# 1 Jaguvus

**1.1** Olgu $a, b \in \mathbb{Z}, a \neq 0$. Siis leidub ülimalt üks $x \in \mathbb{Z}$, nii et $ax = b$ (ehk $xa = b$).

Olgu $a, b \in \mathbb{Z}$, $a \neq 0$. Arvu $x \in \mathbb{Z}$, mis rahuldab tingimust $ax = b$ (ehk $xa = b$), nimetatakse $b$ ja $a$ **suhteks** ja tähistatakse $\frac{b}{a}$ ehk $b/a$ ehk $b : a$.

Suhte leidmine on niisiis osaline tehe täisarvudel, mis on täisarvude korrutamise pöördtehteks. Seda tehet nimetatakse ka **jagamiseks** ja suhet sellest tulenevalt **jagatiseks**. Jagamist tähistavate märkide / ja : prioriteet loetakse võrdseks korrutusmärgi · prioriteediga. Märgi — kasutamise puhul väärtustatakse kõigepealt tema kohal ja all olevad avaldised ja seejärel leitakse suhe.

Olgu $a, b \in \mathbb{Z}$. Kui leidub selline $d \in \mathbb{Z}$, et $ad = b$, siis öeldakse, et arv $a$ **jagab** arvu $b$ ehk arv $b$ **jagub** arvuga $a$, ja kirjutatakse vastavalt $a \mid b$ ehk $b \vdots a$; samuti nimetatakse arvu $a$ arvu $b$ **jagajaks** ning arvu $b$ arvu $a$ **kordseks**.

Olgu $n, m \in \mathbb{N}$. Arvu $n$ nimetatakse arvu $m$ **pärisjagajaks**, kui $n$ on $m$ jagaja ja $n \neq m$.

**1.2** Olgu $a, b \in \mathbb{Z}$, $a \neq 0$. Siis $a \mid b$ (ehk $b \vdots a$) parajasti siis, kui leidub $b$ ja $a$ suhe täisarvudes.

**1.3** Olgu $n, m \in \mathbb{N}$, $n \neq 0$. Siis $n$ on $m$ pärisjagaja parajasti siis, kui mingi 1-st erinev naturaalarv on $m$ ja $n$ suhteks.

**1.4** Olgu $a, b, c \in \mathbb{Z}$, $a, b \neq 0$. Kui $a \mid c$, siis $\frac{c}{a} = b$ parajasti siis, kui $b \mid c$ ja $\frac{c}{b} = a$.

**1.5** Olgu $a, b \in \mathbb{Z}$, $a \neq 0$. Kui $a \mid b$, siis $\frac{b}{a} \mid b$.

**1.6** Olgu $a, b \in \mathbb{Z}$.

a) $a \mid b$ parajasti siis, kui $|a| \mid |b|$.

b) Nende tingimuste kehtimise korral kui lisaks $a \neq 0$, siis $\left|\frac{b}{a}\right| = \frac{|b|}{|a|}$.

**1.7** Olgu $a \in \mathbb{Z}$. Siis $a \mid 0$ ja kui $a \neq 0$, siis $\frac{0}{a} = 0$.

**1.8** Olgu $a \in \mathbb{Z}$. Siis $0 \mid a$ parajasti siis, kui $a = 0$.

**1.9** Olgu $a, b \in \mathbb{Z}$, $a \neq 0$. Siis $\frac{b}{a} = 0$ parajasti siis, kui $b = 0$.

**1.10** Olgu $a \in \mathbb{Z}$.

a) $1 \mid a$ ja $\frac{a}{1} = a$.

b) $a \mid a$ ja kui $a \neq 0$, siis $\frac{a}{a} = 1$. Niisiis jaguvusseos on refleksiivne.

**1.11** Olgu $n \in \mathbb{N}$. Siis $n \mid 1$ parajasti siis, kui $n = 1$.



**1.12** Olgu $a \in \mathbb{Z}$. Siis $a \mid 1$ parajasti siis, kui $|a| = 1$.

**1.13** Olgu $a, b, c \in \mathbb{Z}$. Kui $a \mid b$ ja $b \mid c$, siis $a \mid c$. Teisi sõnu, jaguvusseos on transitiivne.

**1.14** Olgu $n, m \in \mathbb{N}$. Kui $n \mid m$ ja $m \mid n$, siis $n = m$. Teisi sõnu, jaguvusseos naturaalarvudel on antisümmeetriline.

**1.15** Olgu $a, b \in \mathbb{Z}$. Kui $a \mid b$ ja $b \mid a$, siis $|a| = |b|$.

**1.16** Olgu $a_1, \ldots, a_l, b \in \mathbb{Z}$.

a) Kui $a_1 \ldots a_l \mid b$, siis iga $i = 1, \ldots, l$ korral $a_i \mid b$.

b) Kui mingi $i = 1, \ldots, l$ korral $b \mid a_i$, siis $b \mid a_1 \ldots a_l$.

**1.17** Olgu $a, b, c \in \mathbb{Z}$, $c \neq 0$.

a) $ac \mid bc$ parajasti siis, kui $a \mid b$.

b) Nende tingimuste kehtimise korral kui lisaks $a \neq 0$, siis $\frac{bc}{ac} = \frac{b}{a}$.

**1.18** Olgu $a, b, c \in \mathbb{Z}$, $a, b \neq 0$. Siis tingimused

(1) $a \mid c$ ja $b \mid \frac{c}{a}$,

(2) $b \mid c$ ja $a \mid \frac{c}{b}$,

(3) $ab \mid c$

on samaväärsed ning kui need kehtivad, siis $\frac{\frac{c}{a}}{b} = \frac{\frac{c}{b}}{a} = \frac{c}{ab}$.

**1.19** Olgu $a, b, c \in \mathbb{Z}$, $a, b \neq 0$. Kui $a \mid b$, siis $\frac{b}{a} \mid c$ parajasti siis, kui $b \mid ac$, ning kõigi nende tingimuste kehtimise korral $\frac{c}{\frac{b}{a}} = \frac{ac}{b}$.

**1.20** Olgu $a_1, \ldots, a_l, b_1, \ldots, b_l \in \mathbb{Z}$.

a) Kui iga $i = 1, \ldots, l$ korral $a_i \mid b_i$, siis $a_1 \ldots a_l \mid b_1 \ldots b_l$ ja $a_1, \ldots, a_l \neq 0$ korral $\frac{b_1}{a_1} \ldots \frac{b_l}{a_l} = \frac{b_1 \ldots b_l}{a_1 \ldots a_l}$.

b) Kui lisaks $b_1, \ldots, b_l \neq 0$ ja mingi $i = 1, \ldots, l$ korral $|a_i| \neq |b_i|$, siis $|a_1 \ldots a_l|$ on $|b_1 \ldots b_l|$ pärisjagaja.

**1.21** Olgu $a, b, c, d \in \mathbb{Z}$, $a, c \neq 0$. Kui $a \mid b$ ja $c \mid d$, siis $\frac{b}{a} \mid \frac{d}{c}$ parajasti siis, kui $bc \mid ad$, ning nende tingimuste täidetuse korral kui lisaks $b \neq 0$, siis $\frac{\frac{d}{c}}{\frac{b}{a}} = \frac{ad}{bc}$.

**1.22** Olgu $n \in \mathbb{N}$, $m \in \mathbb{N}^+$.

a) Kui $n \mid m$, siis $n \leqslant m$.

b) Kui $n$ on $m$ pärisjagaja, siis $n < m$.

**1.23** Olgu $a, b \in \mathbb{Z}$, $b \neq 0$. Kui $a \mid b$, siis $|a| \leqslant |b|$.

**1.24** Olgu $a, b \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$, nii et $m \mid a$ ja $m \mid b$. Siis $a \leqslant b$ parajasti siis, kui $\frac{a}{m} \leqslant \frac{b}{m}$.

