Lukuteoria 1
Harjoitusten 1 ratkaisuehdotuksia

1. Osoita induktiolla, että

$$\sum_{j=0}^{n} j = \frac{n(n+1)}{2}.$$

Ratkaisu. *Alkuaskel:* Koska

$$\sum_{j=0}^{0} j = 0 = \frac{0(0+1)}{2},$$

väite pätee tapauksessa $n = 0$.
Induktio-oletus: Luvulle $k \in \mathbb{Z}$ pätee $\sum_{j=0}^{k} j = \frac{k(k+1)}{2}$.
Induktioväite: Induktio-oletuksen nojalla saadaan

$$\begin{aligned}\sum_{j=0}^{k+1} j &= \left(\sum_{j=0}^{k} j\right) + (k+1) = \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}.\end{aligned}$$

Induktioväite on todistettu, joten induktiotodistus on valmis.

2. Olkoot $a, b, c \in \mathbb{Z}$. Ovatko seuraavat väitteet totta? Todista tai keksi vastaesimerkki.
(a) Jos $a \mid c$ ja $b \mid c$, niin $ab \mid c$.
(b) Jos $a \mid bc$, niin $a \mid c$.

Ratkaisu. (a) Väite ei pidä paikkaansa. Jos esimerkiksi $a = b = c = 2$, niin $a \mid c$ ja $b \mid c$, mutta $ab \nmid c$.
(b) Väite ei pidä paikkaansa. Jos esimerkiksi $a = 4$ ja $b = c = 2$, niin $a \mid bc$, mutta $a \nmid c$.

3. Olkoot $a, b, c, d \in \mathbb{Z}$. Ovatko seuraavat väitteet totta? Todista tai keksi vastaesimerkki.
(a) Jos $a \mid c$ ja $b \mid d$, niin $(a+b) \mid (c+d)$.
(b) Jos $a \mid c$ ja $b \mid d$, niin $ab \mid cd$.

Ratkaisu. (a) Väite ei pidä paikkaansa. Jos esimerkiksi $a = c = 2$, $b = 3$ ja $d = 6$, niin $a \mid c$ ja $b \mid d$, mutta $(a+b) \nmid (c+d)$.
(b) Todistetaan, että väite pitää paikkaansa. Koska $a \mid c$, pätee $c = ka$ jollakin $k \in \mathbb{Z}$. Samoin pätee $d = lb$ jollakin $l \in \mathbb{Z}$. Saadaan

$$cd = (ka)(lb) = (kl)(ab),$$

missä $kl \in \mathbb{Z}$. Jaollisuuden määritelmän nojalla $ab \mid cd$.

4. Tässä tehtävässä osoitetaan Propositio 2.1.4. Olkoot $a, b, c, m, n \in \mathbb{Z}$. Osoita, että
(a) jos $a \mid b$ ja $b \mid c$, niin $a \mid c$. (transitiivisuus)
(b) jos $a \mid b$ ja $a \mid c$, niin $a \mid (mb + nc)$. (lineaarisuus)

Ratkaisu. (a) Koska $a \mid b$, pätee $b = ka$ jollakin $k \in \mathbb{Z}$, ja koska $b \mid c$, pätee $c = lb$ jollakin $l \in \mathbb{Z}$. Saadaan

$$c = lb = l(ka) = (lk)a,$$

missä $lk \in \mathbb{Z}$. Jaollisuuden määritelmän nojalla $a \mid c$.

(b) Koska $a \mid b$ ja $a \mid c$, pätee $b = ka$ ja $c = la$ joillakin $k, l \in \mathbb{Z}$. Saadaan

$$mb + nc = m(ka) + n(la) = (mk + nl)a,$$

missä $(mk + nl) \in \mathbb{Z}$. Jaollisuuden määritelmän nojalla $a \mid (mb + nc)$.

5. Osoita seuraavat väitteet:

(a) Kahden parillisen luvun summa on parillinen.
(b) Parillisen ja parittoman luvun summa on pariton.
(c) Kahden parittoman luvun summa on parillinen.

