Approbatur 3, demo 2, ratkaisut

Sovitaan, että 0 ei ole luonnollinen luku. Tällöin oletusta $n \neq 0$ ei tarvitse toistaa alla olevissa ratkaisuissa. Se, pidetäänkö nollaa luonnollisena lukuna vai ei, vaihtelee paljon kursseittain ja matematiikan osa-alueittain. Tästä vaihtelevuudesta ei kuitenkaan yleensä koidu ongelmia, kunhan muistaa kirjoittaa näkyville, mikä on valinta kyseessä olevassa kontekstissa.

Merkitään lausumaa "a jakaa b:n" symbolilla $a \mid b$. Tämän voi myös tulkita: "b on a:n monikerta" tai "a on b:n tekijä".

2.1. Tehtävänä on osoittaa induktiolla, että kaikille $n \in \mathbb{N}$ pätee

$$1 + 2 + 3 + \ldots + n = \frac{1}{2}n(n+1)\,. \tag{1}$$

Induktion alkuaskeleessa on osoitettava ehto (1) todeksi, kun $n = 1$. Tällöinhän väite on muotoa

$$1 = \frac{1}{2} \cdot 1(1+1)\,.$$

Tämä nähdään suoraan laskemalla todeksi, sillä $\frac{1}{2} \cdot 1(1+1) = 1$.

Tehdään sitten induktio-oletus eli oletetaan, että $n \geq 1$ ja että ehto (1) pätee n:lle. On osoitettava, että se pätee myös $n+1$:lle eli, että on voimassa

$$1 + 2 + 3 + \ldots + n + (n+1) = \frac{1}{2}(n+1)((n+1)+1)$$

eli, että (kun tuon oikean puolen sulkulausekkeen avaa)

$$1 + 2 + 3 + \ldots + n + (n+1) = \frac{1}{2}(n+1)(n+2) = \frac{1}{2}(n^2 + 3n + 2)\,. \tag{2}$$

Näin se käy:

$$\begin{aligned} 1 + 2 + 3 + \ldots + n + (n+1) &\overset{a)}{=} \frac{1}{2}n(n+1) + n + 1 = \frac{1}{2}n^2 + \frac{1}{2}n + n + 1 \\ &= \frac{1}{2}n^2 + \frac{3}{2}n + 1 = \frac{1}{2}(n^2 + 3n + 2)\,, \end{aligned}$$

joten ehto (2) pätee ja induktioaskel on valmis. Yllä yhtälössä a) on käytetty induktio-oletusta summaan $1 + 2 + 3 + \ldots + n$. □

Yksi tapa "todistaa" summakaava (1) ilman induktiota on tulkita summa n-kertaiseksi ensimmäisen ja viimeisen summattavan keskiarvoksi.

2.2. Oletetaan, että olet juhlissa, joissa on $n+1$, $n \in \mathbb{N}$, osanottajaa. Oletetaan lisäksi, että jokainen vieraista kättelee toisensa kerran. Kysymys kuuluu, montako kättelyä tuli kaiken kaikkiaan tehtyä.

Juhlien osanottajat voidaan numeroida; olkoon siis osanottajien joukko $A = \{1, 2, \ldots, n, n+1\}$. Kättelytapahtuma voidaan tulkita A:n kahden alkion osajoukkona – esimerkiksi $\{1, 2\}$ vastaa tilannetta, jossa henkilö 1 kättelee henkilöä 2. Luonnollisesti $\{1, 2\} = \{2, 1\}$, eli jos henkilö 1 kättelee henkilön 2, niin tulkitaan, että samalla henkilö 2 kättelee henkilön 1. Näillä määrittelyillä tehtävän kysymys kuuluukin, montako kahden alkion osajoukkoa joukon A alkioista voidaan muodostaa. Tähän vastauksen antaa binomikerroin $\binom{n+1}{2}$, jonka arvo on

$$\begin{aligned}\binom{n+1}{2} &= \frac{(n+1)!}{2!(n+1-2)!} = \frac{(n+1)!}{2(n-1)!} \\ &= \frac{1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n \cdot (n+1)}{2 \cdot 1 \cdot 2 \cdot \ldots \cdot (n-1)} \\ &= \frac{1}{2} n(n+1)\,.\end{aligned}$$

Tämähän on sama tulos kuin ykköstehtävän summakaavassa, ja progressiivisesti kättelyjä summaamalla tehtävän voi hahmottaakin – ja ratkaista – jos se luontevammalta tuntuu.

2.3. Tehtävänä on määrätä luvun 496 positiiviset tekijät. Tähän on useita tapoja. Homma hoituisi noin pienelle luvulle tietokoneella pienellä ohjelmalla silmänräpäyksessä. Toimitaan tässä kuitenkin alkulukujen ja niiden potenssien kautta. Ensin tosin huomataan, että 1 ja 496 on selvästi luvun 496 tekijä, koska jokainen luonnollinen luku on jaollinen ykkösellä ja itsellään.

Selvästi $2 \mid 496$, joten myös 2 on tekijä. Mitkä kakkosen potenssit ovat? Kokeillaan. Laskimella nähdään, että $496/4 = 124 \in \mathbb{N}$, joten myös $2^2 = 4$ on tekijä. Samoin nähdään, että $2^3 = 8$ on tekijä. Entä $2^4 = 16$? Jälleen laskimella nähdään, että $496/16 = 31 \in \mathbb{N}$, joten myös 16 on tekijä, ja koska $2 \nmid 31$, ei mikään korkeampi kakkosen potenssi jaa lukua 496. Näistä laskelmista saadaan ensinnäkin tekijöiden joukkoehdokas

$$1, 2, 4, 8, 16, 31, 496 \tag{1}$$

ja toisaalta luvulle 496 esitys

$$496 = 2^4 \cdot 31\,. \tag{2}$$

Koska 31 on alkuluku, ei luvulla 496 esityksen (2) perusteella muita **alkuluku**tekijöitä enää löydykään. Kaikki listauksen (1) eri alkioiden tulot, jotka ovat suuruudeltaan korkeintaan 496, kuitenkin ovat vielä tekijöitä ja ne on lisättävä listaukseen. Näitä ovat

$$2 \cdot 31 = 62,\ 4 \cdot 31 = 124,\ 8 \cdot 31 = 248\,.$$

Täydellinen listaus on siis

$$1, 2, 4, 8, 16, 31, 62, 124, 248, 496\,.$$

Kun nämä summaa lukua 496 lukuun ottamatta yhteen, saa tulokseksi 496.