**1.25** Olgu $m, n, s \in \mathbb{N}^+$, nii et $m \mid s$ ja $n \mid s$. Siis $m \leqslant n$ parajasti siis, kui $\frac{s}{m} \geqslant \frac{s}{n}$.

**1.26** Olgu $m \in \mathbb{N}^+$. Olgu $d_0, \ldots, d_l$ arvu $m$ kõik naturaalarvulised jagajad kasvavas järjekorras. Siis iga $i = 0, \ldots, l$ korral $d_i d_{l-i} = m$.

**1.27** Olgu $a, b, c \in \mathbb{Z}$, nii et $a \mid b$.

a) Tingimused $a \mid c$, $a \mid b + c$ ja $a \mid b - c$ on samaväärsed.

b) Nende täidetuse korral kui lisaks $a \neq 0$, siis $\frac{b+c}{a} = \frac{b}{a} + \frac{c}{a}$ ja $\frac{b-c}{a} = \frac{b}{a} - \frac{c}{a}$.

**1.28** Olgu $a, b_1, \ldots, b_l \in \mathbb{Z}$. Kui iga $i = 1, \ldots, l$ korral $a \mid b_i$, siis $a \mid b_1 + \ldots + b_l$.

Olgu $a \in \mathbb{Z}$. Öeldakse, et $a$ on **paaris**, kui $2 \mid a$, ja $a$ on **paaritu**, kui $2 \nmid a$.

**1.29** 0 on paaris.

**1.30** Olgu $a \in \mathbb{Z}$. Siis $a$ on paaris parajasti siis, kui $|a|$ on paaris.

**1.31** Olgu $a, b \in \mathbb{Z}$. Kui $a \mid b$ ja $a$ on paaris, siis $b$ on paaris.

Olgu $m \in \mathbb{N}^+$. Öeldakse, et $m$ on **algarv**, kui 1 on arvu $m$ ainus pärisjagaja. Öeldakse, et $m$ on **kordarv**, kui arvul $m$ on lisaks teisi pärisjagajaid.

Kõigi algarvude hulka tähistame sümboliga $\mathbb{P}$.

**1.32** Olgu $p \in \mathbb{P}$. Siis $p > 1$.

**1.33** 2 on ainus paaris algarv.

Olgu $m \in \mathbb{N}^+$. Olgu $p \in \mathbb{P}$. Kui $p \mid m$, siis öeldakse, et arv $p$ on arvu $m$ **algtegur**.

**1.34** Olgu $m \in \mathbb{N}^+$, $m \neq 1$. Siis arvu $m$ vähim 1-st suurem jagaja on algarv.

**1.35** Olgu $m \in \mathbb{N}^+$, $m \neq 1$. Olgu $m = pd$, kus $p$ on arvu $m$ vähim algtegur. Siis arvul $d$ ei ole $p$-st väiksemaid algtegureid.

**1.36** Olgu $m \in \mathbb{N}^+$, $m \neq 1$. Siis $m$ on kordarv parajasti siis, kui arvu $m$ vähim algtegur $p$ rahuldab tingimust $p^2 \leqslant m$.

**1.37** Leidub kuitahes pikki järjestikuste naturaalarvude järjendeid, mis ei sisalda algarve.

**1.38** **Eukleidese teoreem** Leidub kuitahes suuri algarve. Teisi sõnu, $\mathbb{P}$ on lõpmatu.



# 2 Jäägiga jagamine

**2.1** Olgu $a \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Siis leidub täpselt üks niisugune paar $(q, r)$, et $a = qm + r$ ning $q \in \mathbb{Z}$ ja $r \in \mathbb{N}$, $r < m$; seejuures $q = \max\{c \in \mathbb{Z} : cm \leqslant a\}$.

Olgu $a \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Olgu $q \in \mathbb{Z}$ ja $r \in \mathbb{N}$, $r < m$. Kui $a = qm + r$, siis öeldakse, et $q$ on $a$ ja $m$ **(täisarvuline) jagatis** ning $r$ on **jääk** arvu $a$ **(täisarvulisel) jagamisel** arvuga $m$; neid (täisarvulist) jagatist ja jääki tähistatakse vastavalt $a \operatorname{div} m$ ja $a \bmod m$. Tehtesümbolid div ja mod olgu kokkuleppeliselt omavahel võrdse, korrutus- ja jagamismärkidest kõrgema ning korrutamist tähistavast järjestkirjutamisest madalama prioriteediga.

**2.2** Olgu $a \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Siis $(a \operatorname{div} m)m + a \bmod m = a$ ja $0 \leqslant a \bmod m < m$.

**2.3** Olgu $m \in \mathbb{N}^+$ ning $a, c \in \mathbb{Z}$. Siis $cm \leqslant a$ parajasti siis, kui $c \leqslant a \operatorname{div} m$.

**2.4** Olgu $a \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Siis $m \mid a$ parajasti siis, kui $a \bmod m = 0$, ning nende tingimuste täidetuse korral $a \operatorname{div} m = \frac{a}{m}$.

**2.5** Olgu $a \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Siis $am \operatorname{div} m = a$ ja $am \bmod m = 0$.

**2.6** Olgu $m \in \mathbb{N}^+$. Olgu $r \in \mathbb{N}$, $r < m$. Siis $r \operatorname{div} m = 0$ ja $r \bmod m = r$.

**2.7** Olgu $a, b \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Siis $(a+bm) \operatorname{div} m = a \operatorname{div} m + b$ ja $(a+bm) \bmod m = a \bmod m$.

**2.8** Olgu $m \in \mathbb{N}^+$ ja $a \in \mathbb{Z}$. Siis $a \operatorname{div} m$ on negatiivne parajasti siis, kui $a$ on negatiivne.

**2.9** Olgu $m \in \mathbb{N}^+$. Olgu $n \in \mathbb{N}$. Kui $n \neq 0$ ja $m \neq 1$, siis $n \operatorname{div} m < n$.

**2.10** Olgu $a, b \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Siis tingimused

(1) $a \leqslant b$,

(2) $a \operatorname{div} m \leqslant b \operatorname{div} m$ ja võrduse kehtimise korral $a \bmod m \leqslant b \bmod m$

on samaväärsed.

**2.11** Olgu $m, n \in \mathbb{N}^+$ ja $s \in \mathbb{N}$. Kui $m \leqslant n$, siis $s \operatorname{div} m \geqslant s \operatorname{div} n$.

**2.12** Olgu $a \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Siis

a) kui $m \nmid a$, siis $(-a) \operatorname{div} m = -a \operatorname{div} m - 1$ ja $(-a) \bmod m = m - a \bmod m$;

b) kui $m \mid a$, siis $(-a) \operatorname{div} m = -a \operatorname{div} m$.

**2.13** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Siis

$$\left(\sum_{i=1}^{l} a_i\right) \operatorname{div} m = \sum_{i=1}^{l} a_i \operatorname{div} m + \left(\sum_{i=1}^{l} a_i \bmod m\right) \operatorname{div} m,$$

$$\left(\sum_{i=1}^{l} a_i\right) \bmod m = \left(\sum_{i=1}^{l} a_i \bmod m\right) \bmod m.$$

**2.14** Olgu $a, b \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Siis

$$(a-b) \text{ div } m = a \operatorname{div} m - b \operatorname{div} m + (a \bmod m - b \bmod m) \operatorname{div} m,$$
$$(a-b) \bmod m = (a \bmod m - b \bmod m) \bmod m.$$

**2.15** Olgu $a, b \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Siis $ab \operatorname{div} m = (a \operatorname{div} m)b + (a \bmod m)b \operatorname{div} m$ ja $ab \bmod m = (a \bmod m)(b \bmod m) \bmod m$.

