Lukuteoria 1 — 25.1.2022

$\mathrm{syt}(a,b)$ on lukujen a ja b suurin yhteinen tekijä: Jos $d \in \mathbb{N}-\{0\}$ ja $d \mid a$ ja $d \mid b$, niin $d \le \mathrm{syt}(a,b)$

$\mathrm{syt}(a,b) \mid a$ ja $\mathrm{syt}(a,b) \mid b$.

Bézout: $\mathrm{syt}(a,b) = x_0 a + y_0 b$ joillain $x_0, y_0 \in \mathbb{Z}$, $\mathrm{syt}(a,b)$ on pienin pos. kokonaisluku, joka void. kirj. tässä muodossa.

$$\{ xa + yb : x, y \in \mathbb{Z} \} = \{ k \,\mathrm{syt}(a,b) : k \in \mathbb{Z} \}.$$

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

$\Leftrightarrow 1 = x_0 a + y_0 b$ joillain $x_0, y_0 \in \mathbb{Z}$.

Seuraus 2.14 Olk. $a, b, c \in \mathbb{Z}$, $\mathrm{syt}(a,b) = 1$.

1) Jos $a \mid c$ ja $b \mid c$, niin $ab \mid c$

2) Jos $a \mid bc$, niin $a \mid c$ (GAUSSIN LEMMA)

$2 = a = b = c$.

Hm-m. $2 \mid 2$
mutta $2 \cdot 2 = 4 \nmid 2$
$\mathrm{syt}(2,2) = 2$

Tod. Bézout : $\exists\ x_0, y_0 \in \mathbb{Z}$: $1 = x_0 a + y_0 b$.

$\Rightarrow$ $c = x_0 ac + y_0 bc$ $\circledast$

1) dclus : $a \mid c \Rightarrow c = ka$
$b \mid c \Rightarrow c = \ell b$ joillain $k, \ell \in \mathbb{Z}$.

$\circledast \Rightarrow c = x_0 ac + y_0 bc = x_0 \ell ab + y_0 k ab = \underbrace{(x_0 \ell + y_0 k)}_{\in \mathbb{Z}} ab$

$= \ell b$ $= ka$

$\Rightarrow ab \mid c$. $\square$

2) Vaite : $a \mid bc \Rightarrow a \mid c$ L.1.3(3) $\Rightarrow a \mid c$. $\square$

$\circledast$: $c = x_0 c a + y_0 bc$

$a \mid a$ $a \mid bc$

Lause 2.15 olk. $a, b, m \in \mathbb{Z}$, $\mathrm{pgcd}(a, m) = 1 = \mathrm{pgcd}(b, m)$. Talloin $\mathrm{pgcd}(ab, m) = 1$.

Tod. Bézout : $\underbrace{xa + ym = 1}_{xa = 1 - ym} = \underbrace{zb + wm}_{zb = 1 - wm}$ joillain $x, y, z, w \in \mathbb{Z}$.

② $\Rightarrow (xa)(zb) = (1 - ym)(1 - wm) = 1 - wm - ym + (ywm)m = 1 + (ywm - w - y)m$

$\Rightarrow 1 = \underbrace{(xz)}_{\in \mathbb{Z}}(ab) + (w + y - ywm)m$.

$\in \mathbb{Z}$

Bézout : $\mathrm{pgcd}(ab, m) = 1$ $\square$

Miten $\mathrm{syt}(a,b)$ voidaan laskea?

(vrt. jakoyhtälö!)

Tärkeä lemma: Jos $a = qb + r$ (⊛), niin $\mathrm{syt}(a,b) = \mathrm{syt}(b,r)$.

Tod. Jos $d \mid b$, $d \mid r$ $\overset{\text{L.1.3(3)}}{\Rightarrow}$ $d \mid a$ $\Rightarrow$ $\mathrm{syt}(b,r) \mid a$, $\mathrm{syt}(b,r) \mid b$

Jos $e \mid a$, $e \mid b$ $\overset{\text{L.1.3(3)}}{\Rightarrow}$ $e \mid r$ $\Rightarrow$ $\mathrm{syt}(a,b) \mid r$, $\mathrm{syt}(a,b) \mid b$

$\Rightarrow \mathrm{syt}(a,b) = \mathrm{syA}(b,r)$. □

Esim. $\mathrm{syt}(56,32) = ?$

jakoyht: $56 = 1 \cdot 32 + 24$ $\quad (0 \le 24 < 32)$

-11- $32 = 1 \cdot 24 + 8$ $\quad 0 \le 8 < 24$

$8 \mid 24 \Rightarrow \mathrm{syt}(8,24) = 8$

Lemma: $8 = \mathrm{syt}(8,24) = \mathrm{syt}(32,24) = \mathrm{syt}(56,32)$.

Euklideen algoritmi.

$1 \leq b < a$

Jakoyhtälö: $\exists\, q_1, r_1 \in \mathbb{Z}$, $0 \leq r_1 < b$ s.e. $a = q_1 b + r_1$.

Jos $r_1 = 0$, niin $b \mid a \Rightarrow syt(a,b) = b$.

