I. KOKONAISLUVUT

I.0 Kokonaislukujen määritelmä

Määr.: Kokonaislukujen joukko on

$$\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/E,$$

missä E on $\mathbb{N}\times\mathbb{N}$:n ekv. rel., jolla $(m,n)\,E\,(m',n') \Leftrightarrow m+n' = n+m'$. Alkion $(m,n)\in\mathbb{N}\times\mathbb{N}$ ekv. luokkaa merk. $[m,n]$:llä.

(Idea: $[m,n]$ tulee olemaan m:n ja n:n erotus.)

Siis $\mathbb{Z} = \{[m,n] \mid m,n\in\mathbb{N}\}$
$= \{[p,0] \mid p\in\mathbb{N}\} \cup \{[0,q] \mid q\in\mathbb{N}_+\}$;
jälkimm. niillä luetellut ovat kaikki eri alkioita.

Halutaan määritellä kok.lukujen yhteenlasku $+$ ja kertolasku $\cdot$ $\mathbb{N}$:n vast. toimitusten avulla:

Määr.: Kun $m,n,p,q\in\mathbb{N}$, asetamme

$$[m,n]+[p,q] = [m+p,\ n+q]$$
$$[m,n]\cdot[p,q] = [mp+nq,\ mq+np].$$

Osoitettava, että laskujen oikea puoli riippuu vain vas. puol. ekv. luokista, ei edustajien (m,n) ja (p,q) valinnasta:

Lemma: $[m,n] = [m',n']$, $[p,q] = [p',q']$
$\Rightarrow$ $[m+p,\ n+q] = [m'+p',\ n'+q']$,
$[mp+nq,\ mq+np] = [m'p'+n'q',\ m'q'+n'p']$.

Tod.: $[m,n] = [m',n'], [p,q] = [p',q'] \Rightarrow m+n' = n+m'$, $p+q' = q+p' \Rightarrow (m+p)+(n'+q') = (m+n')+(p+q') =$
$= (n+m')+(q+p') = (n+q)+(m'+p') \Rightarrow$
$[m+p,\ n+q] = [m'+p',\ n'+q']$ ($\mathbb{N}$:n yhd. laskun liitäänn. ja vaihdann.). Toinen kohta vastaavasti. □

$\mathbb{Z}$:n yhteen- ja kertolaskun perusominaisuudet:

Lause: Kaikilla $x, y, z \in \mathbb{Z}$ on

i) $x+y = y+x$
ii) $x+(y+z) = (x+y)+z$
iii) $x+[0,0] = x$
iv) $xy = yx$
v) $x(yz) = (xy)z$
vi) $x\cdot[1,0] = x$
vii) $x(y+z) = xy+xz$
viii) $xy = [0,0] \Rightarrow x=[0,0]$ tai $y=[0,0]$.

Lisäksi pätee:

ix) Jos $x \in \mathbb{Z}$, niin $\exists y \in \mathbb{Z}$ s.e. $x+y = [0,0]$.

(Huom.: Supistussääntö yht. laskulle $(x+z = y+z \Rightarrow x=y)$ seuraa ix):stä.)

Tod.: Nämä seuraavat $\mathbb{N}$:n ominaisuuksista. Tod. muutamia. Olk. $x=[m,n]$, $y=[p,q]$.

i) $x+y = [m+p, n+q] = [p+m, q+n] = y+x$.

viii) Ol. $xy = [0,0]$, mutta $x = [m,n] \neq [0,0]$, ts. $m \neq n$. Silloin joko $m<n$ tai $m>n$.

Olk. esim. $m>n \Rightarrow m = n+r$, $r \in \mathbb{N}_+$ (ts. $r>0$) $\Rightarrow x = [n+r, n] = [r,0]$ ja

$$[0,0] = xy = [r,0]\cdot[p,q] = [rp+0q, rq+0\cdot p] = [rp, rq]$$

$$\Rightarrow rp = rq \overset{r>0}{\Rightarrow} p=q \Rightarrow y=[p,q]=[0,0].$$

ix) $[m,n]+[n,m] = [m+n, n+m] = [0,0]$, koska $m+n = n+m$. □

Kohdassa ix) mainittu $y \in \mathbb{Z}$ on luvun $x \in \mathbb{Z}$ 1-käs. määräämä ($x+y = [0,0] = x+y' \Rightarrow y = y+[0,0] = y+(x+y') = (y+x)+y' = (x+y)+y' = [0,0]+y' = y'$) $\Rightarrow$ voidaan merkitä $y = -x$, x:n vastaluku. Yo. tod. $\Rightarrow -[m,n] = [n,m]$.