**2.16** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$ ja $m \in \mathbb{N}^+$. Siis

$$\left(\prod_{i=1}^{l} a_i\right) \bmod m = \left(\prod_{i=1}^{l} a_i \bmod m\right) \bmod m.$$

**2.17** Olgu $a \in \mathbb{Z}, l \in \mathbb{N}$ ja $m \in \mathbb{N}^+$. Siis $a^l \bmod m = (a \bmod m)^l \bmod m$.

**2.18** Olgu $a \in \mathbb{Z}$ ja $m, n \in \mathbb{N}^+$. Siis $na \operatorname{div} nm = a \operatorname{div} m$ ja $na \bmod nm = n(a \bmod m)$.

**2.19** Olgu $a \in \mathbb{Z}$ ja $m, n \in \mathbb{N}^+$. Siis $a \operatorname{div} mn = (a \operatorname{div} m) \operatorname{div} n$ ja $a \bmod mn = ((a \operatorname{div} m) \bmod n)m + a \bmod m$.

**2.20** Olgu $a \in \mathbb{Z}$. Siis $a$ on paaris parajasti siis, kui $a \bmod 2 = 0$, ja paaritu parajasti siis, kui $a \bmod 2 = 1$.

**2.21** Olgu $a, b \in \mathbb{Z}$.

a) $a$ ja $b$ on eri paarsusega parajasti siis, kui $a + b$ ja $a - b$ on mõlemad paaritud.

b) $a$ ja $b$ on ühe paarsusega parajasti siis, kui $a + b$ ja $a - b$ on mõlemad paaris.

**2.22** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Siis arv $a_1 + \ldots + a_l$ on paaris parajasti siis, kui hulgas $\{1, \ldots, l\}$ on paarisarv arve $i$, mille korral $a_i$ on paaritu, ja paaritu parajasti siis, kui hulgas $\{1, \ldots, l\}$ on paaritu arv arve $i$, mille korral $a_i$ on paaritu.

**2.23** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Siis arv $a_1 \ldots a_l$ on paaris parajasti siis, kui mingi $i = 1, \ldots, l$ korral $a_i$ on paaris, ja paaritu parajasti siis, kui iga $i = 1, \ldots, l$ korral $a_i$ on paaritu.

# 3 Kongruentsid

Olgu $m \in \mathbb{N}^+$. Olgu $a, b \in \mathbb{Z}$. Kui $a \bmod m = b \bmod m$, siis öeldakse, et arv $a$ on **kongruentne** arvuga $b$ **(mooduli)** $m$ **järgi** ehk ***modulo*** $m$ ja kirjutatakse $a \equiv b \pmod m$.

**3.1** Olgu $m \in \mathbb{N}^+$. Olgu $a, b \in \mathbb{Z}$. Siis $a \equiv b \pmod m$ parajasti siis, kui $m \mid b - a$.

**3.2** Olgu $m \in \mathbb{N}^+$. Olgu $a \in \mathbb{Z}$. Siis $a \equiv a \pmod m$. Teisi sõnu, kongruents $m$ järgi on refleksiivne.

**3.3** Olgu $m \in \mathbb{N}^+$. Olgu $a, b, c \in \mathbb{Z}$. Kui $a \equiv b \pmod m$ ja $b \equiv c \pmod m$, siis $a \equiv c \pmod m$. Teisi sõnu, kongruents $m$ järgi on transitiivne.



**3.4** Olgu $m \in \mathbb{N}^+$. Olgu $a, b \in \mathbb{Z}$. Siis $a \equiv b \pmod m$ parajasti siis, kui $b \equiv a \pmod m$. Teisi sõnu, kongruents $m$ järgi on sümmeetriline.

**3.5** Olgu $m \in \mathbb{N}^+$. Olgu $a \in \mathbb{Z}$. Siis $m \mid a$ parajasti siis, kui $a \equiv 0 \pmod m$.

**3.6** Olgu $m \in \mathbb{N}^+$. Olgu $a \in \mathbb{Z}$ ja $r \in \mathbb{N}, r < m$. Siis $a \equiv r \pmod m$ parajasti siis, kui $r = a \bmod m$.

**3.7** Olgu $m \in \mathbb{N}^+$. Olgu $a \in \mathbb{Z}$. Siis $a \equiv (a \bmod m) \pmod m$.

**3.8** Olgu $m \in \mathbb{N}^+$. Olgu $a, b \in \mathbb{Z}$. Siis $a + bm \equiv a \pmod m$.

**3.9** Olgu $m, n \in \mathbb{N}^+$. Olgu $a, b \in \mathbb{Z}$. Kui $a \equiv b \pmod m$ ja $n \mid m$, siis $a \equiv b \pmod n$.

**3.10** Olgu $m \in \mathbb{N}^+$ ja $d \in \mathbb{Z}, d \mid m$. Olgu $a, b \in \mathbb{Z}$. Kui $a \equiv b \pmod m$, siis $d \mid a$ parajasti siis, kui $d \mid b$.

**3.11** Olgu $m \in \mathbb{N}^+$. Olgu $a, b, c, d \in \mathbb{Z}$ ja $b \equiv d \pmod m$. Siis $a+b \equiv c+d \pmod m$ parajasti siis, kui $a \equiv c \pmod m$.

**3.12** Olgu $m \in \mathbb{N}^+$. Olgu $a, b, c \in \mathbb{Z}$. Siis seosed $a \equiv b \pmod m$, $a + c \equiv b + c \pmod m$ ja $a - c \equiv b - c \pmod m$ on samaväärsed.

**3.13** Olgu $m \in \mathbb{N}^+$. Olgu $a_1, \ldots, a_l, b_1, \ldots, b_l \in \mathbb{Z}$. Kui iga $i = 1, \ldots, l$ korral $a_i \equiv b_i \bmod m$, siis $a_1 + \ldots + a_l \equiv b_1 + \ldots + b_l \pmod m$.

**3.14** Olgu $m, n \in \mathbb{N}^+$. Olgu $a, b \in \mathbb{Z}$. Siis $a \equiv b \pmod m$ parajasti siis, kui $na \equiv nb \pmod{nm}$.

**3.15** Olgu $m \in \mathbb{N}^+$. Olgu $a, b, c \in \mathbb{Z}$. Kui $a \equiv b \pmod m$, siis $ac \equiv bc \pmod m$.

**3.16** Olgu $m \in \mathbb{N}^+$. Olgu $a_1, \ldots, a_l, b_1, \ldots, b_l \in \mathbb{Z}$. Kui iga $i = 1, \ldots, l$ korral $a_i \equiv b_i \pmod m$, siis $a_1 \ldots a_l \equiv b_1 \ldots b_l \pmod m$.

**3.17** Olgu $m \in \mathbb{N}^+$. Olgu $a, b \in \mathbb{Z}$ ja $l \in \mathbb{N}$. Kui $a \equiv b \pmod m$, siis $a^l \equiv b^l \pmod m$.

**3.18** Olgu $m \in \mathbb{N}^+$. Olgu $f : \mathbb{Z} \to \mathbb{Z}$ täisarvuliste kordajatega polünomiaalne funktsioon ja $a, b \in \mathbb{Z}$. Kui $a \equiv b \pmod m$, siis $f(a) \equiv f(b) \pmod m$.

**3.19** Olgu $m \in \mathbb{N}^+$. Olgu $f : \mathbb{Z} \to \mathbb{Z}$ täisarvuliste kordajatega polünomiaalne funktsioon ja $a \in \mathbb{Z}$. Kui $m \mid f(a)$, siis leidub täisarvuliste kordajatega polünomiaalne funktsioon $g : \mathbb{Z} \to \mathbb{Z}$, nii et $\deg f = \deg g + 1$ ja iga $x \in \mathbb{Z}$ korral $f(x) \equiv (x - a)g(x) \pmod m$.

# 4 Positsioonilised arvusüsteemid

Olgu $b \in \mathbb{N}^+$. Positsioonilisi arvusüsteeme käsitledes nimetatakse arve hulgast $\{r \in \mathbb{N} : r < b\}$ **$b$-ndsüsteemi numbriteks** ehk **$b$-ndnumbriteks**.

