Lukuteoria 1 — 20.1.2022

$a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$

$$\text{syt}(a,b) = \max\{\underbrace{d \in \mathbb{N} : d \mid a \text{ ja } d \mid b}_{D}\}.$$

Luvuilla a ja b suurin yhteinen tekijä

Huom: Jos $a = 0 = b$, niin $d \mid a^{=0}$ ja $d \mid b^{=0}$ $\forall\, d \in \mathbb{N}$ $\Rightarrow D = \mathbb{N}$ ja $\mathbb{N}$:llä ei ole suurinta alkiota.

$$\text{L. 1.3:} \quad \left.\begin{array}{l} d \mid a \Rightarrow d \leq |a| \\ d \mid b \Rightarrow d \leq |b| \end{array}\right\} \Rightarrow \quad d \leq \max\{|a|, |b|\}.$$

Huom. $D \neq \emptyset$ koska $\left.\begin{array}{l} 1 \cdot a = a \\ 1 \cdot b = b \end{array}\right\} \Rightarrow 1 \in D.$

Huom. $d \mid a \Leftrightarrow d \mid -a \Leftrightarrow -a = cd \Rightarrow a = -1 \cdot c \cdot d \Rightarrow d \mid a$

$\Uparrow$

$a = bd \Rightarrow -a = -1 \cdot b \cdot d \Rightarrow d \mid -a$

$\Rightarrow \text{syt}(a,b) = \text{syt}(-a,b) = \text{syt}(-a,-b) = \text{syt}(a,-b)$

Esim. $n \in \mathbb{N}$ $\quad \text{syt}(n, n+1) = 1$.

Jos $d \mid n$ ja $d \mid n+1$, niin L.1.3 $\Rightarrow$ $d \mid \underbrace{(n+1) - n}_{=1}$ $\overset{\text{L.1.3}}{\Rightarrow}$ $|d| \leq 1 \Rightarrow d = \pm 1$.

Bézout'n yhtälö

Lause 2.4 Olk. $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. Olk.

$$J = \{ xa + yb : x, y \in \mathbb{Z} \} \cap (\mathbb{N} - \{0\}).$$

Tällöin $\text{syt}(a,b) = \min J$ = joukon J pienin alkio.

Tod. Ainakin yksi luvuista $\pm a, \pm b$ on positiivinen. $\Rightarrow J \neq \emptyset$.

Hyvän järj. periaate $\Rightarrow$ joukossa J on pienin alkio $g \in J$

Os. ensin, että $g \mid a$ ja $g \mid b$. Jos $g \nmid a$, niin ja luvuille:

$$\exists r, q \in \mathbb{Z},\ 0 < r < g : \quad a = gq + r.$$

$g \in J \rightarrow g = x_0 a + y_0 b$ joillain $x_0, y_0 \in \mathbb{Z}$

$$0 < r = a - gq = a - (x_0 a + y_0 b) q = \underbrace{(1 - x_0 q)}_{\in \mathbb{Z}} a - \underbrace{(y_0 q)}_{\in \mathbb{Z}} b \in J$$

Ristiriita, sillä ol. mukaan g on J:n pienin alkio, jolle pätee myös $g \leq r$, siis $g \mid a$.

Vastaavasti $g \mid b$.

Olk. d a:n ja b:n yhtl. jakaja: $d \mid a$ ja $d \mid b$

$$g = x_0 a + y_0 b \Rightarrow d \mid g \overset{2.1.3(3)}{\Rightarrow} |d| \leq g.$$ Siis $g = \mathrm{syt}(a,b)$. □

Seuraus (Bézoutin yhtälö) Olk. $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. Tällöin on $x_0, y_0 \in \mathbb{Z}$: $\mathrm{syt}(a,b) = x_0 a + y_0 b$. □

Huom $\mathrm{syt}(2,3) = 1$. $3 - 2 = 1 = -3 + 4$

$\rightsquigarrow$ Kertoimet x_0, y_0 Bézoutin yhtälössä eivät ole 1-käsitteisiä. (2.2)

Seuraus Olk. $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. Tällöin $c \mid a$ ja $c \mid b \Leftrightarrow c \mid \mathrm{syt}(a,b)$

Todi. Jos $c \mid \mathrm{syt}(a,b)$
mutta $\mathrm{syt}(a,b) \mid a$ ja $\mathrm{syt}(a,b) \mid b$ } $\overset{\text{L.1.3}}{\Rightarrow}$ (trans.) $c \mid a$ ja $c \mid b$.

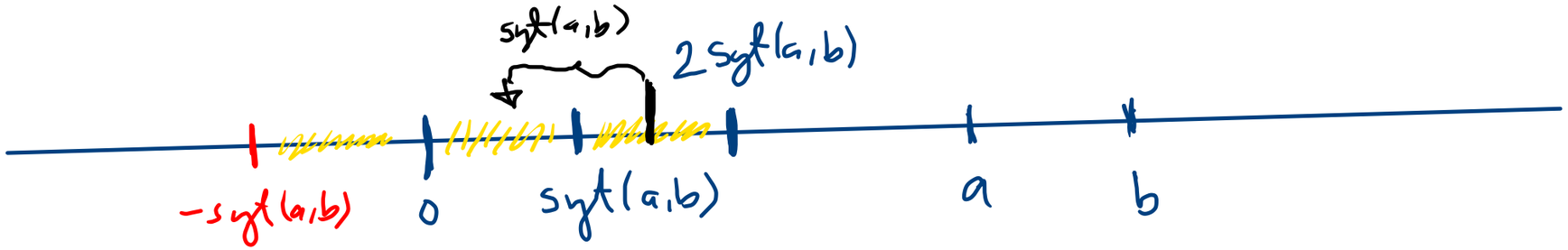
Jos $c \mid a$ ja $c \mid b$, niin L. 1.3 nojalla $c \mid xa+yb \quad \forall\, x,y \in \mathbb{Z}$ $\Rightarrow c \mid \mathrm{syt}(a,b)$.

