Lukuteoria 1 11.1.2022

Luennot ti ja to 7 vk.
Harjoitusvastaanotto ke klo 14.

Harjoituksista kyvitystä max 5p.
Koe 30p.

Läpäisy 15 p.

Harj. pal. tiistaina klo 18 mennessä sähköpostilla.
tehtävät jaossa torstaina
ratkaisuja kotisivulle ti klo 18 jälkeen.

Sisältö
- $\mathbb{N}$, $\mathbb{Z}$, jaollisuus ~~>~~ induktio jälkeyhtälö
- lukujärjestelmiä 10-järj. 2-järj. jne.
- jaollisuussääntöjä
- suurin yhteinen tekijä, Euklideen algoritmi
- alkuluku ja $2, 3, 5, 7, 11, 13, \ldots$
- kongruenssi. $a, b \in \mathbb{Z}$. $a \equiv b \bmod q \Leftrightarrow b = a + kq$ jollain $k \in \mathbb{Z}$.
  $q \in \mathbb{Z}, q \geq 2$

$ax \equiv b \bmod q$.

1 Jaollisuus.

Merkintöjä. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ **kokonaisluvut**

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ **luonnolliset luvut**

Huom. joissain kirjoissa / joillain kursseilla valitaan $\mathbb{N} = \{1, 2, 3, \dots\}$.

$\mathbb{Z}$:ssa ja $\mathbb{N}$:ssä laskutoimitukset $+, \cdot$

järjestys $\leq, <$:

$a \leq b \iff b = a + c$ jollain $c \in \mathbb{N}$

$a < b \iff b = a + c$ jollain $c \in \mathbb{N} - \{0\}$.

Induktioperiaate. Olk. $Q \subset \mathbb{N}$ s.e. $0 \in Q$ ja kaikille $k \in Q$ pätee $k+1 \in Q$. Tällöin $Q = \mathbb{N}$. (Aksiooma)

$Q = \{0, 1, 2, \dots\} = \mathbb{N}$.

Määr. Olk. $m, n \in \mathbb{Z}$. n on **jaollinen** m:llä, jos $n = km$ jollain $k \in \mathbb{Z}$.

Tällöin m on n:n **tekijä** tai **jakaja**, m **jakaa** luvun n.

Jos m ei jaa lukua n, merk. $m \nmid n$.

$m \mid n$.

Esim. 1) Jos $n \in \mathbb{Z}$, niin $1 \mid n$, sillä $n = n \cdot 1$
$n \mid n$, sillä $n = 1 \cdot n$

2) $2 \mid 6$, sillä $6 = 3 \cdot 2$
$3 \mid 6$
$-2 \mid 6$
$6 = (-3)(-2)$

$\rightsquigarrow$ Luvun 6 tekijät ovat $\pm 1, \pm 2, \pm 3, \pm 6$

Lause 1.3 Olk. $n, m, a, b, d \in \mathbb{Z}$. Tällöin

1) $n \mid n$ (refleksiivisyys) ok.
2) jos $d \mid n$ ja $n \mid m$, niin $d \mid m$ (transitiivisuus) ok
3) jos $d \mid n$ ja $d \mid m$, niin $d \mid (an + bm)$ (lineaarisuus)
4) jos $d \mid n$, niin $ad \mid an$.
5) jos $ad \mid an$, niin $d \mid n$. ok
ja $a \neq 0$
6) $1 \mid n$ ok
7) $n \mid 0$
8) jos $0 \mid n$, niin $n = 0$

Tod
2) $d \mid n \Rightarrow n = dk_1$ jollain $k_1 \in \mathbb{Z}$
$m \mid n \Rightarrow m = nk_2$ — " — $k_2 \in \mathbb{Z}$
Siis $m = nk_2 = (dk_1)k_2 = d(\underbrace{k_1 k_2}_{\in \mathbb{Z}})$,
joten $d \mid m$. □

5) $ad \mid an \Rightarrow an = adk$ jollain $k \in \mathbb{Z}$
$\overset{a \neq 0}{\Rightarrow} n = dk \Leftrightarrow d \mid n$.

9) Jos $d \mid n$, niin $|d| \leq |n|$
ja $n \neq 0$

10) Jos $d \mid n$ ja $n \mid d$, niin $d = \pm n$

$|d| = |n|$

Tod. 9) $d \mid n \Rightarrow n = kd$ jollain $k \in \mathbb{Z}$.

$n \neq 0 \overset{8)}{\Rightarrow} d \neq 0$

$k \neq 0$

$\Rightarrow k \geq 1$

$|n| = |kd| = \underbrace{|k|}_{\geq 1} |d| \geq |d|$

Loput harjoituksissa.

Esim. $0 \mid k$. $k \in \mathbb{Z}$ s.e. $3 \mid k$. Tällöin $3 \mid (k^2 + k + 9)$:

$9 = 3 \cdot 3 \Rightarrow 3 \mid 9$

$3 \mid k \overset{3)}{\Rightarrow} 3 \mid k \cdot k = k^2$

$3) \Rightarrow 3 \mid k^2 + k$ $\quad (n = m = k,\ a = k,\ b = 1)$

$3) \Rightarrow 3 \mid (k^2 + k) + 9$.

Torstaina: Jakoyhtälö $0 \mid k$. $a, b \in \mathbb{Z}$, $b \neq 0$. Tällöin on 1-käsitteiset $q, r \in \mathbb{Z}$. joille $a = qb + r$ ja $0 \leq r < |b|$