Olgu $b \in \mathbb{N}^+$ ja $n \in \mathbb{N}$. Olgu jada $d : \mathbb{N} \to \{r \in \mathbb{N} : r < b\}$ selline, et

$$n = \sum_{i \in \mathbb{N}} d_i b^i. \tag{1}$$

Siis esitust (1) nimetatakse arvu $n$ **esituseks (positsioonilises arvusüsteemis) alusel** $b$ ehk **esituseks** $b$**-ndsüsteemis** ehk $b$**-ndesituseks**. Lihtsuse mõttes ütleme edaspidi, et jada $d$ annab arvu $n$ esituse (1) ehk jada $d$ esitab arvu $n$ $b$-ndsüsteemis.

**4.1** Olgu $b \in \mathbb{N}^+$. Olgu $n \in \mathbb{N}$ ja $d : \mathbb{N} \to \{r \in \mathbb{N} : r < b\}$. Siis jada $d$ esitab $b$-ndsüsteemis arvu $n$ parajasti siis, kui $d_0 = n \bmod b$ ja jada $(d_{i+1} : i \in \mathbb{N})$ esitab $b$-ndsüsteemis arvu $n \operatorname{div} b$.

**4.2** Olgu $b \in \mathbb{N}^+$. Siis arvu 0 ainsa $b$-ndesituse annab nulljada $(0 : i \in \mathbb{N})$.

**4.3** Olgu $b \in \mathbb{N}^+$, $b \neq 1$. Siis iga naturaalarv $n$ on $b$-ndsüsteemis üheselt esitatav, st jada $d : \mathbb{N} \to \{r \in \mathbb{N} : r < b\}$, mis annab esituse (1), leidub ja on üheselt määratud.

**4.4** Olgu $b \in \mathbb{N}^+$ ja $k \in \mathbb{N}$. Esitagu jada $d = (d_i : i \in \mathbb{N})$ $b$-ndsüsteemis arvu $n$. Siis $d_k = (n \operatorname{div} b^k) \bmod b = \dfrac{n \bmod b^{k+1} - n \bmod b^k}{b^k}$.

Olgu $b \in \mathbb{N}^+$ ja $k \in \mathbb{N}$. Esitagu jada $d = (d_i : i \in \mathbb{N})$ $b$-ndsüsteemis arvu $n$. Öeldakse, et $n$ on $b$-ndsüsteemis $k$**-kohaline**, kui $|\{i \in \mathbb{N} : \text{mingi } j \geqslant i \text{ korral } d_j \neq 0\}| = k$.

**4.5** Olgu $b \in \mathbb{N}^+$. Olgu $n \in \mathbb{N}$. Siis $n$ on $b$-ndsüsteemis 0-kohaline parajasti siis, kui $n = 0$.

**4.6** Olgu $b \in \mathbb{N}^+$. Olgu $n, k \in \mathbb{N}^+$. Siis $n$ on $b$-ndsüsteemis $k$-kohaline parajasti siis, kui $b^{k-1} \leqslant n < b^k$.

**4.7** Olgu $b \in \mathbb{N}^+$. Olgu $n, m \in \mathbb{N}$ ja $k, l \in \mathbb{N}$. Kui $n$ on $b$-ndsüsteemis $k$-kohaline ja $m$ on $b$-ndsüsteemis $l$-kohaline ning $k < l$, siis $n < m$.

**4.8** Olgu $b \in \mathbb{N}^+$. Olgu $n, m \in \mathbb{N}$. Esitagu jadad $d = (d_i : i \in \mathbb{N})$ ja $c = (c_i : i \in \mathbb{N})$ $b$-ndsüsteemis vastavalt arvud $n$ ja $m$. Siis $n < m$ parajasti siis, kui leidub indeks $k$, nii et $d_k \neq c_k$, ning $m = \max\{k \in \mathbb{N} : d_k \neq c_k\}$ korral $d_m < c_m$.

**4.9** Olgu $b \in \mathbb{N}^+$, $b \neq 1$. Olgu $n \in \mathbb{N}$. Esitagu jada $d = (d_i : i \in \mathbb{N})$ $b$-ndsüsteemis arvu $n$. Siis leidub indeks $k$, nii et $d_k + 1 < b$, ning jada $c$, mis defineeritakse reegliga

$$c_k = \begin{cases} 0, & \text{kui } k < m, \\ d_k + 1, & \text{kui } k = m, \\ d_k, & \text{kui } k > m, \end{cases}$$

kus $m = \min\{k \in \mathbb{N} : d_k + 1 < b\}$, esitab $b$-ndsüsteemis arvu $n + 1$.

**4.10** Olgu $b \in \mathbb{N}^+$, $b \neq 1$. Olgu $n \in \mathbb{N}$. Esitagu jada $d = (d_i : i \in \mathbb{N})$ $b$-ndsüsteemis arvu $n+1$. Siis leidub indeks $k$, nii et $d_k > 0$, ning jada $c$, mis defineeritakse reegliga

$$c_k = \begin{cases} b - 1, & \text{kui } k < m, \\ d_k - 1, & \text{kui } k = m, \\ d_k, & \text{kui } k > m, \end{cases}$$



kus $m = \min\{k \in \mathbb{N} : d_k > 0\}$, esitab $b$-ndsüsteemis arvu $n$.

**4.11** Olgu $b \in \mathbb{N}^+$, $b \neq 1$. Olgu $k \in \mathbb{N}$. Siis jada $d$, mis defineeritakse reegliga

$$d_i = \begin{cases} 1, & \text{kui } i = k, \\ 0, & \text{kui } i \neq k, \end{cases}$$

esitab $b$-ndsüsteemis arvu $b^k$.

**4.12** Olgu $b \in \mathbb{N}^+$ ja $k \in \mathbb{N}$. Olgu $n \in \mathbb{N}$. Andku jada $d = (d_i : i \in \mathbb{N})$ arvu $n$ esituse alusel $b$ ja jada $c = (c_i : i \in \mathbb{N})$ alusel $b^k$. Siis iga $i \in \mathbb{N}$ korral

$$c_i = \sum_{\substack{j \in \mathbb{N} \\ j < k}} d_{ik+j} b^j$$

ja seejuures on viimane summa arvu $c_i$ esitus alusel $b$.

**4.13** Olgu $b \in \mathbb{N}^+$. Olgu $a \in \mathbb{Z}$ ja $n \in \mathbb{N}$, $m \in \mathbb{N}^+$. Andku jada $d$ arvu $n$ $b$-ndesituse. Kui $b \equiv a \pmod m$, siis

$$n \equiv \sum_{i \in \mathbb{N}} d_i a^i \pmod m.$$

**4.14** Olgu $b \in \mathbb{N}^+$, $b \neq 1$ ja $k \in \mathbb{N}$. Olgu $m \in \mathbb{N}$, nii et $m \mid b$. Olgu $n \in \mathbb{N}$ ja esitagu jada $d = (d_i : i \in \mathbb{N})$ $b$-ndsüsteemis arvu $n$. Siis

a) $n \equiv d_0 \pmod m$;

b) $n$ jagub $m$-ga parajasti siis, kui $d_0$ jagub $m$-ga.

Olgu $b \in \mathbb{N}^+$. Olgu $n \in \mathbb{N}$. Esitagu jada $d = (d_i : i \in \mathbb{N})$ arvu $n$ $b$-ndsüsteemis. Siis arvu $n$ **ristsummaks** $b$-ndsüsteemis nimetatakse arvu $n$ $b$-ndesituse $b$-ndnumbrite summat, st arvu

$$\sum_{i \in \mathbb{N}} d_i.$$

Arvu $n$ **alternatiivseks ristsummaks** $b$-ndsüsteemis nimetatakse arvu

$$\sum_{i \in \mathbb{N}} (-1)^i d_i.$$

**4.15** Olgu $b \in \mathbb{N}^+$, $b \neq 1$. Olgu $m \in \mathbb{N}$.

a) Kui $m \mid b - 1$, siis iga naturaalarv on $m$ järgi kongruentne oma ristsummaga $b$-ndsüsteemis.

b) Kui $m \mid b + 1$, siis iga naturaalarv on $m$ järgi kongruentne oma alternatiivse ristsummaga $b$-ndsüsteemis.