Kok. luvuille määr. järjestys $\mathbb{N}$:n järjestyksen avulla:

Määr.: Kun $[m,n], [p,q] \in \mathbb{Z}$, asetetaan

$$[m,n] \leq [p,q] \iff m+q \leq n+p.$$

Osoitettava, että määr. oikea puoli ei riipu vas. p. ehd. luokkien edustajien valinnasta: ol., että $m+q \leq n+p$ ja $[m,n] = [m',n']$, $[p,q] = [p',q']$. Osoitettava, että $m'+q' \leq n'+p'$.

$$\left.\begin{aligned} &m+q \leq n+p \\ &m+n' = n+m' \\ &p+q' = q+p' \end{aligned}\right\} \Rightarrow \begin{aligned} (m'+q')+(n+p) &= (m'+n)+(p+q') \\ &= (m+n')+(q+p') = (m+q)+(n'+p') \\ &\leq (n+p)+(n'+p') = (n'+p')+(n+p) \end{aligned}$$

$$\Rightarrow m'+q' \leq n'+p' \quad \left(\text{sillä } m'+q' > n'+p' \Rightarrow (m'+q')+(n+p) > (n'+p')+(n+p)\right).$$

Huom.: $[m,n] > [0,0] \iff m > n$
$\iff [m,n] = [r,0]$, $r \in \mathbb{N}_+$ (ks. viii): n tod.).
Vastaavasti $[m,n] < [0,0] \iff [m,n] = [0,s] = -[s,0]$, $s \in \mathbb{N}_+$.

Lause: Yll. relaatio $\leq$ on (täysi) järjestys $\mathbb{Z}$:ssa. Lisäksi kaikilla $x,y,z \in \mathbb{Z}$ on

$$x < y \Rightarrow x+z < y+z$$
$$x > [0,0],\ y > [0,0] \Rightarrow xy > [0,0].$$

Tod. mallikin transitiivisuus. $[m,n] \leq [p,q]$, $[p,q] \leq [r,s]$
$\Rightarrow m+q \leq n+p$, $p+s \leq q+r$
$\Rightarrow (m+s)+(p+q) = (m+q)+(p+s) \leq (n+p)+(q+r)$
$= (n+r)+(p+q)$
$\Rightarrow m+s \leq n+r \Rightarrow [m,n] \leq [r,s]$. □

Lause: Kuvaus $f: \mathbb{N} \to \mathbb{Z}$, $f(n) = [n,0]$ $\forall n \in \mathbb{N}$, on injektio, ja kaikilla $m,n \in \mathbb{N}$ on

i) $f(m+n) = f(m)+f(n)$
ii) $f(mn) = f(m)\cdot f(n)$
iii) $m \leq n \Rightarrow f(m) \leq f(n)$.

Tod.: Inj.: $f(m) = f(n) \Rightarrow [m,0] = [n,0] \Rightarrow m+0 = 0+n \Rightarrow m = n$.

i) $f(m+n) = [m+n, 0] = [m+n, 0+0] = [m,0] + [n,0]$
$= f(m) + f(n)$.

ii) $f(m\cdot n) = [mn, 0] = [mn + 0\cdot 0,\ m\cdot 0 + n\cdot 0]$
$= [m,0]\cdot[n,0] = f(m)\cdot f(n)$.

iii) $m \le n \Rightarrow m+0 \le 0+n \Rightarrow [m,0] \le [n,0] \Rightarrow f(m) \le f(n)$. □

Yleensä samastetaan f:n välityksellä joukot $\mathbb{N}$ ja $f(\mathbb{N}) \subset \mathbb{Z}$ (f inj. $\Rightarrow \mathbb{N} \cong f(\mathbb{N})$) s.e.

