksikäsitteisyyden myös tapauksessa $r < r_1$. □

Esimerkki 1.5. Todista, että minkään kokonaisluvun kuutio ei ole muotoa $4k+2$ millään $k \in \mathbb{Z}$.

Ratkaisu. Olkoon a kokonaisluku. Silloin joko $a = 4q$, $a = 4q+1$, $a = 4q+2$, tai $a = 4q+3$ jollekin kokonaisluvulle $q \in \mathbb{Z}$. Toisin sanoen, kun a jaetaan neljällä, jakojäännös on jokin luvuista 0, 1, 2 tai 3. Silloin joko

$a^3 = (4q)^3 = 64q^3 = 4 \cdot 16q^3 + 0,$

$a^3 = (4q+1)^3 = 64q^3 + 48q^2 + 12q + 1 = 4(16q^3 + 12q^2 + 3q) + 1,$

$a^3 = (4q+2)^3 = 64q^3 + 96q^2 + 48q + 8 = 4(16q^3 + 24q^2 + 12q + 2) + 0$ tai

$a^3 = (4q+3)^3 = 64q^3 + 144q^2 + 108q + 27 = 4(16q^3 + 36q^2 + 27q + 6) + 3$

Koska jakoyhtälön antama esitys on yksikäsitteinen, on jokin ylläolevista luvun a^3 esitys, kun a^3 jaetaan neljällä. Tilannetta, jossa jakojäännös olisi ollut 2, ei esiintynyt.

Esimerkki 1.6. Todista jakoyhtälön avulla, että jos a on pariton ja a^2 jaetaan neljällä, niin jakojäännös on yksi.

Suurin yhteinen tekijä Olkoot $a_1, \ldots, a_n \in \mathbb{Z}$ s.e. $a_{i_0} \neq 0$ jollekin $i_0 \in \{1, \ldots, n\}$. Tällöin joukko

$$A = \{k \in \mathbb{N} : \quad k \mid a_i \quad \forall \quad i = 1, \ldots, n\}$$

on epätyhjä, sillä $1 \in A$. Toisaalta, Lemman 1.3 nojalla $|k| = k \leq a_{i_0}$. On ilmeistä, että joukossa A (=lukujen $a_1, \ldots, a_n$ yhteisten tekijöiden joukko) on yksikäsitteinen suurin alkio. Näin ollen seuraava määritelmä on mielekäs:

Määritelmä 1.7. Olkoot $a_1, \ldots, a_n \in \mathbb{Z}$ lukuja, joista ainakin yksi ei ole nolla. Lukujoukon $\{a_1, \ldots, a_n\}$ *suurin yhteinen tekijä* (*greatest common divisor, gcd*) $d = \text{syt}(a_1, \ldots, a_n)$ on suurin luku $d \in \mathbb{N}$, jolle $d \mid a_i$ kaikilla $i = 1, 2, \ldots, n$. Toisin sanoen

$$\text{syt}(a_1, \ldots, a_n) = \max\{\, k \in \mathbb{Z} : k \mid a_i \text{ kaikilla } i = 1, 2, 3, \ldots, n \,\}.$$

Mikäli $\text{syt}(a, b) = 1$, lukuja a ja b sanotaan *keskenään jaottomiksi* tai *suhteellisiksi alkuluvuiksi* (*relatively prime*, *coprime*).

Esimerkki 1.8. Kokonaislukujen a ja 0 yhteisiä tekijöitä ovat luvun a tekijät. Jos $a > 0$, niin luvun a suurin tekijä on selvästi a itse. Siis, jos $a > 0$, niin $\text{syt}(a, 0) = a$.

Sama hieman yleisemmin:

Esimerkki 1.9. Olkoot $a_1, \ldots, a_n \in \mathbb{Z} \setminus 0$. Tällöin

$$\text{syt}(0, a_1, \ldots, a_n) = \text{syt}(a_1, \ldots, a_n)$$

sillä

$$A_1 = \{n \in \mathbb{N} : n \mid a_i \quad \forall \quad i = 1, \ldots, n\} = \{n \in \mathbb{N} : n \mid a_i \quad \forall \quad i = 1, \ldots, n \quad \text{ja} \quad n \mid 0\} = A_2.$$

(Jos $n \in A_1$, niin $n \in A_2$, koska triviaalisti $n \mid 0$. Siis $A_1 \subset A_2$. Selvästi $A_2 \subset A_1$.)