**4.16** Olgu $b \in \mathbb{N}^+$, $b \neq 1$. Olgu $m \in \mathbb{N}$.

a) Kui $m \mid b-1$, siis suvaline naturaalarv jagub $m$-ga parajasti siis, kui tema ristsumma $b$-ndsüsteemis jagub $m$-ga.

b) Kui $m \mid b+1$, siis suvaline naturaalarv jagub $m$-ga parajasti siis, kui tema alternatiivne ristsumma $b$-ndsüsteemis jagub $m$-ga.

# 5 Suurim ühistegur ja vähim ühiskordne

Olgu $(a_i : i \in I)$ täisarvude pere. Öeldakse, et naturaalarv $d$ on arvude $a_i$, $i \in I$, **suurim ühistegur**, kui $d$ on arvude $a_i$, $i \in I$, ühine jagaja ning arvude $a_i$, $i \in I$, iga ühine jagaja $c$ jagab arvu $d$.

Olgu $(a_i : i \in I)$ täisarvude pere. Öeldakse, et naturaalarv $m$ on arvude $a_i$, $i \in I$, **vähim ühiskordne**, kui $m$ on arvude $a_i$, $i \in I$, ühine kordne ning arv $m$ jagab arvude $a_i$, $i \in I$, iga ühist kordset $c$.

**5.1** Ühelgi perel pole mitut erinevat suurimat ühistegurit ega mitut erinevat vähimat ühiskordset.

Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. **$\mathbb{Z}$-lineaarseks kombinatsiooniks** arvudest $a_1, \ldots, a_l$ nimetatakse suvalist summat

$$\sum_{i=1}^{l} w_i a_i.$$

Pere $a = (a_1, \ldots, a_l)$ **$\mathbb{Z}$-lineaarne kate** on hulk, mis koosneb parajasti kõigist $\mathbb{Z}$-lineaarsetest kombinatsioonidest arvudest $a_1, \ldots, a_l$. Pere $a$ $\mathbb{Z}$-lineaarset katet tähistame $\mathcal{L}_{\mathbb{Z}}(a_1, \ldots, a_l)$.

**5.2** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Siis $\mathcal{L}_{\mathbb{Z}}(a_1, \ldots, a_l)$ on kinnine $\mathbb{Z}$-lineaarsete kombinatsioonide suhtes.

Olgu $M \subseteq \mathbb{Z}$. Olgu $d \in \mathbb{Z}$. Kui $M$ koosneb parajasti arvu $d$ kõigist kordsetest, siis ütleme, et $d$ on hulga $M$ **moodustaja**.

**5.3** Olgu $a = (a_1, \ldots, a_l)$ täisarvude pere. Siis pere $a$ lineaarsel kattel $\mathcal{L}_{\mathbb{Z}}(a_1, \ldots, a_l)$ leidub naturaalarvuline moodustaja ja see on parajasti arvude $a_1, \ldots, a_l$ suurim ühistegur.

**5.4** Olgu $a = (a_1, \ldots, a_l)$ täisarvude pere. Siis arvude $a_1, \ldots, a_l$ kõigi ühiste kordsete hulgal leidub naturaalarvuline moodustaja ja see on parajasti arvude $a_1, \ldots, a_l$ vähim ühiskordne.

Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Siis arvude $a_1, \ldots, a_l$ suurimat ühistegurit tähistame $\gcd(a_1, \ldots, a_l)$ ja vähimat ühiskordset $\operatorname{lcm}(a_1, \ldots, a_l)$.

**5.5** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Siis

a) iga $i = 1, \ldots, l$ korral $\gcd(a_1, \ldots, a_l) \mid a_i$ ja kui $c \in \mathbb{Z}$ on selline, et iga $i = 1, \ldots, l$ korral $c \mid a_i$, siis $c \mid \gcd(a_1, \ldots, a_l)$;

b) iga $i = 1, \ldots, l$ korral $a_i \mid \operatorname{lcm}(a_1, \ldots, a_l)$ ja kui $c \in \mathbb{Z}$ on selline, et iga $i = 1, \ldots, l$ korral $a_i \mid c$, siis $\operatorname{lcm}(a_1, \ldots, a_l) \mid c$.



**5.6** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Olgu $s \in \mathbb{Z}$. Siis $s \in \mathcal{L}_{\mathbb{Z}}(a_1, \ldots, a_l)$ parajasti siis, kui $\gcd(a_1, \ldots, a_l) \mid s$.

**5.7** Olgu $a_1, \ldots, a_l, b_1, \ldots, b_l \in \mathbb{Z}$. Olgu iga $i = 1, \ldots, l$ korral $|a_i| = |b_i|$. Siis $\gcd(a_1, \ldots, a_l) = \gcd(b_1, \ldots, b_l)$ ja $\operatorname{lcm}(a_1, \ldots, a_l) = \operatorname{lcm}(b_1, \ldots, b_l)$.

**5.8** Olgu $a_1, \ldots, a_l, b_1, \ldots, b_m \in \mathbb{Z}$. Kui $\{a_i : i = 1, \ldots, l\} \subseteq \{b_1, \ldots, b_m\}$, siis $\gcd(b_1, \ldots, b_m) \mid \gcd(a_1, \ldots, a_l)$ ja $\operatorname{lcm}(a_1, \ldots, a_l) \mid \operatorname{lcm}(b_1, \ldots, b_m)$.

**5.9** Olgu $a_1, \ldots, a_l, b_1, \ldots, b_m \in \mathbb{Z}$. Kui $\{a_i : i = 1, \ldots, l\} = \{b_j : j = 1, \ldots, m\}$, siis $\gcd(a_1, \ldots, a_l) = \gcd(b_1, \ldots, b_m)$ ja $\operatorname{lcm}(a_1, \ldots, a_l) = \operatorname{lcm}(b_1, \ldots, b_m)$.

**5.10** Olgu $a = (a_1, \ldots, a_l)$ täisarvude pere.

a) Kui komponent $a_i$ jagab selle pere igat komponenti, siis $\gcd(a_1, \ldots, a_l) = |a_i|$ ja kui lisaks $l > 1$, siis $\operatorname{lcm}(a_1, \ldots, a_l) = \operatorname{lcm}(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_l)$.

b) Kui selle pere iga komponent jagab komponenti $a_i$, siis $\operatorname{lcm}(a_1, \ldots, a_l) = |a_i|$ ja kui lisaks $l > 1$, siis $\gcd(a_1, \ldots, a_l) = \gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_l)$.

**5.11** Tühja pere suurim ühistegur on 0 ja vähim ühiskordne on 1.

**5.12** 1-liikmelise pere suurim ühistegur ja vähim ühiskordne on võrdsed selle pere ainsa liikme absoluutväärtusega.

**5.13** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Siis

a) $\gcd(a_1, \ldots, a_l) = 0$ parajasti siis, kui iga $i = 1, \ldots, l$ korral $a_i = 0$,

b) $\operatorname{lcm}(a_1, \ldots, a_l) = 1$ parajasti siis, kui iga $i = 1, \ldots, l$ korral $|a_i| = 1$.

**5.14** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Siis $\operatorname{lcm}(a_1, \ldots, a_l) = 0$ parajasti siis, kui mingi $i = 1, \ldots, l$ korral $a_i = 0$.

