Eukleideen algoritmi

Kahden kokonaisluvun a ja b, joista molemmat eivät ole nollia, suurin yhteinen tekijä $\text{syt}(a,b)$ saadaan lasketuksi *Eukleideen algoritmilla*. Siinä sovelletaan jakoalgoritmia toistuvasti. Oletetaan nyt, että $b \neq 0$.

$$\begin{array}{rcll} a & = & q_1 b + r_1, & 0 < r_1 < |b| \\ b & = & q_2 r_1 + r_2, & 0 < r_2 < |r_1| \\ r_1 & = & q_3 r_2 + r_3, & 0 < r_3 < |r_2| \\ & \vdots & & \vdots \\ r_{n-2} & = & q_n r_{n-1} + r_n, & 0 < r_n < |r_{n-1}| \\ r_{n-1} & = & q_{n+1} r_n (+0). & \end{array}$$

Jakaminen päättyy, koska jakojäännökset muodostavat aidosti vähenevän jonon positiivisia kokonaislukuja. Osoitetaan, että viimeinen jakojäännös r_n (> 0) on haettu suurin yhteinen tekijä:

$$r_n = \text{syt}(a,b).$$

Koska $r_n \mid r_{n-1}$, niin viimeistä edellisen yhtälön mukaan myös $r_n \mid r_{n-2}$. Jatkamalla yhtälöketjussa ylöspäin nähdään, että $r_n \mid a$ ja $r_n \mid b$. Jos luvuilla a ja b on yhteinen tekijä c, niin ensimmäisen yhtälön mukaan $c \mid r_1$, vastaavasti toisen yhtälön mukaan $c \mid r_2$. Jatkamalla näin loppuun saakka nähdään, että $c \mid r_n$. Täten luku r_n on lukujen a ja b yhteisistä tekijöistä suurin.

Eukleideen algoritmi antaa myös eräät sellaiset luvut u ja v, joilla $r_n = ua + vb$. Näiden lukujen löytämiseksi käydään yhtälöketjua lävitse alhaalta ylöspäin samalla sijoittaen eliminoiden luvut $r_{n-1}, r_{n-2}, \ldots, r_2, r_1$.

Linkit:
Jaollisuus ja alkuluvut

Jakoalgoritmi

Suurin yhteinen tekijä