$$\mathbb{N} \ni n \text{ "}=\text{"} f(n) = [n,0] \in \mathbb{Z}.$$

Kun $x \in \mathbb{Z}$, on tällöin $x \ge 0 \Leftrightarrow x \in \mathbb{N}$ (samastuksessa $\mathbb{N} = f(\mathbb{N})$) ja $x < 0 \Leftrightarrow x = -r$, $r \in \mathbb{N}_+$.
Kun $m, n \in \mathbb{N}$, on lopuksi

$$[m,n] = [m,0] + [0,n] = [m,0] - [n,0] = m - n.$$

I.1 Kokonaislukujen tekijöihinjako

Määr.: Ol. $a, b \in \mathbb{Z}$. Sanomme, että a on jaollinen b:llä (l. b jakaa a:n l. b on a:n tekijä l. a on b:n monikerta), merk. $b \mid a$, jos $\exists c \in \mathbb{Z}$ s.e. $a = bc$. Muuten merk. $b \nmid a$.

Relaation $\mid$ ominaisuuksia:

i) $a \mid a \quad \forall a \in \mathbb{Z}$
ii) $a \mid b$ ja $b \mid a \Leftrightarrow a = b$ tai $a = -b$
iii) $a \mid b$ ja $b \mid c \Rightarrow a \mid c$
iv) $a \mid b$ ja $a \mid c \Rightarrow a \mid (b+c)$.

Tod.: i) $a = a \cdot 1$.
ii) $\Leftarrow$ selvä. $\Rightarrow$: $a = bc$, $b = ad$ $(c, d \in \mathbb{Z})$
$\Rightarrow a = bc = (ad)c = a(dc) \Rightarrow a(1-dc) = 0$.
Jos $a = 0$, niin myös $b = ad = 0\cdot d = 0$; jos taas $a \neq 0$, niin $a(1-dc) = 0 \Rightarrow 1 - dc = 0 \Rightarrow dc = 1$
$\Rightarrow |c| = 1 \Rightarrow c = \pm 1 \Rightarrow a = bc = \pm b$.
iii) $b = a\cdot a_1$, $c = b\cdot b_1 \Rightarrow c = (a\cdot a_1)b_1 = a\cdot(a_1 b_1)$.
iv) $b = a\cdot a'$, $c = a\cdot a'' \Rightarrow b + c = aa' + aa'' = a(a'+a'')$. □

Huom.: $\mathbb{Z}$:n relaatio $|$ on siis refl. ja transit., mutta ei (aivan) antisymm. $\mathbb{N}$:ssä vast. relaatio on myös antisymm., siis osittaisjärjestys.

Esim.: $1 \mid a \ \forall a \in \mathbb{Z}$; $a \mid 0 \ \forall a \in \mathbb{Z}$; $a \mid 1 \Leftrightarrow a = \pm 1$;
$b \mid 12 \Leftrightarrow b = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6$ tai ± 12.

Kun $a, b \in \mathbb{Z}$, yleensä $b \nmid a$ (jaksi ei mene "tasan").
Pätee kuitenkin

Lause 2 (jakoyhtälö): $a, b \in \mathbb{Z}$, $b \neq 0$
$\Rightarrow \exists$ 1-käs. $q, r \in \mathbb{Z}$ s.e. $0 \leq r < |b|$ ja

$$a = q \cdot b + r.$$

Tod.: olem.olo: Olk. ensin $b > 0$. Tark. joukkoa
$A = \{a - nb \mid n \in \mathbb{Z}\} \cap \mathbb{N} \subset \mathbb{N}$. $A \neq \emptyset$ ($a - nb \in A$, kun n riittävän pieni) $\Rightarrow \exists \ r = \min A$.
Tällöin $r \geq 0$ ja $r = a - qb$ eräälle $q \in \mathbb{Z}$.
Jos olisi $r \geq b$, niin $r - b = a - (q+1)b \in A$,
ja $r - b < r \Rightarrow r \neq \min A$, RR.
Siten $0 \leq r < b$ ja $a = qb + r$.
Olk. sitten $b < 0$. $-b > 0 \Rightarrow \exists q, r$ s.e.
$0 \leq r < -b$ ja $a = q(-b) + r \Rightarrow 0 \leq r < |b|$
ja $a = (-q) \cdot b + r$.

