# Aritmetiikan peruslause

Yhdistetty luku $n$ voidaan aina hajottaa muotoon

$$n = n_1 n_2, \qquad 1 < n_1 < n, \quad 1 < n_2 < n.$$

Jatkamalla tässä tekijöiden $n_1$ ja $n_2$ hajottamista (jos mahdollista) saadaan lopuksi luvulle $n$ *alkutekijähajotelma*:

$$n = p_1 p_2 \cdots p_k \qquad (p_1, p_2, \ldots, p_k \text{ ovat alkulukuja}).$$

Alkutekijähajotelma voidaan kirjoittaa myös muodossa

$$n = q_1^{h_1} q_2^{h_2} \cdots q_s^{h_s} \qquad (q_1, \ldots q_s \text{ ovat erisuuria alkulukuja, } h_i \geq 1 \ \forall i).$$

Tätä muotoa sanotaan luvun *kanoniseksi (alkutekijä)hajotelmaksi*.

**Esimerkki.** $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 5 = 2^2 \cdot 3 \cdot 5^3$.

**Lause.** Olkoot $a$ ja $b$ suhteellisia alkulukuja, toisin sanoen $\text{syt}(a,b) = 1$. Jos $a \mid bc$, niin $a \mid c$.

*Todistus.* Tiedämme, että lukujen $a$ ja $b$ suurin yhteinen tekijä voidaan esittää muodossa $1 = ua + vb$, joillakin kokonaisluvuilla $u$ ja $v$. Nyt $c = c \cdot 1 = c(ua + vb) = uac + vbc$. Koska $a \mid uac$ ja oletuksen nojalla $a \mid bc$, niin $a \mid (uac + vbc)$ eli $a \mid c$. □

**Lause.** Olkoon $p$ alkuluku. Jos $p \mid a_1 \cdots a_k$ $(a_i \in \mathbb{Z})$, niin $p$ jakaa jonkin luvuista $a_i$.

*Todistus.* Jos $p \mid a_1$, niin väite on todistettu. Oletetaan, että $p \nmid a_1$, silloin $p$ ja $a_1$ ovat suhteellisia alkulukuja. Koska $p \mid a_1(a_2 \cdots a_k)$ niin edellisen lauseen nojalla $p \mid a_2 \cdots a_k$. Toistamalla argumenttia ensin lukuun $a_2$ ja sen jälkeen niin pitkälle kuin on tarve löydetään lopulta luku $a_i$, jonka $p$ jakaa. □

Kahden edellisen lauseen avulla voidaan todistaa seuraava **aritmetiikan peruslause**.

**Lause.** Jokainen kokonaisluku $n > 1$ voidaan esittää alkulukujen tulona eli muodossa

$$n = p_1 p_2 \cdots p_t \qquad (p_i \in \mathbb{P},\ 1 \leq i \leq t)$$

tekijöiden $p_i$ järjestystä vaille yksikäsitteisesti.

*Todistus.* Alkutekijähajotelman olemassaolo perusteltiin sivun alussa. Todistetaan vielä, että kyseinen hajotelma on yksikäsitteinen. Tehdään vastaoletus, että luvulle $n$ olisi kaksi esitystä $n = p_1 p_2 \cdots p_t$ ja $n = q_1 q_2 \cdots q_r$, missä kaikki luvut $p_i$ ja $q_i$ ovat alkulukuja. Silloin $p_1 \mid q_1 q_2 \cdots q_r$, joten edellisen lauseen nojalla $p_1$ jakaa jonkin luvuista $q_i$. Voidaan olettaa, että $p_1 \mid q_1$. Koska molemmat luvut ovat alkulukuja on $p_1 = q_1$. Tämän jälkeen jää tarkasteltavaksi yhtälö

$$p_2 \cdots p_t = q_2 \cdots q_r.$$

Jatkamalla samoin saadaan $p_2 = q_2, \ldots, p_t = q_r$ (ja $r = t$). □

On luonnollista sopia, että luvulla 1 on esitys "tyhjänä" alkulukutulona (siis $t = 0$). Negatiivisilla kokonaisluvuilla on yksikäsitteinen esitys muodossa $-p_1 p_2 \cdots p_t$.

Kahden luvun $a$ ja $b$ suurin yhteinen tekijä voidaan laskea määrittämällä ensin lukujen kanoniset hajotelmat. Jos $a$ ja $b$ ovat suuria on Eukleideen algoritmi kuitenkin nopeampi menetelmä.

---

**Linkit**:
Jaollisuus ja alkuluvut
Jakoalgoritmi
Suurin yhteinen tekijä
Eukleideen algoritmi