Siis sillä ei ole merkitystä, kuuluuko 0 tarkasteltaviin lukuihin vai ei.

Lukujen 12 ja 30 suurin yhteinen tekijä on 6. Luvun 6 voi kirjoittaa lukujen 12 ja 30 *lineaarikombinaationa*: Esimerkiksi

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

Esitys ei siis ole yksikäsitteinen, mutta ainakin yksi sellainen on olemassa:

Lause 1.10 (syt **lineaarikombinaationa).** *Olkoot a ja b kokonaislukuja, joista ainakin toinen on erisuuri kuin* 0*, ja olkoon $d := \text{syt}(a, b)$. Silloin on olemassa kokonaisluvut u ja v siten, että $d = au + bv$.*

Todistus. Olkoon S niiden lukujen a ja b lineaarikombinaatioiden joukko, jotka ovat lisäksi luonnollisia lukuja, eli

$$S = \{au + bv \mid u, v \in \mathbb{Z}\} \cap \mathbb{N}.$$

Lauseen todistamiseksi etsimme joukon S pienimmän alkion, ja todistamme, että se on $\text{syt}(a, b)$.

Ensinnäkin, $a^2+b^2 = aa+bb$ kuuluu joukkoon S, ja koska ainakin toinen luvuista a, $b \neq 0$, niin $aa+bb > 0$. Näin ollen joukko S on epätyhjä, ja järjestysaksiooman mukaan joukossa S on pienin alkio. Olkoon t tämä pienin joukon S alkio. Silloin $t = au + bv$ joillekin u, $v \in \mathbb{Z}$. Väitämme, että $t = \text{syt}(a, b)$.

Väite 1: $t \mid a$. Jakoyhtälön perusteella on olemassa kokonaisluvut q ja r siten, että $a = tq + r$, missä $0 \leq r < t$. Todistetaan, että $r = 0$, jolloin $t \mid a$.

Vastaoletus: Oletetaan, että $r > 0$. Tällöin

$$\begin{aligned} r &= a - tq = a - (au+bv)q \\ &= (a - aqu) - (bv)q \\ &= a(1-qu) + b(-vq). \end{aligned}$$

Näin ollen r on lukujen a ja b lineaarikombinaatio, ja koska $r > 0$, on $r \in S$. Koska $0 < r < t$ ja t on joukon S pienin positiivinen alkio, on löydetty ristiriita. Siis $r = 0$.

Samanlaisella päättelyllä osoitetaan, että $t \mid b$.

Siis t on lukujen a ja b yhteinen tekijä.

Väite 2: t on suurin. Olkoon nyt c mikä tahansa lukujen a ja b yhteinen tekijä. Osoitetaan, että $c \leq t$, jolloin t on lukujen a ja b suurin yhteinen tekijä.

Koska $c \mid a$ ja $c \mid b$, on $a = r_1 c$ ja $b = r_2 c$ joillekin kokonaisluvuille r_1, r_2. Tästä seuraa:

$$t = au + bv = (r_1 c)u + (r_2 c)v = c(r_1 u + r_2 v).$$

Täten $c \mid t$. Mutta tällöin $c \leq |t|$, ja koska $t \geq 0$, on $c \leq t$. □

Seuraus 1.11. *Olkoot a ja b kokonaislukuja, joista ainakin toinen poikkeaa nollasta. Tällöin* $\operatorname{syt}(a, b) = 1$ *jos ja vain jos on olemassa u, $v \in \mathbb{Z}$, joille $au + bv = 1$.*

Todistus. Harjoitustehtävä. □

Lineaarikombinaatioesityksen avulla voidaan todistaa seuraava tulos, joka voisi olla yhteisen tekijän määritelmänä.

Seuraus 1.12. *Olkoot a ja b kokonaislukuja, joista ainakin toinen on erisuuri kuin 0, ja olkoon d positiivinen kokonaisluku. Silloin d on lukujen a ja b suurin yhteinen tekijä, jos ja vain jos seuraavat kaksi ehtoa toteutuvat:*

1. *$d \mid a$ ja $d \mid b$, ja*
2. *jos $c \mid a$ ja $c \mid b$, niin $c \mid d$.*

Todistus. a) Oletetaan ensin, että $d = \operatorname{syt}(a, b)$. Silloin $d \geq 1$ ja d toteuttaa ehdon 1 määritelmänsä nojalla. Olkoon nyt c mikä tahansa lukujen a ja b yhteinen tekijä, ts. $c \mid a$ ja $c \mid b$. Silloin $a = rc$ ja $b = sc$ joillekin kokonaisluvuille r ja s. Lauseen 1.10 perusteella luku d voidaan esittää lukujen a ja b lineaarikombinaationa, ts. on olemassa kokonaisluvut u ja v, joille $d = au + bv$. Silloin $c \mid d$, koska

$$d = au + bv = (rc)u + (sc)v = c(ru + sv).$$

b) Oletetaan, että d toteuttaa lauseen ehdot, ja todistetaan, että $d = \operatorname{syt}(a, b)$.