1-käsitteisyys: Ol. $a = qb + r = q'b + r'$, missä
$q, q', r, r' \in \mathbb{Z}$ ja $0 \leq r < |b|$, $0 \leq r' < |b|$.
Vastaol.: $q \neq q'$, ts. $|q - q'| \geq 1$
$\Rightarrow |b| = 1 \cdot |b| \leq |q - q'| \cdot |b| = |(q - q')b| = |r' - r|$,
toisaalta $-|b| < r' - r < |b|$, joten $|b| \leq |r' - r| < |b|$,
RR. $\therefore$ Täytyy olla $q = q'$, ja siis myös $r = r'$. □

Ol. $a, b \in \mathbb{Z}$, ainakin toinen $\neq 0$. Tark. a:n ja b:n positiivisia yhteisiä tekijöitä; niiden joukko on

$$Y = \{c \in \mathbb{N}_+ \mid c \mid a \text{ ja } c \mid b\}.$$

$Y \neq \emptyset$ (ainakin $1 \in Y$). Y:n suurin alkio (jos olemassa) on a:n ja b:n suurin yhteinen tekijä, merk. $syt(a, b)$. Jos $syt(a, b) = 1$, sanotaan, että

a ja b ovat keskenään jaottomat.

Lemma: Yo. tilanteessa $syt(a,b)$ on olemassa; se on joukon $\{xa+yb \mid x,y \in \mathbb{Z}\}$ pienin positiivinen luku.

Tod.: Merk. $A = \{xa+yb \mid x,y \in \mathbb{Z}\} \cap \mathbb{N}_+ \subset \mathbb{N}$.
$a \neq 0$ tai $b \neq 0 \Rightarrow A \neq \emptyset$; siis $\exists\, d = \min A$, $d \geq 1$ ja $d = ua + vb$ eräillä $u, v \in \mathbb{Z}$.
Jakoyhtälö $\Rightarrow a = qd + r$, $q, r \in \mathbb{Z}$, $0 \leq r < d$.
Jos $r > 0$, niin $r = a - qd = (1-qu)a + (-qv)b \in A$
$\Rightarrow d \neq \min A$, RR; siis $r = 0$ ja $d \mid a$.
Vastaavasti $d \mid b$. Siis $d \in Y$.
Toisaalta $c \in Y \Rightarrow c \geq 1$, ja $c \mid a$, $c \mid b$
$\Rightarrow c \mid (ua+vb) \Rightarrow c \mid d \Rightarrow d = cc'$ eräillä $c' \geq 1$
$\Rightarrow c \leq d$.
$\therefore$ d on Y:n pienin alkio, ts. $d = syt(a,b)$. □

Lause 3: Yo: luvuilla $d = syt(a,b)$ on seur. ominaisuudet:

a) $d \geq 1$ on a:n ja b:n yhteinen tekijä
i) d on jaollinen jokaisella a:n ja b:n yht. tekijällä
ii) $\exists\, u, v \in \mathbb{Z}$ s.e. $d = ua + vb$ (Bezout). □

Huom.: Esitys $d = ua + vb$ ei ole 1-käs.;
$(u+nb)a + (v-na)b = ua + vb \quad \forall n \in \mathbb{Z}$.

Seuraus: a ja b kesk. jaottomat $\Leftrightarrow$
$\exists\, u, v \in \mathbb{Z}$ s.e. $1 = ua + vb$.

Tod.: $\Rightarrow$ tod. yllä.
$\Leftarrow$ Ol. $1 = ua + vb$, $u, v \in \mathbb{Z}$. Olk. $d = syt(a,b)$
$\Rightarrow d \geq 1$ ja $d \mid a$, $d \mid b \Rightarrow d \mid (ua+vb) \Rightarrow d \mid 1$
$\Rightarrow d = 1$. □

Ol. $a, b \in \mathbb{Z}$, ainakin $b \neq 0$. $syt(a,b)$ löytyy Eukleideen algoritmilla, so. kirjoittamalla peräkk. jakoyhtälöitä:

$$a = q_1 b + r_1, \quad 0 < r_1 < |b|$$
$$b = q_2 r_1 + r_2, \quad 0 < r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2$$

$$r_{n-2} = q_n r_{n-1} + r_n \quad , \quad 0 < r_n < r_{n-1}$$
$$r_{n-1} = q_{n+1} r_n + 0$$

($r_0 = |b| > r_1 > r_2 > \dots \geq 0 \Rightarrow \exists$ (pienin) n s.e. $r_{n+1} = 0$).