Ratkaisu. Olkoot $a, b \in \mathbb{Z}$ parillisia ja $c, d \in \mathbb{Z}$ parittomia. Tällöin on sellaiset luvut $k_1, k_2, k_3, k_4 \in \mathbb{Z}$ että

$$a = 2k_1, \quad b = 2k_2, \quad c = 2k_3 + 1, \quad d = 2k_4 + 1.$$

Osoitetaan nyt tehtävän väitteet:

(a) $a+b = 2k_1+2k_2 = 2(k_1+k_2)$, missä $(k_1+k_2) \in \mathbb{Z}$. Siis $a+b$ on parillinen.
(b) $a + c = 2k_1 + (2k_3 + 1) = 2(k_1 + k_3) + 1$, missä $(k_1 + k_3) \in \mathbb{Z}$. Siis $a + c$ on pariton.
(c) $c + d = (2k_3 + 1) + (2k_4 + 1) = 2(k_3 + k_4 + 1)$, missä $(k_3 + k_4 + 1) \in \mathbb{Z}$. Siis $c + d$ on parillinen.

6. Osoita seuraavat väitteet:

(a) Jos $a \in \mathbb{Z}$ ja a^2 on parillinen, niin a on parillinen.
(b) Jos $a, b \in \mathbb{Z}$ ja luku ab on pariton, niin sekä a että b ovat parittomia.

Ratkaisu.

(a) Jakojäännöslauseen nojalla luku a on joko parillinen tai pariton. Jos se olisi pariton, olisi sellainen $k \in \mathbb{Z}$ että $a = 2k + 1$. Tällöin olisi

$$a^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1,$$

missä $(2k^2 + 2k) \in \mathbb{Z}$, eli a^2 olisi pariton, mikä on vastoin oletusta. Siis a ei voi olla pariton, joten se on parillinen.

(b) Jos a olisi parillinen, olisi $a = 2k$ jollakin $k \in \mathbb{Z}$. Tällöin olisi $ab = 2(kb)$, missä $kb \in \mathbb{Z}$. Siis ab olisi parillinen, mikä on vastoin oletusta. Siis a on pariton.
Jos b olisi parillinen, olisi $b = 2l$ jollakin $l \in \mathbb{Z}$, jolloin $ab = 2(al)$ olisi parillinen, mikä on taas vastoin oletusta. Siis myös b on pariton.

7. Olkoot a, b, c parittomia kokonaislukuja. Osoita, että yhtälöllä

$$ax^2 + bx + c = 0$$

ei ole ratkaisua rationaalilukujen joukossa.

Ratkaisu. Tehdään vastaoletus, että on luku $x_0 \in \mathbb{Q}$ joka toteuttaa yhtälön. Tällöin $x_0 = \frac{m}{n}$ joillekin kokonaisluvuille m, n, $n \neq 0$. Voidaan olettaa, että vähintään toinen luvuista m, n on pariton, koska jos molemmat olisivat parillisia, voitaisiin supistaa kakkosella niin kauan että vähintään toinen on pariton.

Kertomalla yhtälö $ax_0^2 + bx_0 + c = 0$ puolittain luvulla n^2 saadaan yhtälö

$$am^2 + bmn + cn^2 = 0.$$

Tavoitteena on osoittaa, että luku $am^2 + bmn + cn^2$ on pariton. Tällöin pääsemme ristiriitaan, sillä luku 0 on parillinen.

Luvut m ja n valittiin niin, että vähintään toinen niistä on pariton. Meillä on siis kolme vaihtoehtoa:

(a) Luvut m ja n ovat parittomia.
(b) Luku m on parillinen ja n on pariton.
(c) Luku m on pariton ja n on parillinen.

Tarkastellaan ensi vaihtoehtoa (a). Tällöin luvut $am^2 = amm$, bmn ja $cn^2 = cnn$ ovat kaikki kolmen parittoman luvun tuloja. Kolmen parittoman luvun tulo on pariton, joten luku $am^2 + bmn + cn^2$ on kolmen parittoman luvun summana pariton.

Tarkastellaan seuraavaksi vaihtoehtoa (b). Tässä tapauksessa luvut am^2 ja bmn ovat parillisia ja cn^2 on pariton, joten luku $am^2 + bmn + cn^2$ on kahden parillisen ja yhden parittoman luvun summana pariton.

Vaihtoehto (c) on samanlainen kuin vaihtoehto (b): Nyt luvut bmn ja cn^2 ovat parillisia ja am^2 on pariton, joten tässäkin tapauksessa luku $am^2 + bmn + cn^2$ on pariton.

Olemme päätelleet, että luku $am^2 + bmn + cn^2$ on pariton. Tämä on ristiriidassa vastaoletuksesta seuraavan yhtälön $am^2 + bmn + cn^2 = 0$ kanssa. Siis vastaoletus on väärin. Olemme todistaneet väitteen.