Lukuteoria 1 13.1.2022

Määr. $m, n \in \mathbb{Z}$. n jaollinen m:llä / m jakaa luvun n, jos $\exists k \in \mathbb{Z}$: $n = km = mk$.

$m \mid n$.

Jos $q_1 b + r_1 = a = q_2 b + r_2$ ja $0 \le r_1, r_2 < |b|$, niin $\underbrace{q_1 = q_2 \text{ ja } r_1 = r_2}$

Lause 1.6. (Jakoyhtälö) Olk. $a, b \in \mathbb{Z}$, $b \neq 0$. Tällöin on 1-käsitteiset $q, r \in \mathbb{Z}$,

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

Esim. 1) $b = 2$. Jakoyhtälö: Jos $a \in \mathbb{Z}$, niin $\overbrace{a = 2q}^{a \text{ parillinen}}$ jollain $q \in \mathbb{Z}$

tai $\underbrace{a = 2q + 1}_{a \text{ on pariton.}}$ — " —

Tämä jakoyhtälön erikoistapaus: Jokainen kokonaisluku on parillinen tai pariton.

2) $b = 3$. Jos $a \in \mathbb{Z}$, niin $a = \begin{cases} 3q + 0 \\ 3q + 1 \\ 3q + 2 \end{cases}$ jollain $q \in \mathbb{Z}$.

3) $\underline{b=4}$. $n \in \mathbb{Z} \Rightarrow n = 4q + r$ joillakin $q \in \mathbb{Z}$, $r \in \{0,1,2,3\}$.

$$n^2 = (4q+r)^2 = \underbrace{16q^2}_{} + \underbrace{8qr}_{} + r^2 = 4N + r^2 = \begin{cases} 4N & \text{, jos } r=0 \\ 4N+1 & \text{, jos } r=1 \\ 4(N+1) & \text{, jos } r=2 \\ 4(N+2)+1 & \text{, jos } r=3. \end{cases}$$

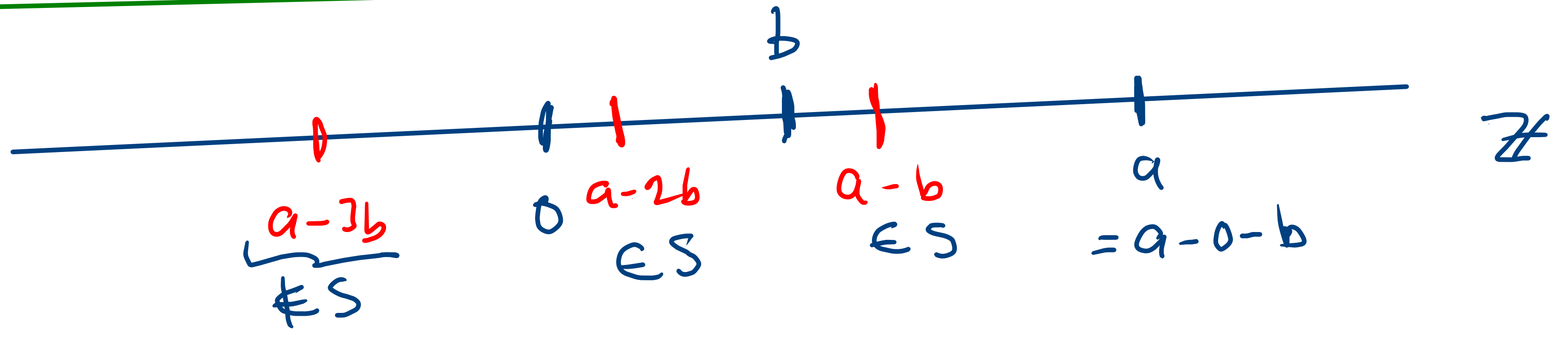
L. 13: nämä 4:llä jaollisia.

$0^2 = 0$
$1^2 = 1$
$2^2 = 4$
$3^2 = 9 = 2 \cdot 4 + 1$

Tulos: Kokonaisluvun neliön jakojäännös 4:llä jaettuna on 0 tai 1.

Jakoyhtälön todistus. Osoitetaan ensin, että väitteen mukaisia lukuja q ja r on.

$$S = \{ y \in \mathbb{N} : y = a - qb, \ q \in \mathbb{Z} \}$$



$a, b > 0$

Huom: $a = \underset{q}{2}b + \underbrace{a-2b}_{r}$

Os. että joukolla S on pienin alkio.

Miksi pienin alkio on mielenkiintoinen? Koska pienin alkio on haluttu jakojäännös.

Jos $r \in S$ on joukon S pienin alkio, niin

- $r = a - qb$ jollain $q \in \mathbb{Z}$ $\Rightarrow$ $\underline{\underline{a}} = qb + (a - qb) = \underline{\underline{qb + r}}$
- Ol. $b > 0$ ja $r \geq b$. Tällöin

$$a - (q+1)b = \underbrace{a - qb}_{r} - b = r - b \geq 0 \Rightarrow a - (q+1)b \in S$$

Mutta $a - (q+1)b < a - qb$. Siis r ei olekaan pienin alkio joukon S

Siis täytyy olla $r < b$.