V. Viimeinen poist. jakojäännös $r_n = \mathrm{syt}(a,b)$.

T. 1) Luetaan yhtälöt alhaalta ylös: $r_n \mid r_{n-1} \Rightarrow$
$r_n \mid (q_n r_{n-1} + r_n) = r_{n-2} \Rightarrow \dots \Rightarrow r_n \mid (q_2 r_1 + r_2) = b$
$\Rightarrow r_n \mid (q_1 b + r_1) = a \quad \therefore r_n \mid a$ ja $r_n \mid b$.

2) Ol. $c \mid a$ ja $c \mid d$. Luetaan yhtälöt ylhäältä alas:
$c \mid (a - q_1 b) = r_1 \Rightarrow c \mid (b - q_2 r_1) = r_2 \Rightarrow \dots \Rightarrow c \mid r_n$.
$\therefore d$ on s.y.l. □

Yo. jakoyhtälöiden avulla löydetään myös eräät $u_k, v_k \in \mathbb{Z}$, jolla $r_k = u_k a + v_k b$ $(1 \leq k \leq n)$. Nimittäin
$r_1 = a - q_1 b$, ja jos $r_{k-2} = u_{k-2} a + v_{k-2} b$ $(= |b|$, jos $k=2)$,
$r_{k-1} = u_{k-1} a + v_{k-1} b$ $(2 \leq k < n)$, niin

$$\begin{aligned} r_k &= r_{k-2} - q_k r_{k-1} \\ &= (u_{k-2} - q_k u_{k-1}) a + (v_{k-2} - q_k v_{k-1}) b . \end{aligned}$$

Esim. 3:
$$\begin{aligned} 657 &= 2 \cdot 306 + 45 \\ 306 &= 6 \cdot 45 + 36 \\ 45 &= 1 \cdot 36 + 9 \\ 36 &= 4 \cdot 9 + 0 \end{aligned} \Rightarrow \mathrm{syt}(306, 657) = 9.$$

$45 = 657 - 2 \cdot 306 \Rightarrow$
$36 = 306 - 6 \cdot 45 = 306 - 6 \cdot (657 - 2 \cdot 306)$
$= 13 \cdot 306 - 6 \cdot 657 \Rightarrow$
$9 = 45 - 36 = (657 - 2 \cdot 306) - (13 \cdot 306 - 6 \cdot 657)$
$= 7 \cdot 657 - 15 \cdot 306$.

Määr.: Kok. luku p on jaoton l. alkuluku, jos $p > 1$ ja p:n ainoat tekijät ovat ± 1 ja $\pm p$.

Lause 4: p alkuluku, $a, b \in \mathbb{Z}$, $p \mid ab$
$\Rightarrow p \mid a$ tai $p \mid b$.

Tod.: p alkuluku $\Rightarrow \mathrm{syt}(p, a) = 1$ tai p.
jos $\mathrm{syt}(p,a) = p$, niin $p \mid a$. Olk. nyt $\mathrm{syt}(p,a) = 1$

(ks. $p \nmid a$). Lause 3 $\Rightarrow$ $\exists u, v \in \mathbb{Z}$ s.e. $1 = up + va$

$\Rightarrow$ $b = 1 \cdot b = (up + va)b = (ub)p + v \cdot (ab)$.

Koska $p \mid ab$, tästä nähdyy, että $p \mid b$. $\square$

Huom.: Induktiolla saadaan: p alkuluku, $p \mid a_1 a_2 \cdots a_k$

$\Rightarrow$ $p \mid a_i$ jollakin $i \in \{1, 2, \ldots, k\}$.

(jos $k \geq 2$, niin $p \mid (a_1 \cdots a_{k-1}) \cdot a_k \overset{\text{Lause 4}}{\Rightarrow} p \mid a_1 \cdots a_{k-1}$ tai $p \mid a_k$; ind.ol. $\Rightarrow$ $p \mid a_i$ jollakin $i \in \{1, \ldots, k-1\}$ tai $p \mid a_k$.)

Lause 5 (Aritmetiikan perauslause): Jokainen luk. luku $n \geq 1$ voidaan esittää alkulukujen tulona eli muodossa

$$n = p_1 p_2 \cdots p_s \quad (p_i\text{:t alkulukuja})$$

tekijöiden p_i järjestystä vaille 1-käsitteisesti.

(Sopimus: $1 = 0$:n alkulukuinen "tyhjä" tulo (ts. $s = 0$).)