Ehdon 1 mukaan $d \mid a$ ja $d \mid b$, eli d on todella lukujen a ja b yhteinen tekijä. Jos c on mielivaltainen lukujen a ja b yhteinen tekijä, niin ehdon 2 mukaan silloin $c \mid d$. Tästä seuraa $c \leq |d|$. Mutta koska d on oletuksen mukaan positiivinen, on $|d| = d$ ja siten $c \leq d$. Näin ollen d on lukujen a ja b suurin yhteinen tekijä. □

Tämän seurauksen voi helposti yleistää koskemaan n luvun $a_1, \ldots, a_n$ yhteistä tekijää $\operatorname{syt}(a_1, \ldots, a_n)$.

Jos $a \mid bc$, niin milloin pätee, että $a \mid b$ tai $a \mid c$? Helposti nähdään, että edellä mainittu ei aina toteudu, esimerkiksi $6 \mid 3 \cdot 4$, mutta $6 \nmid 3$ ja $6 \nmid 4$.

Lause 1.13. *Jos $a \mid bc$ ja* $\operatorname{syt}(a, b) = 1$, *niin $a \mid c$.*

Todistus. Koska $\text{syt}(a,b) = 1$, on Lauseen 1.10 nojalla 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 $r \in \mathbb{Z}$ ja siten

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

Siis $a \mid c$. □

Lemma 1.14. *Oletetaan, että $a, b > 0$. Jos $\text{syt}(a,b) = d$, niin $\frac{a}{d}$ ja $\frac{b}{d}$ ovat keskenään jaottomia.*

Todistus. Harjoitustehtävä. □

Esimerkki 1.15. Osoita, että jos $c > 0$, niin

$$\text{syt}(ca, cb) = c \cdot \text{syt}(a,b).$$

Suurimman yhteisen tekijän etsimiseen on tehokas *Eukleideen algoritmi*. Algoritmin perustelemiseksi tarvitsemme seuraavan aputuloksen:

Lemma 1.16. *Olkoot a, b, $m \in \mathbb{Z} \setminus \{0\}$. Tällöin*

$$\text{syt}(bm + a, b) = \text{syt}(a,b).$$

Todistus. Olkoot

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

Osoitetaan, että $A_1 = A_2$, eli että luvuilla $bm + a$ ja b on samat yhteiset tekijät kuin luvuilla a ja b.

Väite 1: $A_1 \subseteq A_2$. Olkoon k lukujen $bm + a$ ja b yhteinen tekijä, ts. $k \mid (bm + a)$ ja $k \mid b$.

Nyt Lemman 1.3 kohdan 6 mukaan $k \mid (1 \cdot (bm + a) + (-m) \cdot b)$ eli $k \mid a$. Siis k on myös lukujen a ja b yhteinen tekijä.

Väite 2: $A_2 \subseteq A_1$. Olkoon k lukujen a ja b yhteinen tekijä, ts. $k \mid a$ ja $k \mid b$. Edelleen Lemman 1.3 kohdan (6) perusteella

$$k \mid (1 \cdot a + m \cdot b)$$

eli $k \mid (bm + a)$. Siis k on lukujen $bm + a$ ja b yhteinen tekijä.

