Diofantoksen yhtälö

Diofantoksen yhtälö on yhtälö, jolle etsitään kokonaislukuratkaisua. Lineaarisen kahden tuntemattoman Diofantoksen yhtälön $ax+my=c$ (luvut a,m ja c ovat tunnettuja) ratkaiseminen on ekvivalenttia kongruenssin

$$ax \equiv c \pmod{m}$$

ratkaisemisen kanssa. Seuraavaksi todistetaan tätä kongruenssia koskeva tulos.

Lause. Jos $\text{syt}(a,m)=1$, kongruensilla $ax \equiv c \pmod{m}$ on yksikäsitteinen ratkaisu $x \in \mathbb{Z}$ välillä $0 \leq x \leq m-1$.

Todistus. Oletuksen $\text{syt}(a,m)=1$ nojalla on olemassa sellaiset luvut u ja v, että $au+mv=1$. Täten $a(uc)+m(vc)=c$ ja kongruenssin $ax \equiv c \pmod{m}$ yksi ratkaisu on $x=uc$. Lisäksi kongruenssin kaikki ratkaisut ovat keskenään kongruentteja. Nimittäin, jos x_1 ja x_2 ovat kongruenssin kaksi eri ratkaisua, niin $ax_1 \equiv ax_2 \pmod{m}$. Sivulla Kongruenssi olevan lauseen kohdan (ii) mukaan tästä seuraa, että $x_1 \equiv x_2 \pmod{m}$. Ratkaisuista on siis tarkalleen yksi halutulla välillä. □

Linkit:
Suurin yhteinen tekijä

Kongruenssi

Esimerkki Diofantoksen yhtälön ja kongruenssin käytöstä