Tod.: Esityksen olem. alo: Tod. induktiolla luvuun $n \in \mathbb{N}_+$ sukeen väite "jokainen $k \in \mathbb{N}_+$, $k \leq n$, on alkulukujen tulo". Tapaus $n = 1$ on selvä.

Olk. $n > 1$. Ind. ol.: jokainen $k < n$ on alkulukujen tulo. Jos n on itse alkuluku, silloin on vaadittu esitys ($s = 1$). Muuten tap. n:llä on muitakin pos. tekijöitä kuin 1 ja n $\Rightarrow$ $n = n' \cdot n''$, missä $1 < n' < n$ ja $1 < n'' < n$. Ind. ol. $\Rightarrow$ $n' = p_1' \cdots p_{s'}'$, $n'' = p_1'' \cdots p_{s''}''$ alkulukujen tuloja $\Rightarrow$ $n = n' \cdot n'' = p_1' \cdots p_{s'}' \cdot p_1'' \cdots p_{s''}''$ alkul. tulo.

1-käsitteisyys: Ol. $p_1 \cdots p_s = q_1 \cdots q_r$, p_i:t ja q_j:t alkulukuja, $r, s \in \mathbb{N}$. Väit. ol. $s \leq r$.

jos $s = 0$, on $1 = q_1 \cdots q_r$. jos $s \geq 1$, niin $p_s \mid q_1 \cdots q_r \Rightarrow p_s \mid q_j$ eräällä j (Lause 4).

Vaihtamalla tekijöiden q_j järjestystä void. ol. $p_s \mid q_r$; p_s, q_r alkul. $\Rightarrow$ $p_s = q_r$. Supist. p_s:llä $\Rightarrow$ $p_1 \cdots p_{s-1} = q_1 \cdots q_{r-1}$. Jos $s - 1 \geq 1$, voidaan jatkaa. Saadaan: Kun $q_1, \ldots, q_r$ järj. sopivasti, on $p_s = q_r$, $p_{s-1} = q_{r-1}$, $\ldots$, $p_1 = q_{r-s+1}$ ja $1 = q_1 \cdots q_{r-s}$. $q_1, \ldots, q_{r-s}$ alkul. $\Rightarrow$ täytyy olla $r - s = 0$ eli $r = s$. $\square$

Yo. esitys $n = p_1 \cdots p_s$ on n:n alkutekijähajotelma. Se voidaan myös kirj. muodossa

$n = q_1^{h_1} \cdot q_2^{h_2} \cdot \ldots \cdot q_r^{h_r}$; $q_1, \ldots, q_r$ eri alkulukuja, $h_i \in \mathbb{N}$ $\forall i$.

Tässä $q_1^{h_1} \cdot q_2^{h_2} \cdot \ldots \cdot q_r^{h_r} = q_1^{k_1} \cdot q_2^{k_2} \cdot \ldots \cdot q_r^{k_r} \Leftrightarrow$ $h_i = k_i$ $\forall i$.

Huom.: Ol. $a = q_1^{h_1} \cdot \ldots \cdot q_r^{h_r}$, $b = q_1^{k_1} \cdot \ldots \cdot q_r^{k_r}$, missä $q_1, \ldots, q_r$ eri alkulukuja ja $h_i, k_i \in \mathbb{N}$ $\forall i$. Tällöin

$$\mathrm{syt}(a,b) = q_1^{n_1} \cdot \ldots \cdot q_r^{n_r}, \quad n_i = \min\{h_i, k_i\} \ \forall i.$$

Vastaavasti $c = q_1^{m_1} \cdot \ldots \cdot q_r^{m_r}$, $m_i = \max\{h_i, k_i\}$ $\forall i$ on a:n ja b:n pienin yhteinen jaettava, ts. $a \mid c$, $b \mid c$ ja c on pienin tällainen.

Esim. 4: $72 = 2^3 \cdot 3^2$, $60 = 2^2 \cdot 3 \cdot 5$
$\Rightarrow \mathrm{syt}(72,60) = 2^2 \cdot 3 = 12$, $\mathrm{pyj}(72,60) = 2^3 \cdot 3^2 \cdot 5 = 360$.

Huom.: $\mathrm{pyj}(a,b) \cdot \mathrm{syt}(a,b) = ab$.

Merk. $\mathbb{P}$ = alkulukujen joukko.

Lause 1 (Eukleides): $\mathbb{P}$ on ääretön.

