Jaollisuus ja alkuluvut

Kokonaislukujen joukko on $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

Jos kokonaisluku a on jaollinen kokonaisluvulla b, toisin sanoen on olemassa sellainen kokonaisluku c, että $a = bc$, merkitään $b \mid a$. Tällöin sanotaan, että b *jakaa* luvun a, b on luvun a *tekijä* tai a on luvun b *monikerta*. Jos a ei ole luvun b monikerta merkitään $b \nmid a$.

Esimerkki. $2 \mid 10$, $(-3) \mid 9$, $5 \nmid 11$.

Jaollisuudella on seuraavat yksinkertaiset ominaisuudet:

(a) $1 \mid a \; \forall \; a \in \mathbb{Z}$

(b) $a \mid a \; \forall a \in \mathbb{Z}$

(c) jos $a \mid b$ ja $b \mid a$, niin $a = \pm b$

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

(e) jos $a \mid b$ ja $a \mid c$, niin $a \mid (ub + vc)$ kaikilla $u, v \in \mathbb{Z}$

Todistetaan kohta (e) ja jätetään muiden kohtien miettiminen harjoitukseksi. Oletetaan, että $a \mid b$ ja $a \mid c$, silloin on olemassa sellaiset luvut r ja s, että $ub + vc = u(ar) + v(as) = a(ur + vs)$, joten $a \mid (ub + vc)$.

Määritelmä. Kokonaislukua $p > 1$, jonka ainoat tekijät ovat ± 1 ja $\pm p$, sanotaan *alkuluvuksi*. Muita kokonaislukuja sanotaan *yhdistetyiksi* luvuiksi.

Alkulukujen joukosta käytetään merkintää $\mathbb{P}$, siis

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots\}.$$

Lause. Alkulukuja on äärettömän monta.

Todistus. Tehdään vastaoletus, että $p_1, \ldots, p_k$ ovat kaikki alkuluvut. Muodostetaan luku $n = p_1 p_2 \cdots p_k + 1$. Koska alkulukuja ylipäänsä on olemassa, on $n > 1$ ja täten se voidaan hajottaa tekijöihin. On siis olemassa sellainen alkuluku q, että $q \mid n$. Koska $p_1, \ldots, p_k$ ovat kaikki alkuluvut, niin voidaan olettaa, että $q = p_i$. On olemassa sellainen kokonaisluku c, että $p_1 \cdots p_k + 1 = cp_i$, siis $1 = p_i(c - p_1 \cdots p_{i-1} p_{i+1} \cdots p_k)$. Koska $c - p_1 \cdots p_{i-1} p_{i+1} \cdots p_k \in \mathbb{Z}$ niin $p_i \mid 1$, mikä on mahdotonta, sillä p_i on alkuluku. □

Linkit:
Jakoalgoritmi