Suurin yhteinen tekijä

Kahdella kokonaisluvulla a ja b on aina vähintään yksi yhteinen positiivinen tekijä, nimittäin 1.

Määritelmä. Olkoot a ja b kokonaislukuja, joista ainakin toinen on nollasta eroava. Lukujen a ja b *suurin yhteinen tekijä*, $\text{syt}(a,b)$, on luku d, joka määritellään seuraavasti:

(a) $d > 0$,

(b) $d \mid a$ ja $d \mid b$,

(c) jos $c \mid a$ ja $c \mid b$, niin $c \mid d$.

Luku $\text{syt}(a,b)$ on siis lukujen a ja b yhteisistä tekijöistä suurin.

Jos lukujen a ja b suurin yhteinen tekijä on 1 sanotaan, että luvut a ja b ovat *suhteellisia alkulukuja*.

Lause. Jos a ja b eivät molemmat ole nollia, niin $\text{syt}(a,b)$ on olemassa ja se on yksikäsitteinen. Lisäksi on olemassa sellaiset kokonaisluvut u ja v, että

$$\text{syt}(a,b) = ua + vb$$

Todistus. Todistetaan, että $\text{syt}(a,b)$ on joukon $A = \{xa + yb \mid x,y \in \mathbb{Z}\}$ pienin positiivinen luku, tämä todistaa lauseen väitteet.

Koska luvut a ja b eivät ole molemmat nollia, on joukossa A selvästi nollasta eroavia alkioita. Todetaan lisäksi, että joukossa A on positiivisia alkioita. Jos $x \in A$ ja $x < 0$, niin $x = x_0a + y_0b$ joillekin luvuille x_0 ja y_0. Silloin $-x = (-x_0)a + (-y_0)b$ on joukon A positiivinen luku.

Oletetaan, että joukon A pienin positiivinen luku on $d = ua + vb$. Näytetään ensin, että $d \mid a$. Jakoalgoritmia käyttäen saadaan

$$a = qd + r, \qquad \text{missä } 0 \leq r < d.$$

Tästä saadaan

$$r = a - qd = a - q(ua + vb) = (1 - qu)a + (-qv)b.$$

Näin ollen r kuuluu joukkoon A. Luvun d minimaalisuudesta johtuen on $r = 0$, siis $d \mid a$.

Samoin nähdään, että $d|b$; siis d on lukujen a ja b yhteinen tekijä. Jos myös c on näiden yhteinen tekijä, niin $c \mid (ua + vb)$ eli c jakaa luvun d. Koska $d > 0$, niin $c \leq d$, ja siis $d = \text{syt}(a,b)$. □

Huomaa, että edellisen lauseen luvut u ja v eivät ole yksikäsitteisiä. Esimerkiksi $\text{syt}(4,6) = 2 = 2 \cdot 4 - 1 \cdot 6 = (-1) \cdot 4 + 1 \cdot 6$.

Linkit:
Jaollisuus ja alkuluvut
Jakoalgoritmi
Eukleideen algoritmi