**5.15** Olgu $a_1, \ldots, a_l, b_1, \ldots, b_l \in \mathbb{Z}$. Kui iga $i = 1, \ldots, l$ korral $a_i \mid b_i$, siis $\gcd(a_1, \ldots, a_l) \mid \gcd(b_1, \ldots, b_l)$ ja $\operatorname{lcm}(a_1, \ldots, a_l) \mid \operatorname{lcm}(b_1, \ldots, b_l)$.

**5.16** Olgu $I$ ja $\Gamma$ lõplikud hulgad ja $s : I \to \Gamma$. Olgu $(a_i : i \in I)$ täisarvude pere. Siis

a) $\gcd(a_i : i \in I) = \gcd(\gcd(a_i : s(i) = \gamma) : \gamma \in \Gamma)$,

b) $\operatorname{lcm}(a_i : i \in I) = \operatorname{lcm}(\operatorname{lcm}(a_i : s(i) = \gamma) : \gamma \in \Gamma)$.

**5.17** Olgu Olgu $m_1, \ldots, m_l \in \mathbb{N}^+$. Olgu $a, b \in \mathbb{Z}$. Siis iga $i = 1, \ldots, l$ korral $a \equiv b \pmod{m_i}$ parajasti siis, kui $a \equiv b \pmod{\operatorname{lcm}(m_1, \ldots, m_l)}$.

**5.18** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Olgu $m \in \mathbb{N}$. Siis

a) $m \gcd(a_1, \ldots, a_l) = \gcd(ma_1, \ldots, ma_l)$;

b) kui $l > 0$, siis $m \operatorname{lcm}(a_1, \ldots, a_l) = \operatorname{lcm}(ma_1, \ldots, ma_l)$.

**5.19** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Olgu $m \in \mathbb{N}^+$ arvude $a_1, \ldots, a_l$ ühine jagaja. Siis

a) $\dfrac{\gcd(a_1, \ldots, a_l)}{m} = \gcd\left(\dfrac{a_1}{m}, \ldots, \dfrac{a_l}{m}\right)$;

b) kui $l > 0$, siis $\dfrac{\operatorname{lcm}(a_1, \ldots, a_l)}{m} = \operatorname{lcm}\left(\dfrac{a_1}{m}, \ldots, \dfrac{a_l}{m}\right)$.

**5.20** Olgu $a \in \mathbb{Z}$. Olgu $d_1, \ldots, d_l \in \mathbb{Z} \setminus \{0\}$, $l > 0$. Kui iga $i = 1, \ldots, l$ korral $d_i \mid a$,

siis $\gcd(d_1,\dots,d_l)\operatorname{lcm}\left(\frac{a}{d_1},\dots,\frac{a}{d_l}\right)=\gcd\left(\frac{a}{d_1},\dots,\frac{a}{d_l}\right)\operatorname{lcm}(d_1,\dots,d_l)=|a|$.

Olgu $a=(a_1,\dots,a_l)$, $l>0$, täisarvude pere. Olgu iga $k=1,\dots,l$ korral

$$A_k=\prod_{\substack{i=1\\ i\neq k}}^{l}a_i.$$

Siis tähistame $\overline{(a_1,\dots,a_l)}=(A_1,\dots,A_l)$.

**5.21** Olgu $a_1,\dots,a_l\in\mathbb{Z}\setminus\{0\}$, $l>0$. Olgu $c\in\mathbb{Z}$. Siis

a) $c$ on arvude $a_1,\dots,a_l$ ühine kordne parajasti siis, kui $a_1\dots a_l \mid c\gcd\overline{(a_1,\dots,a_l)}$.

b) $c$ on arvude $a_1,\dots,a_l$ ühine jagaja parajasti siis, kui $c\operatorname{lcm}\overline{(a_1,\dots,a_l)}\mid a_1\dots a_l$.

**5.22** Olgu $a_1,\dots,a_l\in\mathbb{Z}$, $l>0$. Siis $\operatorname{lcm}(a_1,\dots,a_l)\gcd\overline{(a_1,\dots,a_l)}=\gcd(a_1,\dots,a_l)\operatorname{lcm}\overline{(a_1,\dots,a_l)}=|a_1\dots a_l|$.

Olgu $a_1,\dots,a_l\in\mathbb{Z}$. Öeldakse, et arvud $a_1,\dots,a_l$ on **ühistegurita**, kui $\gcd(a_1,\dots,a_l)=1$.

**5.23** Olgu $a_1,\dots,a_l\in\mathbb{Z}$. Siis arvud $a_1,\dots,a_l$ on ühistegurita parajasti siis, kui arvudel $a_1,\dots,a_l$ ei leidu ühist algarvulist jagajat.

**5.24** Olgu $a_1,\dots,a_l\in\mathbb{Z}$. Olgu $m\in\mathbb{N}^+$ arvude $a_1,\dots,a_l$ ühine jagaja. Siis $m=\gcd(a_1,\dots,a_l)$ parajasti siis, kui arvud $\frac{a_1}{m},\dots,\frac{a_l}{m}$ on ühistegurita.

**5.25** Olgu $a_1,\dots,a_l\in\mathbb{Z}\setminus\{0\}$, $l>0$. Olgu $m\in\mathbb{N}$ arvude $a_1,\dots,a_l$ ühine kordne. Siis $m=\operatorname{lcm}(a_1,\dots,a_l)$ parajasti siis, kui arvud $\frac{m}{a_1},\dots,\frac{m}{a_l}$ on ühistegurita.

Vaatleme lähemalt suurima ühisteguri ja vähima ühiskordse võtmist 2-elemendiliste perede korral — gcd ja lcm on siis kui binaarsed tehted täisarvudel.

**5.26** Olgu $n\in\mathbb{N}$. Siis

a) $\gcd(n,n)=n$,

b) $\operatorname{lcm}(n,n)=n$.

**5.27** Olgu $a\in\mathbb{Z}$. Siis

a) $\gcd(a,a)=|a|$,

b) $\operatorname{lcm}(a,a)=|a|$.

**5.28** Olgu $a,b\in\mathbb{Z}$. Siis

a) $\gcd(a,b)=\gcd(b,a)$,

b) $\operatorname{lcm}(a,b)=\operatorname{lcm}(b,a)$.

Teisi sõnu, binaarsed gcd ja lcm on kommutatiivsed.

**5.29** Olgu $a,b,c\in\mathbb{Z}$. Siis

a) $\gcd(\gcd(a,b),c)=\gcd(a,\gcd(b,c))$,



b) $\operatorname{lcm}(\operatorname{lcm}(a,b),c)=\operatorname{lcm}(a,\operatorname{lcm}(b,c))$.

Teisi sõnu, binaarsed gcd ja lcm on assotsiatiivsed.

**5.30** Olgu $n,m\in\mathbb{N}$. Siis tingimused $n\mid m$, $\gcd(n,m)=n$ ja $\operatorname{lcm}(n,m)=m$ on samaväärsed.

**5.31** Olgu $a,b\in\mathbb{Z}$. Siis tingimused $a\mid b$, $\gcd(a,b)=|a|$ ja $\operatorname{lcm}(a,b)=|b|$ on samaväärsed.

**5.32** Olgu $n,m\in\mathbb{N}$. Siis

a) $\gcd(n,\operatorname{lcm}(n,m))=n$,

b) $\operatorname{lcm}(n,\gcd(n,m))=n$.

Teisi sõnu, binaarsed gcd ja lcm naturaalarvudel neelduvad teineteise toimel.

**5.33** Olgu $a,b\in\mathbb{Z}$. Siis

a) $\gcd(a,\operatorname{lcm}(a,b))=|a|$,

b) $\operatorname{lcm}(a,\gcd(a,b))=|a|$.

**5.34** Olgu $n\in\mathbb{N}$. Siis

a) $\gcd(0,n)=\gcd(n,0)=n$,

b) $\operatorname{lcm}(1,n)=\operatorname{lcm}(n,1)=n$.

Teisi sõnu, 0 ja 1 on vastavalt binaarse gcd naturaalarvudel ja binaarse lcm naturaalarvudel ühikelement.