Koska luvuilla $bm + a$ ja b sekä luvuilla a ja b on samat yhteiset tekijät, niillä on myös sama suurin yhteinen tekijä. □

Esimerkki 1.17. Lemman 1.16 mukaan siis

$$\mathrm{syt}(a,b) = \mathrm{syt}(bm+a,b).$$

Erityisesti saadaan $\mathrm{syt}(a,b) = \mathrm{syt}(a-b,b)$, kun valitaan $m=-1$. Tämän avulla voimme etsiä lukujen 161 ja 203 suurimman yhteisen tekijän:

$$\begin{aligned}
\mathrm{syt}(203,161) &= \mathrm{syt}(203{-}161,161) = \mathrm{syt}(42,161) = \mathrm{syt}(161,42)\\
&= \mathrm{syt}(161{-}42,42) = \mathrm{syt}(119,42)\\
&= \mathrm{syt}(119{-}42,42) = \mathrm{syt}(77,42)\\
&= \mathrm{syt}(77{-}42,42) = \mathrm{syt}(35,42) = \mathrm{syt}(42,35)\\
&= \mathrm{syt}(42{-}35,35) = \mathrm{syt}(7,35) = 7.
\end{aligned}$$

Saman tuloksen saa toki nopeamminkin: Lemman 1.16 mukaan esimerkiksi

$$\mathrm{syt}(161,42) = \mathrm{syt}(161{-}4{\cdot}42,42) = \mathrm{syt}(-7,42) = 7.$$

Tehtävä. Laske samaan tapaan lukujen 353 ja 153 suurin yhteinen tekijä.

Lause 1.18 (Eukleideen algoritmi). *Olkoot a ja b positiivisia kokonaislukuja ja olkoon $a \geq b$. Jos $b \mid a$, niin $\mathrm{syt}(a,b) = b$. Jos $b \nmid a$, sovella toistuvasti jakoyhtälöä:*

$$\begin{aligned}
a &= bq_0 + r_0,\ 0 < r_0 < b\\
b &= r_0q_1 + r_1,\ 0 \leq r_1 < r_0\\
r_0 &= r_1q_2 + r_2,\ 0 \leq r_2 < r_1\\
r_1 &= r_2q_3 + r_3,\ 0 \leq r_3 < r_2,\\
&\vdots
\end{aligned}$$

Prosessi päättyy, kun saadaan jakojäännös $r_{n+1} = 0$. Tämän täytyy tapahtua äärellisellä määrällä askelia, ts. jollekin kokonaisluvulle n on

$$\begin{aligned}
r_{n-2} &= r_{n-1}q_n + r_n,\ 0 < r_n < r_{n-1}\\
r_{n-1} &= r_nq_{n+1} + 0.
\end{aligned}$$

Viimeistä edellinen jakojäännös $r_n = \mathrm{syt}(a,b)$.

Todistus. Kyseisessä prosessissa saadaan aidosti pienenevä jono jakojäännöksiä $r_0 > r_1 > r_2 > \ldots \geq 0$, ja luvut $r_i \in \mathbb{N}$, joten jossakin vaiheessa saadaan $r_{n+1} = 0$.

Jos $b \mid a$, on $a = bq + 0$, joten Lemman 1.16 perusteella $\mathrm{syt}(a,b) = \mathrm{syt}(bq+0,b) = \mathrm{syt}(b,0) = b$.

Jos $b \nmid a$, Lemman 1.16 toistuva soveltaminen osoittaa, että

$$\begin{aligned}
\mathrm{syt}(a,b) &= \mathrm{syt}(bq_0 + r_0, b) = \mathrm{syt}(b, r_0)\\
&= \mathrm{syt}(r_0q_1 + r_1, r_0) = \mathrm{syt}(r_0, r_1)\\
&= \mathrm{syt}(r_1, r_2) = \ldots = \mathrm{syt}(r_{n-2}, r_{n-1})\\
&= \mathrm{syt}(r_{n-1}, r_n) = \mathrm{syt}(r_n, 0) = r_n.
\end{aligned}$$

□

Esimerkki 1.19. Etsitään $\text{syt}(78, 123)$ Eukleideen algoritmilla:

$$\begin{aligned} 123 &= 78{\cdot}1 + 45 \\ 78 &= 45{\cdot}1 + 33 \\ 45 &= 33{\cdot}1 + 12 \\ 33 &= 12{\cdot}2 + 9 \\ 12 &= 9{\cdot}1 + 3 \\ 9 &= 3{\cdot}3 + 0, \end{aligned}$$

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

Esimerkki 1.20. Etsitään luvun $3 = \text{syt}(78, 123)$ esitys lukujen 78 ja 123 lineaarikombinaationa.

