Eukleideen algoritmi

Suurten lukujen jakaminen alkutekijöihin osoittautuu melko työlääksi, varsinkin, jos yli 31:n alkulukuja. Myös s.y.t.:n määrittäminen edellisen seurauksena vie aikaa. Onneksi on Eukleideen algoritmi

Lause, Eukleideen algoritmi:
Kahden positiivisen luvun a ja b s.y.t. voidaan määrittää *Eukleideen algoritmilla* seuraavasti: Jaetaan ensin suurempi luku pienemmällä. Jos jää jakojäännös, niin jaetaan sillä jakaja (eli pienempi luku). Näin jatketaan, eli jaetaan jakojäännöksellä aina jakaja, kunnes jako menee tasan. Viimeinen jakaja on kysytty s.y.t.

Huomautus p.y.m. saadaan sitten jakamalla tulo ab s.y.t.:llä.

Esimerkki 1 Määritä $\text{syt}(84,120)$

$$120 = 84 \cdot 1 + 36$$
$$84 = 36 \cdot 2 + 12$$
$$36 = 12 \cdot 3 + 0$$

Eukleideen algoritmilla, tiedetään, että

$$\text{syt}(84,120) = 12.$$

Esimerkki 2 Määritä $\text{syt}(507,832)$.

$$832 = 507 \cdot 1 + 325$$
$$507 = 325 \cdot 1 + 182$$
$$325 = 182 \cdot 1 + 143$$
$$182 = 143 \cdot 1 + 39$$
$$143 = 39 \cdot 3 + 26$$
$$39 = 26 \cdot 1 + 13$$
$$26 = 13 \cdot 2 + 0$$

Nyt varsinainen hyöty nähdään selvemmin. Siis

$$\text{syt}(507,832) = 13.$$

Esimerkki 3 Määritä $\text{syt}(234, 584, 819)$.

Kolmen tai useamman luvun tapauksessa määritetään ensin kahden luvun syt ja sitten määritetään saadusta s.y.t.:stä ja seuraavasta luvusta s.y.t.

$$584 = 234 \cdot 2 + 116$$
$$234 = 116 \cdot 2 + 2$$
$$116 = 2 \cdot 58 + 0$$

$\longrightarrow$

$$819 = 2 \cdot 409 + 1$$
$$2 = 1 \cdot 2 + 0$$

Siis

$$\text{syt}(234, 584, 819) = 1.$$

Tulos kertoo, että kyseisillä luvuilla ei ole (siis kaikilla) yhteistä tekijää kuin ykkönen. ($234 = 2 \cdot 3^2 \cdot 13$, $584 = 2^3 \cdot 73$ ja $819 = 3^2 \cdot 7 \cdot 13$).

Eukleideen algoritmi antaa s.y.t.:n lisäksi myös keinon esittää s.y.t. lukujen a ja b lausekkeena eli lineaarikombinaationa.

Lause, s.y.t.:n lauseke eli lineaarikombinaatio:
Olkoon $a, b \neq 0$. Tällöin on olemassa sellaiset x ja y, että

$$\text{syt}(a, b) = ax + by.$$

Tarkastellaan jälleen lukuja 84 ja 120.
Näille $\text{syt}(84,120) = 12$, joka saatiin Eukleideen algoritmista.

$$120 = 84 \cdot 1 + 36$$
$$84 = 36 \cdot 2 + 12$$
$$36 = 12 \cdot 3 + 0$$

Ideana on kulkea nyt takaisin tuloksesta lukuihin 120 ja 84. Siis

$$\begin{aligned}\text{syt}(84,120) &= 12 \\ &= 84 - 36 \cdot 2 \\ &= 84 - (120 - 84 \cdot 1) \cdot 2\end{aligned}$$

Siis $\text{syt}(84,120) = 12 = 3 \cdot 84 - 2 \cdot 120$. Siis $x = 3$ ja $y = -2$.

Vaihtoehtoinen tapa on kirjoittaa Eukleideen algoritmin yhtälöt ratkaistuun muotoon, eli $12 = 84 - 36 \cdot 2$, $36 = 120 - 84 \cdot 1$ ja sitten sijoittaa, $12 = 84 - (120 - 84) \cdot 2 = 3 \cdot 84 - 2 \cdot 120$.

Esimerkki 2 Määritä $\text{syt}(365, 51)$ ja esitä se muodossa $365x + 51y$.

$\text{syt}(365, 51) = 1$, ja sanotaan, että ne ovat *keskenään jaottomia*. Lisäksi puhutaan, että luvut 365 ja 51 ovat *suhteellisia alkulukuja* (keskenään).

$$365 = 51 \cdot 7 + 8$$
$$51 = 8 \cdot 6 + 3$$
$$8 = 3 \cdot 2 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

Edelleen

$$\begin{aligned}1 &= 3 - 2 \\ &= 3 - (8 - 3 \cdot 2) = -8 + 3 \cdot 3 \\ &= -8 + (51 - 8 \cdot 6) \cdot 3 = 3 \cdot 51 - 19 \cdot 8 \\ &= 3 \cdot 51 - 19 \cdot (365 - 51 \cdot 7) = -19 \cdot 365 + 136 \cdot 51\end{aligned}$$

Siis

$$\text{syt}(365, 51) = 1 = 365 \cdot \underbrace{(-19)}_{=x} + 51 \cdot \underbrace{136}_{=y}.$$