**5.35** Olgu $a\in\mathbb{Z}$. Siis

a) $\gcd(0,a)=\gcd(a,0)=|a|$,

b) $\operatorname{lcm}(1,a)=\operatorname{lcm}(a,1)=|a|$.

**5.36** Olgu $a\in\mathbb{Z}$. Siis

a) $\gcd(1,a)=\gcd(a,1)=1$,

b) $\operatorname{lcm}(0,a)=\operatorname{lcm}(a,0)=0$.

Teisi sõnu, 1 ja 0 on vastavalt binaarse gcd ja lcm nullelement.

**5.37** Olgu $m\in\mathbb{N}^+$. Olgu $a,b\in\mathbb{Z}$. Kui $a\equiv b\pmod m$, siis $\gcd(a,m)=\gcd(b,m)$.

**5.38** Olgu $m\in\mathbb{N}^+$. Olgu $a\in\mathbb{Z}$. Siis $\gcd(a,m)=\gcd(a+m,m)=\gcd(a-m,m)=\gcd(a\bmod m,m)$.

**5.39** Olgu $a,b_1,\dots,b_l\in\mathbb{Z}$. Siis

$$\gcd\left(a,\prod_{i=1}^{l}b_i\right)=\gcd\left(a,\prod_{i=1}^{l}\gcd(a,b_i)\right).$$

**5.40** Olgu $a,b_1,\dots,b_l\in\mathbb{Z}$. Siis

$$a\mid\prod_{i=1}^{l}b_i\iff a\mid\prod_{i=1}^{l}\gcd(a,b_i).$$

**5.41** Olgu $a, b, c \in \mathbb{Z}$. Kui $a \mid bc$, siis $a \mid \gcd(a, b)c$.

**5.42** Olgu $a, b \in \mathbb{Z}$. Siis $\gcd(a, b)\operatorname{lcm}(a, b) = |ab|$.

Olgu $a, b \in \mathbb{Z}$. Kui $a$ ja $b$ on ühistegurita (ehk $\gcd(a, b) = 1$), siis kirjutatakse $a \perp b$.

**5.43** Olgu $a, b \in \mathbb{Z}$. Siis $a \perp b$ parajasti siis, kui $b \perp a$. Teisi sõnu, seos $\perp$ on sümmeetriline.

**5.44** Olgu $a \in \mathbb{Z}$. Siis $a \perp 1$ (ehk $1 \perp a$).

**5.45** Olgu $a \in \mathbb{Z}$. Siis tingimused $a \perp 0$ (ehk $0 \perp a$), $a \perp a$ ja $|a| = 1$ on samaväärsed.

**5.46** Olgu $a, b, c \in \mathbb{Z}$. Kui $a \mid c$ ja $b \perp c$, siis $a \perp b$.

**5.47** Olgu $a, b \in \mathbb{Z}$. Kui $a \mid b$ ja $a \perp b$, siis $|a| = 1$.

**5.48** Olgu $a, b \in \mathbb{Z}$. Siis $a \perp b$ parajasti siis, kui iga $p \in \mathbb{P}$ korral $p \nmid a$ või $p \nmid b$.

**5.49** Olgu $a \in \mathbb{Z}$. Olgu $p \in \mathbb{P}$. Siis tingimused $p \mid a$, $a \not\perp p$ ja $\gcd(a, p) = p$ on samaväärsed.

**5.50** Olgu $a, b \in \mathbb{Z}$. Olgu $m \in \mathbb{N}^+$. Kui $a \equiv b \pmod{m}$, siis $a \perp m$ parajasti siis, kui $b \perp m$.

**5.51** Olgu $a, b \in \mathbb{Z}$. Olgu $m \in \mathbb{N}^+$. Kui $a \perp b$, siis leiduvad $k, l \in \mathbb{N}$, nii et $ka + lb \equiv 1 \pmod{m}$.

**5.52** Olgu $a, b_1, \ldots, b_l \in \mathbb{Z}$. Siis tingimused

(1) iga $i = 1, \ldots, l$ korral $a \perp b_i$,

(2) $a \perp b_1 \ldots b_l$,

(3) $a \perp \operatorname{lcm}(b_1, \ldots, b_l)$

on samaväärsed.

**5.53** Olgu $a, b, c \in \mathbb{Z}$. Kui $a \perp b$, siis $\gcd(a, bc) = \gcd(a, c)$.

**5.54** **Eukleidese lemma** Olgu $a, b, c \in \mathbb{Z}$. Kui $a \mid bc$ ja $a \perp b$, siis $a \mid c$.

**5.55** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Olgu $p \in \mathbb{P}$. Siis $p \mid a_1 \ldots a_l$ parajasti siis, kui mingi $i = 1, \ldots, l$ korral $p \mid a_i$.

**5.56** Olgu $a \in \mathbb{Z}$. Olgu $p \in \mathbb{P}$ ja $l \in \mathbb{N}^+$. Siis tingimused $p \mid a^l$, $p \mid a$ ja $p^l \mid a^l$ on samaväärsed.

**5.57** Olgu $p \in \mathbb{P}$. Olgu $f : \mathbb{Z} \to \mathbb{Z}$ täisarvuliste kordajatega polünomiaalne funktsioon ja $a_1, \ldots, a_n \in \mathbb{Z}$ paarikaupa mittekongruentsed $p$ järgi. Kui iga $i = 1, \ldots, n$ korral $p \mid f(a_i)$, siis $n \leqslant \min(p, \deg f)$.

**5.58** Olgu $a, b \in \mathbb{Z}$. Olgu $m \in \mathbb{N}^+$ arvude $a, b$ ühine jagaja. Siis $\gcd(a, b) = m$ parajasti siis, kui $\frac{a}{m} \perp \frac{b}{m}$.

**5.59** Olgu $a, b \in \mathbb{Z} \setminus \{0\}$. Olgu $m \in \mathbb{N}$ arvude $a, b$ ühine kordne. Siis $\operatorname{lcm}(a, b) = m$ parajasti siis, kui $\frac{m}{a} \perp \frac{m}{b}$.



**5.60** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Olgu $k \in \mathbb{N}$. Siis

a) kui $l > 0$, siis $\gcd(a_1^k, \ldots, a_l^k) = \gcd(a_1, \ldots, a_l)^k$;

b) $\operatorname{lcm}(a_1^k, \ldots, a_l^k) = \operatorname{lcm}(a_1, \ldots, a_l)^k$.

**5.61** Olgu $a, b \in \mathbb{Z}$. Olgu $l \in \mathbb{N}^+$. Siis $a^l \mid b^l$ parajasti siis, kui $a \mid b$.

**5.62** Olgu $m \in \mathbb{N}^+$. Olgu $a, b, c \in \mathbb{Z}$. Kui $c \perp m$, siis $ca \equiv cb \pmod{m}$ parajasti siis, kui $a \equiv b \pmod{m}$.

**5.63** Olgu $m \in \mathbb{N}^+$. Olgu $a, b, c \in \mathbb{Z}$. Siis $ca \equiv cb \pmod{m}$ parajasti siis, kui $a \equiv b \pmod{\frac{m}{\gcd(c, m)}}$.

**5.64** Olgu $m \in \mathbb{N}^+$. Olgu $a, b, c, d \in \mathbb{Z}$, nii et $b \equiv d \pmod{m}$. Kui $b \perp m$ (ehk $d \perp m$), siis $ab \equiv cd \pmod{m}$ parajasti siis, kui $a \equiv c \pmod{m}$.

**5.65** Olgu $a, b \in \mathbb{Z}$. Olgu $l, m \in \mathbb{N}^+$. Siis $a \perp b$ parajasti siis, kui $a^l \perp b^m$.

**5.66** Olgu $a_1, \ldots, a_l \in \mathbb{Z}$. Siis arvud $a_1, \ldots, a_l$ on paarikaupa ühistegurita parajasti siis, kui perede $(a_1, \ldots, a_l)$ ja $\overline{(a_1, \ldots, a_l)}$ vastavad komponendid on ühistegurita.