Ratkaistaan ensin 3 viimeistä edellisestä yhtälöstä:

$$3 = 12 - 9.$$

Ratkaistaan 9 kolmanneksi viimeisestä yhtälöstä ja sijoitetaan edelliseen:

$$3 = 12 - (33 - 2{\cdot}12) = 3{\cdot}12 - 33.$$

Ratkaistaan 12 kolmannesta yhtälöstä ja sijoitetaan:

$$3 = 3(45{-}33) - 33 = 3{\cdot}45 - 4{\cdot}33,$$

ja 33 toisesta yhtälöstä:

$$3 = 3{\cdot}45 - 4(78{-}45) = 7{\cdot}45 - 4{\cdot}78,$$

ja lopuksi 45 ensimmäisestä yhtälöstä:

$$3 = 7(123{-}78) - 4{\cdot}78 = 7{\cdot}123 - 11{\cdot}78.$$

Tehtävä. Laske lukujen 203 ja 161 suurin yhteinen tekijä Eukleideen algoritmilla ja muodosta vastaava lineaarikombinaatioesitys.

1.2. Lineaarinen Diofantoksen yhtälö

Määritelmä 1.21. *Diofantoksen yhtälö* on yhden tai usean muuttujan yhtälö, jolle etsitään kokonaislukuratkaisuja. Kahden muuttujan *lineaarinen Diofantoksen yhtälö* on muotoa

$$ax + by = c,$$

missä $a, b, c \in \mathbb{Z}$.

Lause 1.22. *Diofantoksen yhtälö $ax + by = c$ on ratkeava, jos ja vain jos* $\text{syt}(a, b) \mid c$.

Todistus. Merkitään $\text{syt}(a,b) = d$. Oletetaan, että $ax + by = c$ on ratkeava. Koska $d \mid a$ ja $d \mid b$, niin $d \mid ax + by$ eli $d \mid c$. Siis $\text{syt}(a,b) \mid c$. Oletetaan käänteisesti, että $\text{syt}(a,b) \mid c$ eli $d \mid c$. Lauseen 1.10 mukaan on olemassa sellaiset kokonaisluvut u ja v, että

$$d = au + bv.$$

Toisaalta, on olemassa sellainen e, että $de = c$. Näin ollen

$$a(ue) + b(ve) = c,$$

joten yhtälö $ax + by = c$ on ratkeava. □

Huomautus. Yllä oleva lause antaa menetelmän, jolla voidaan tarkistaa, onko yhtälö $ax + by = c$ ratkeava. Seuraava lause antaa menetelmän, jolla ratkaisut saadaan.

Lause 1.23. *Olkoot a, b ja c kokonaislukuja. Merkitään $\text{syt}(a,b) = d$. Jos yhtälö $ax + by = c$ on ratkeava, niin yhtälön kaikki ratkaisut ovat*

$$\begin{cases} x = x_0 + \dfrac{bt}{d}, \\ y = y_0 - \dfrac{at}{d}, \end{cases} \quad t \in \mathbb{Z}, \tag{1.2}$$

missä x_0, y_0 on yksi ratkaisu.

Todistus. Kyseessä olevat lukuparit ovat ratkaisuja, sillä

$$a(x_0 + \frac{bt}{d}) + b(y_0 - \frac{at}{d}) = ax_0 + by_0 = c.$$

Todistetaan, että näin saadaan kaikki ratkaisut. Olkoon x, y mielivaltainen ratkaisu. Silloin

$$ax + by = c = ax_0 + by_0,$$

joten

$$a(x - x_0) + b(y - y_0) = 0.$$

Kun jaetaan puolittain luvulla d, saadaan

$$\frac{a}{d}(x - x_0) + \frac{b}{d}(y - y_0) = 0$$

eli

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0). \tag{1.3}$$

Näin ollen

$$\frac{b}{d} \mid \frac{a}{d}(x - x_0).$$

Lemman 1.14 ja Lauseen 1.13 nojalla

$$\frac{b}{d} \mid x - x_0.$$

Siis

$$x - x_0 = \frac{b}{d}t$$

eli

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

Nyt yhtälön 1.3 nojalla

$$\frac{a}{d}\frac{b}{d}t = -\frac{b}{d}(y - y_0),$$

joten

$$y = y_0 - \frac{at}{d}.$$

Siis kaava (1.2) on voimassa. □

Huomautus. Yksittäinen ratkaisu saadaan esimerkiksi kokeilemalla tai Eukleideen algoritmilla.

Esimerkki 1.24. Ratkaise yhtälö $19x + 94y = 1994$.

Esimerkki 1.25. Ratkaise yhtälö $15x + 6y = 199$.

Esimerkki 1.26. Ratkaise yhtälö $52x + 62y = 6$.