Tod.: Vastaol.: $\mathbb{P} = \{p_1, \ldots, p_n\}$ äärellinen. Ainakin $2 \in \mathbb{P} \Rightarrow n \geq 1$. Merk. $x = p_1 \cdot \ldots \cdot p_n + 1 \in \mathbb{Z}$. $x > 1 \Rightarrow x$:llä on alkutekijöitä (Lause 5) $\Rightarrow$ $p_i \mid x$ eräällä $i \in \{1, \ldots, n\} \Rightarrow x = p_i \cdot y$ eräällä $y \in \mathbb{Z}$ $\Rightarrow$ $1 = x - p_1 \cdot \ldots \cdot p_n = p_i\left(y - \prod_{j \neq i} p_j\right)$, RR, koska $p_i \geq 2$. $\square$

Alkutekijähajotelman ehtiminen: Ol. $N \in \mathbb{Z}$, $N \geq 2$. Haluamme muodostaa N:n alkutekijähajotelman. Havainto: Jokin N on alkuluku tai jokin sen alkutekijä on $\leq \sqrt{N}$. Voidaan siis menetellä seuraavasti:

I. Luetteloidaan kaikki alkuluvut $p \leq \sqrt{N}$.
II. Onko N jaollinen jollakin alkuluvulla $p \leq \sqrt{N}$?
   ei $\Rightarrow$ N itse alkuluku, voidaan lopettaa
   kyllä $\Rightarrow$ $N = p \cdot N'$, $p \leq \sqrt{N}$ alkuluku; siirr. kohtaan III.
III. Korvataan N N':lla ja siirr. kohtaan II.

Kohta I vaic. suorittaa seur. menetelmälkä, ks.
Eratosteneen seulalla:

1. Listataan kaikki luvut $2, 3, 4, \ldots, M$.
2. Ympyröidään 2 ja pyyhitään yli monikerrat $4, 6, 8, \ldots$.
3. Ympyröidään pienin luku p, jota ei vielä ole ympyröity eikä ylipyyhitty, ja pyyhitään yli monikerrat $p \cdot p, (p+1) \cdot p, \ldots$ ($2p, 3p, \ldots, (p-1)p$ on jo ylipyyhitty).
4. Toistetaan kohtaa 3, kunnes kaikki listatut luvut on ympyröity tai ylipyyhitty.

Tulos: Alkuluvut $\leq M$ on ympyröity.

	(2)	(3)	4	(5)	6	(7)	8	9	10
(11)	12	(13)	14	15	16	(17)	18	(19)	20
21	22	(23)	24	25	26	27	28	(29)	30
(31)	32	33	34	35	36	(37)	38	39	40
(41)	42	(43)	44	45	46	(47)	48	49	50

$\therefore$ Alkuluvut ≤ 50 ovat $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$.

I.2 Kokonaisluvut modulo n.

Olk. $n \in \mathbb{Z}$, $n \geq 1$, kiinteä. Merk. $n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid n \mid x\} \subset \mathbb{Z}$. Tällöin $0 = n \cdot 0 \in n\mathbb{Z}$, $x, y \in n\mathbb{Z} \Rightarrow x + y \in n\mathbb{Z}$, ja $x \in n\mathbb{Z}, a \in \mathbb{Z} \Rightarrow xa \in n\mathbb{Z}$.

Lemma: $\mathbb{Z}$:n relaatio $a \equiv_n b \iff a - b \in n\mathbb{Z}$ on ekvivalenssi. Kaikilla $a, a', b, b' \in \mathbb{Z}$ on

$$a \equiv_n a',\ b \equiv_n b' \Rightarrow a + b \equiv_n a' + b',\ ab \equiv_n a'b'.$$

Tod.: Refl.: $a \equiv_n a$, koska $a - a = 0 \in n\mathbb{Z}$.
Symm.: $a \equiv_n b \Rightarrow a - b \in n\mathbb{Z}$
$\Rightarrow b - a = (a - b) \cdot (-1) \in n\mathbb{Z} \Rightarrow b \equiv_n a$.
Transit.: $a \equiv_n b,\ b \equiv_n c \Rightarrow a - b \in n\mathbb{Z},\ b - c \in n\mathbb{Z}$
$\Rightarrow a - c = (a - b) + (b - c) \in n\mathbb{Z}$.