**5.67** Olgu $a_1, \ldots, a_l \in \mathbb{Z} \setminus \{0\}$. Siis tingimused

(1) $a_1, \ldots, a_l$ on paarikaupa ühistegurita,

(2) $\overline{(a_1, \ldots, a_l)}$ komponendid on ühistegurita,

(3) $\operatorname{lcm}(a_1, \ldots, a_l) = |a_1 \ldots a_l|$

on samaväärsed.

**5.68** Olgu $a, b_1, \ldots, b_l \in \mathbb{Z}$. Kui $b_1, \ldots, b_l$ on paarikaupa ühistegurita, siis $b_i \mid a$ iga $i = 1, \ldots, l$ korral parajasti siis, kui $b_1 \ldots b_l \mid a$.

**5.69** Olgu $m_1, \ldots, m_l \in \mathbb{N}^+$. Olgu $a, b \in \mathbb{Z}$. Kui $m_1, \ldots, m_l$ on paarikaupa ühistegurita, siis $a \equiv b \pmod{m_i}$ iga $i = 1, \ldots, l$ korral parajasti siis, kui $a \equiv b \pmod{m_1 \ldots m_l}$.

**5.70** Olgu $a, b \in \mathbb{Z}$, kus $a \neq 0$ või $b \neq 0$. Olgu $v, w, x, y \in \mathbb{Z}$.

a) $ax + by = av + bw$ parajasti siis, kui mingi $k \in \mathbb{Z}$ korral $x = v + k\frac{b}{\gcd(a, b)}$ ja $y = w - k\frac{a}{\gcd(a, b)}$.

b) Kui $a \perp b$, siis $ax + by = av + bw$ parajasti siis, kui mingi $k \in \mathbb{Z}$ korral $x = v + kb$ ja $y = w - ka$.

# 6 Kanooniline esitus

Olgu $m \in \mathbb{N}^+$. Olgu jada $k : \mathbb{P} \to \mathbb{N}$ selline, et hulk

$$m = \prod_{p \in \mathbb{P}} p^{k_p}. \tag{2}$$

Seda esitust nimetatakse arvu $m$ **kanooniliseks esituseks**.

**6.1** Arvu 1 ainsa kanoonilise esituse annab nulljada ($0 : p \in \mathbb{P}$).

**6.2** Olgu arv $m \in \mathbb{N}^+$ esitatud kanooniliselt kujul (2). Olgu $p \in \mathbb{P}$ ja $l \in \mathbb{N}$. Siis $p^l \mid m$ parajasti siis, kui $l \leqslant k_p$.

**6.3 Aritmeetika põhiteoreem** Olgu $m \in \mathbb{N}^+$. Siis $m$ on üheselt kanooniliselt esituv, st jada $k : \mathbb{P} \to \mathbb{N}$, mis annab esituse (2), leidub ja on üheselt määratud.

Olgu $m \in \mathbb{N}^+$ ja $p \in \mathbb{P}$. Kirjutisega $p \triangleright m$ tähistagem algarvu $p$ astendajat arvu $m$ kanoonilises esituses (st arvu $k_p$ esitusest (2)). Märgi $\triangleright$ prioriteet olgu kokkuleppeliselt kõrgem kui korrutusmärgil $\cdot$ ja jagamismärgil :, kuid madalam kui korrutamist tähistaval järjestkirjutamisel.

**6.4** Olgu $m, n \in \mathbb{N}^+$. Siis $m = n$ parajasti siis, kui iga $p \in \mathbb{P}$ korral $p \triangleright m = p \triangleright n$.

**6.5** Olgu $p \in \mathbb{P}$. Siis $p \triangleright 1 = 0$.

**6.6** Olgu $p \in \mathbb{P}$. Olgu $l \in \mathbb{N}$.

a) $p \triangleright p^l = l$.

b) Iga $q \in \mathbb{P}$, $q \neq p$ korral $p \triangleright q^l = 0$.

**6.7** Olgu $m_1, \ldots, m_l \in \mathbb{N}^+$. Olgu $p \in \mathbb{P}$. Siis $p \triangleright m_1 \ldots m_l = p \triangleright m_1 + \ldots + p \triangleright m_l$.

**6.8** Olgu $m \in \mathbb{N}^+$ ja $l \in \mathbb{N}$. Olgu $p \in \mathbb{P}$. Siis $p \triangleright m^l = l(p \triangleright m)$.

**6.9** Olgu $m, n \in \mathbb{N}^+$. Siis $n \mid m$ parajasti siis, kui iga $p \in \mathbb{P}$ korral $p \triangleright n \leqslant p \triangleright m$.

**6.10** Olgu $m, n \in \mathbb{N}^+$, kus $n \mid m$. Olgu $p \in \mathbb{P}$. Siis $p \triangleright \dfrac{m}{n} = p \triangleright n - p \triangleright n$.

**6.11** Olgu $m, n \in \mathbb{N}^+$, $m > n$. Olgu $p \in \mathbb{P}$.

a) Kui $p \triangleright m = p \triangleright n$, siis $p \triangleright (m+n) \geqslant p \triangleright m = p \triangleright n$ ja $p \triangleright (m-n) \geqslant p \triangleright m = p \triangleright n$.

b) Kui $p \triangleright m \neq p \triangleright n$, siis $p \triangleright (m+n) = p \triangleright (m-n) = \min(p \triangleright m, p \triangleright n)$.

**6.12** Olgu $m_1, \ldots, m_l \in \mathbb{N}^+$. Olgu $p \in \mathbb{P}$. Siis

a) $p \triangleright \gcd(m_1, \ldots, m_l) = \min(p \triangleright m_1, \ldots, p \triangleright m_l)$;

b) $p \triangleright \operatorname{lcm}(m_1, \ldots, m_l) = \max(p \triangleright m_1, \ldots, p \triangleright m_l)$.

**6.13** Olgu $n, m \in \mathbb{N}^+$. Siis $n \perp m$ parajasti siis, kui iga $p \in \mathbb{P}$ korral $p \triangleright n = 0$ või $p \triangleright m = 0$.

**6.14 Legendre'i valem** Olgu $n \in \mathbb{N}$. Olgu $p \in \mathbb{P}$. Siis

$$p \triangleright n! = \sum_{i \in \mathbb{N}^+} n \operatorname{div} p^i.$$

**6.15** Olgu $a, b_1, \ldots, b_l \in \mathbb{Z}$. Siis

a) $\gcd(a, \operatorname{lcm}(b_1, \ldots, b_l)) = \operatorname{lcm}(\gcd(a, b_1), \ldots, \gcd(a, b_l))$;

b) $\operatorname{lcm}(a, \gcd(b_1, \ldots, b_l)) = \gcd(\operatorname{lcm}(a, b_1), \ldots, \operatorname{lcm}(a, b_l))$.

Teisi sõnu, gcd ja lcm on teineteise suhtes distributiivsed.



**6.16** Olgu $m \in \mathbb{N}^+$. Olgu $a_1, \ldots, a_l \in \mathbb{Z}$ ja $k_1, \ldots, k_l \in \mathbb{N}$. Kui $a_1^{k_1} = \ldots = a_l^{k_l} = m$, siis leidub $n \in \mathbb{N}^+$, nii et $n^{\operatorname{lcm}(k_1, \ldots, k_l)} = m$.

**6.17** Olgu $m_1, \ldots, m_l$ paarikaupa ühistegurita. Olgu $d \in \mathbb{Z}$ ja $k \in \mathbb{N}$. Kui $m_1 \ldots m_l = d^k$, siis leiduvad $n_1, \ldots, n_l \in \mathbb{N}^+$, nii et iga $i = 1, \ldots, l$ korral $m_i = n_i^k$.