Jakoalgoritmi

Mistä tiedetään onko annettu (suuri) luku N alkuluku? Entä jos luku ei ole alkuluku, miten löydetään sen tekijät? Alkeellinen menetelmä sen ratkaisemiseksi onko luku a jaollinen luvulla b on jakoalgoritmi eli jaon suorittaminen jakokulmassa. Seuraava lause koskee jaon tulosta.

Lause. (Jakoalgoritmi) Jos $a, b \in \mathbb{Z}$ ja $b \neq 0$, niin on olemassa sellaiset yksikäsitteiset kokonaisluvut q ja r, että

$$a = qb + r, \qquad 0 \leq r < |b|.$$

Todistus. Jos $b > 0$, valitaan joukosta $\{a - nb \mid n \in \mathbb{Z}\}$ pienin ei-negatiivinen kokonaisluku $r = a - qb$. Silloin $r < b$, sillä muuten $a - (q+1)b$ olisi vielä pienempi ei-negatiivinen kokonaisluku.

Tapaus $b < 0$ palautetaan edelliseen korvaamalla b luvulla $-b$:

$$a = q(-b) + r = (-q)b + r, \qquad 0 \leq r < -b = |b|.$$

Todistetaan vielä, että luvut q ja r ovat yksikäsitteiset. Oletetaan, että q' ja r' olisivat toiset sellaiset luvut, joille

$$a = q'b + r' \qquad 0 \leq r' < |b|.$$

Silloin $a = q'b + r' = qb + r$, josta saadaan $r - r' = (q' - q)b$. Koska $0 \leq r, r' < |b|$, niin $-|b| < r - r' < |b|$. Siis $0 \leq |r - r'| < |b|$ ja toisaalta $|r - r'| = |q' - q||b|$, joten välttämättä $|r - r'| = 0$, toisin sanoen $r = r'$ ja täten myös $q = q'$. □

Esimerkki. $30 = 4 \cdot 7 + 2, \qquad 17 = (-2)(-7) + 3, \qquad -11 = (-3) \cdot 5 + 4.$

Linkit:
Jaollisuus ja alkuluvut