$\Rightarrow$ r on haluttu jakojäännös.

Tapaus $b < 0$ käsitellään samaan tapaan.

Os. siis, että joukossa S on pienin alkio.

$m \in S$ on pienin, jos $m \leq s$ $\forall$ $s \in S$.

Hyvän järjestyksen periaate: Jos $A \subset \mathbb{N}$, $A \neq \emptyset$, niin joukossa A on pienin alkio.

Tämä seuraa induktioperiaatteesta.

$\Rightarrow$ Riittää osoittaa, että $S \neq \emptyset$.

Uskomme tämän. (ks. kurssimateriaali)
Jos $A \neq \emptyset$, niin on $a \in A$. Joukossa $A^{o} = \{ b \in A : b \leq a \}$ on äärellinen määrä alkioita. Yksi näistä pienin.

Os. ~~että~~ $S = \{ y \in \mathbb{N} : y = a - qb ,\ q \in \mathbb{Z} \}$.

1) Jos $a \geq 0$, niin $a = a - 0 \cdot b \in S \Rightarrow S \neq \emptyset$.

2) Jos $a < 0$ ja $b > 0$, $b \geq 1$, niin $a - ab = \underbrace{a}_{<0}(\underbrace{1-b}_{\leq 0}) \geq 0 \Rightarrow a - ab \in S$
$\Rightarrow S \neq \emptyset$.

3) Jos $a < 0$ ja $b < 0$, $b \leq -1$, niin $a + ab \in S \Rightarrow S \neq \emptyset$.

$\Rightarrow$ Jakoyhtälön lukuja q, r on.

Os. ~~että~~ ne ovat 1-käsitteiset. Ol. ~~että~~ $q_1 b + r_1 = a = q_2 b + r_2$
ja $0 \leq r_1, r_2 < |b|$.

$\Rightarrow (q_1 - q_2) b = q_1 b - q_2 b = r_2 - r_1$. Siis $b \mid r_2 - r_1$.

Jos $q_1 \neq q_2$, niin $|q_1 - q_2| \geq 1 \Rightarrow |r_2 - r_1| = |(q_1 - q_2) b| = \underbrace{|q_1 - q_2|}_{\geq 1} |b| \geq |b|$

Tämä on mahdotonta, koska $0 \leq r_1, r_2 < |b| \Rightarrow |r_1 - r_2| < |b|$
$\Rightarrow |r_1 - r_2| \leq |b| - 1$.

Siis $\underline{q_1 = q_2} \Rightarrow q_1 - q_2 = 0$
$\Rightarrow r_2 - r_1 = 0 \cdot b = 0 \Rightarrow \underline{r_1 = r_2}$. $\square$

Varoitus: Hyvän järjestyksen periaate ei päde kokonaislukujen joukolle:

$\mathbb{Z} \subset \mathbb{Z}$, $\mathbb{Z} \neq \emptyset$. Mutta $\mathbb{Z}$:ssa ei ole pienintä alkiota.

1.3 Lukujärjestelmät

Lause 1.8 Olk. $n, k \in \mathbb{N} - \{0\}$ (kantaluku k), $k \geq 2$. Tällöin on 1-käs. $s \in \mathbb{N}$, $a_0, \dots, a_s \in \mathbb{Z}$, $0 \leq a_0, \dots, a_s < k$, joille pätee

$$n = a_0 + a_1 k + a_2 k^2 + \dots + \underbrace{a_s}_{\neq 0} k^s$$

Esim. $k = 10 \leadsto n = a_0 + a_1 \cdot 10 + a_2 \underbrace{10^2}_{100} + \dots + a_s 10^s$

$$\overset{\text{merkintä}}{=} (a_s \cdots a_2 a_1 a_0)_{10} = a_s a_{s-1} \cdots a_2 a_1$$

10-järjestelmä. $\leadsto \underbrace{-n}_{<0} = -a_s a_{s-1} \cdots a_2 a_1$

5

$\underline{k=2}$ $\leadsto$ 2-järjestelmä binaariluvut.

$$n = \underbrace{a_0}_{= a_0 2^0} + a_1 \cdot 2 + a_2 2^2 + \dots + a_s 2^s = \sum_{j=0}^{s} a_j 2^j \underset{\text{merkintä}}{=} (a_s \cdots a_0)_2$$

$a_0, \dots, a_s \in \{0, 1\}$.

<u>Esim.</u> 1) $175 = 5 + 7 \cdot 10 + 1 \cdot 10^2$

2) binaariluku $10011_2 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 = 1_{10} + 2_{10} + 0 + 0 + 16_{10} = 19_{10}$

<u>Ratkomo</u> to 14 – 18

ma

ti