Jos $r_1 > 0$, niin toistetaan:

Jakoyhtälö $\exists\, q_2, r_2 \in \mathbb{Z}$, $0 \leq r_2 < r_1$ s.e. $b = q_2 r_1 + r_2$

Jos $r_2 = 0$, niin $r_1 \mid b \Rightarrow syt(r_1, b) = r_1$

$\parallel$

$syt(a,b)$

Jos $r_2 > 0$, niin toistetaan

Jakoyhtälö: $\exists\, q_3, r_3 \in \mathbb{Z}$: $0 \leq r_3 < r_2$ $\quad r_1 = q_3 r_2 + r_3$

Jos $r_3 = 0$, niin $r_2 \mid r_1 \Rightarrow syt(r_2, r_1) = r_2$

$\parallel$

$syt(r_1, b) = syt(a,b)$

jne.

Huom. $b > r_1 > r_2 > r_3 \rightsquigarrow$ algoritmi pysähtyy viimeistään kun $r_b = 0$

Lause. syt(a,b) on Eukleideen algoritmin viimeinen positiivinen jakojäännös.

Esim. syt(78, 267)

$267 = 3 \cdot 78 + 33 \iff 33 = 267 - 3 \cdot 78$

$78 = 2 \cdot 33 + 12 \iff 12 = 78 - 2 \cdot 33$

$33 = 2 \cdot 12 + 9 \iff 9 = 33 - 2 \cdot 12$

$12 = 1 \cdot 9 + 3$ — Eukl. alg: syt(78, 267) = 3

$9 = 3 \cdot 3$

syt(78,267) = 3

$3 = 12 - 9 = 12 - (33 - 2 \cdot 12) = 3 \cdot 12 - 33 = 3(78 - 2 \cdot 33) - 33$

$= 3 \cdot 78 - 7 \cdot 33 = 3 \cdot 78 - 7(267 - 3 \cdot 78) = 24 \cdot 78 - 7 \cdot 267$

⇝ Kun syt(a,b) määritetään Eukl. algoritmilla, niin peruuttamalla saadaan Bézout'n yhtälö syt(a,b):lle.

3 Alkuluvut

Määr. Luonn. luku $p > 1$ on **alkuluku**, jos sen { tekijät ovat ± 1 ja $\pm p$. / pos. tekijät ovat 1 ja p.

Jos $q \in \mathbb{N} - \{0, 1\}$ ja q ei ole alkuluku, niin q on **yhdistetty luku**.

Jos p on alkuluku, $a \in \mathbb{Z} - \{0\}$ ja $p \mid a$, niin p on luvun a { **alkutekijä** / **alkuluvun tekijä** }.

Huom. 1) 1 { ei ole alkuluku / ei ole yhd. luku }.

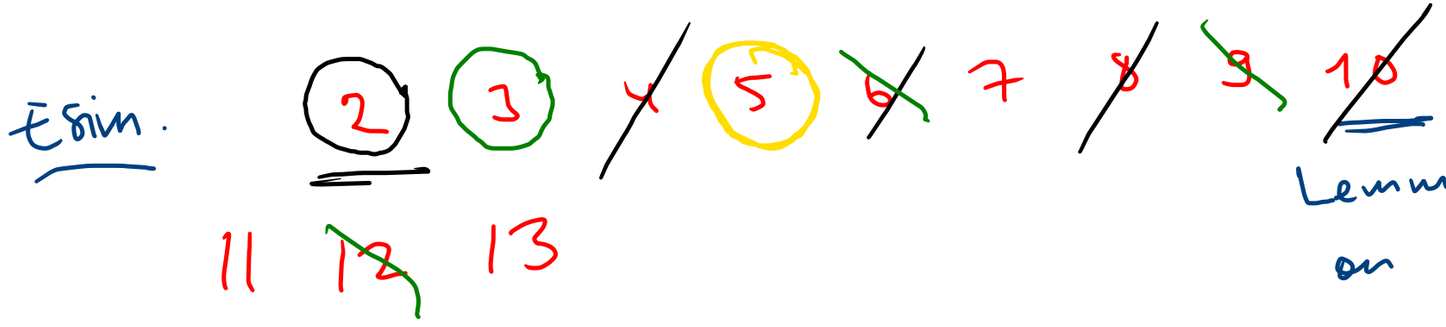
2) 2 on alkuluku, sillä 2:n tekijät ovat $\pm 1, \pm 2$.
Muut parilliset luvut eivät ole alkulukuja: jos $a \in \mathbb{N}$, $a > 2$ ja $2 \mid a$, niin a:n tekijöitä ovat ainakin $1, 2$ ja $a \neq \pm 2 \neq \pm 1$
$\rightsquigarrow$ lukua tekijöitä!

3) Olk. p, q alkuluku, $p \neq q$. Tällöin $syt(p,q) = 1$.

Tod. p:n pos. tekijät $= 1, p$
q:n pos. tekijät $= 1, q$
$\Rightarrow$ ainoa pos. yht. tekijä on 1
$\Rightarrow syt(p,q) = 1$.

Lemma 3.3. Olk. $n \in \mathbb{N} - \{0,1\}$. Tällöin n on yhd. luku
$\Leftrightarrow \exists$ p alkuluku, $p \leq \sqrt{n}$ s.e $p \mid n$.

Esim.



Lemma: Jos 10 yhd. luku, niin on alkuluku $p \leq 3$ s.e. $p \mid 10$