Bézout: $\mathrm{syt}(a,b) = x_0 a + y_0 b$ jollain $x_0, y_0 \in \mathbb{Z}$

□

Lause 2.7. $a, b, c \in \mathbb{Z}$, $(a,b) \neq (0,0)$. Tällöin

$c = ka + lb$ jollain $k, l \in \mathbb{Z}$ $\Leftrightarrow$ $\mathrm{syt}(a,b) \mid c$



Tod. "$\Rightarrow$" $\mathrm{syt}(a,b) \mid a$, $\mathrm{syt}(a,b) \mid b$ $\overset{\text{L. 1.3}}{\Rightarrow}$ $\mathrm{syt}(a,b) \mid ka+lb$.

"$\Leftarrow$" Jos $\mathrm{syt}(a,b) \mid c$ $\Rightarrow$ $c = k\,\mathrm{syt}(a,b) = k(x_0 a + y_0 b) = \underline{(kx_0)a + (ky_0)b}$

Bézout ||

$x_0 a + y_0 b$

□

Seuraus Olk. $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. Lineaarinen Diofantoksen yhtälö

Yhtälöllä $ax + by = c$ on kokonaisluku-ratkaisuja $\Leftrightarrow$ $\mathrm{syt}(a,b) \mid c$.

Esim. yhtälöllä $6x + 21y = c$ on kokonaislukuratkaisuja $\iff 3 \mid c$

$\iff c = 3k$ jollain $k \in \mathbb{Z}$.

6:n tekijät $\pm 1, \pm 2, \pm 3, \pm 6$

21 — " — $\pm 1, \pm 3, \pm 7, \pm 21$

$\Rightarrow \operatorname{syt}(6, 21) = 3$

Esim $3 = 6 \cdot (-3) + 21 \cdot 1$ siis $(x, y) = (-3, 1)$ on lin. Diof.

yhtälön $6x + 21y = 3$ ratkaisu.

Lause 2.11 Olk. $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$, $c \in \mathbb{N} - \{0\}$. Tällöin

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

Tod. L. 2.4 : $\operatorname{syt}(a, b) = \min \{ xa + yb : x, y \in \mathbb{Z} \} \cap (\mathbb{N} - \{0\})$.

$$\operatorname{syt}(ca, cb) = \min \{ \underbrace{x(ca) + y(cb)}_{c(xa+yb)} : x, y \in \mathbb{Z} \} \cap (\mathbb{N} - \{0\})$$

$c > 0$

Huom: c:llä kertominen ei muuta järjestystä.

$$= c \min \{ xa + yb : x, y \in \mathbb{Z} \} \cap (\mathbb{N} - \{0\}) = c \operatorname{syt}(a, b).$$

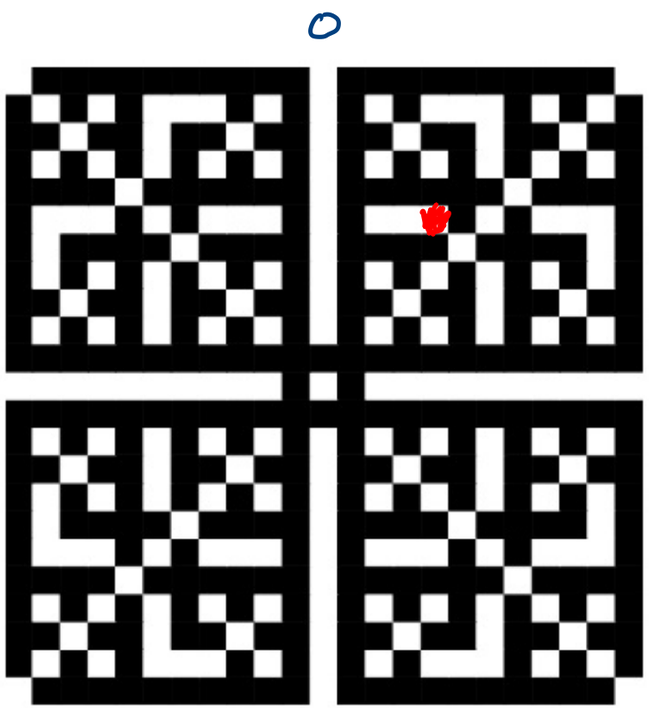
□

Seuraus Jos $d \mid a$ ja $d \mid b$, niin $\operatorname{syt}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\operatorname{syt}(a,b)}{d}$

Erityisesti $\operatorname{syt}\left(\frac{a}{\operatorname{syt}(a,b)}, \frac{b}{\operatorname{syt}(a,b)}\right) = 1.$

Tod. **Harj.** (Käyttää L. 2. 11.)

Määr. Jos $\operatorname{syt}(a,b) = 1$, niin { a ja b ovat suhteellisia alkulukuja. / keskenään jaottomia. } (a,b) on suhteellinen alkulukupari.



$\bullet = (4,6)$
$\operatorname{syt}(4,6) = 2$

$-11 \leq a, b \leq 11.$
Kuvassa suht. alkulukuparit mustalla.