2.4. Olkoon $n \in \mathbb{N}$. Väitteenä on, että luku $n^3 + 2n$ on jaollinen luvulla 3.

Jos n itse on jaollinen luvulla 3, niin väite pätee selvästi. Voidaan siis olettaa, että $3 \nmid n$. Tällöin, koska täsmälleen joka kolmas luonnollinen luku on jaollinen kolmosella, pätee

$$3 \mid n-1 \quad \text{tai} \tag{1}$$
$$3 \mid n+1\,. \tag{2}$$

Oletetaan ensin, että $3 \mid n-1$. Tällöin on olemassa luku $k \in \mathbb{N}$ siten, että $n-1 = 3k$ eli $n = 3k+1$. Siten

$$\begin{aligned} n^3+2n &= n(n^2+2) = (3k+1)((3k+1)^2+2) \\ &= (3k+1)(9k^2+6k+1+2) = (3k+1)(9k^2+6k+3) = 27k^3+18k^2+9k+9k^2+6k+3 \\ &= 27k^3+27k^2+15k+3 = 3(9k^3+9k+5+1)\,, \end{aligned}$$

joten väite pätee tässä tapauksessa.

Oletetaan sitten, että $3 \mid n+1$. Tällöin on olemassa $k \in \mathbb{N}$ siten, että $n+1 = 3k$ eli $n = 3k-1$. Siten

$$\begin{aligned} n^3+2n &= n(n^2+2) = (3k-1)((3k-1)^2+2) \\ &= (3k-1)(9k^2-6k+1+2) = (3k-1)(9k^2-6k+3) = 27k^3-18k^2+9k-9k^2-6k-3 \\ &= 27k^3-27k^2+3k-3 = 3(9k^3-9k^2+k-1)\,, \end{aligned}$$

joten väite pätee myös tässä tapauksessa ja on näin kokonaisuudessaan todistettu. □

2.5. Tehtävänä on määrittää lukujen 2626 ja 1104 suurin yhteinen tekijä. Tehdään tämä Eukleideen algoritmilla.

$$2626 = 2 \cdot 1104 + 418 \tag{1}$$
$$1104 = 2 \cdot 418 + 268 \tag{2}$$
$$418 = 1 \cdot 268 + 150 \tag{3}$$
$$268 = 1 \cdot 150 + 118 \tag{4}$$
$$150 = 1 \cdot 118 + 32 \tag{5}$$
$$118 = 3 \cdot 32 + 22 \tag{6}$$
$$32 = 1 \cdot 22 + 10 \tag{7}$$
$$22 = 2 \cdot 10 + 2 \tag{8}$$
$$10 = 5 \cdot 2\,,$$

joten $syt(2626, 1104) = 2$. Lisäksi ylläolevista laskelmista saadaan esitys

$$\begin{aligned}
2 &\overset{a)}{=} 22 - 2 \cdot 10 \overset{b)}{=} 22 - 2(32 - 22) = 22 - 2 \cdot 32 + 2 \cdot 22 \overset{c)}{=} -2 \cdot 32 + 3 \cdot 22 \\
&\overset{d)}{=} -2 \cdot 32 + 3(118 - 3 \cdot 32) \overset{e)}{=} -11 \cdot 32 + 3 \cdot 118 \\
&\overset{f)}{=} -11(150 - 1 \cdot 118) + 3 \cdot 118 \overset{g)}{=} -11 \cdot 150 + 14 \cdot 118 \\
&\overset{h)}{=} -11 \cdot 150 + 14(268 - 1 \cdot 150) \overset{i)}{=} -25 \cdot 150 + 14 \cdot 268 \\
&\overset{j)}{=} -25(418 - 1 \cdot 268) + 14 \cdot 268 \overset{k)}{=} -25 \cdot 418 + 39 \cdot 268 \\
&\overset{l)}{=} -25 \cdot 418 + 39(1104 - 2 \cdot 418) \overset{m)}{=} -103 \cdot 418 + 39 \cdot 1104 \\
&\overset{n)}{=} -103(2626 - 2 \cdot 1104) + 39 \cdot 1104 \overset{o)}{=} -103 \cdot 2626 + 245 \cdot 1104\,,
\end{aligned}$$

mikä on tehtävän toisessa osassa vaadittua muotoa. Edellä olevassa yhtälöketjussa on edetty seuraavasti:

a): Yhtälöstä (8) on saatu esitys luvulle 2.
b): Yhtälöstä (7) on saatu esitys luvulle 10 ja se on sijoitettu 10:n paikalle.
c): Sulut on laskettu auki ja 22:n monikerrat yhdistetty (selvästihän $22+2\cdot 22 = 1\cdot 22+2\cdot 22 = 3\cdot 22$)
d): Yhtlöstä (6) on saatu esitys luvulle 22.
e): Sulut on laskettu auki ja luvun 32 monikerrat yhdistetty.
f): Yhtälöstä (5) on saatu esitys luvulle 32.
g): Sulut on laskettu auki ja luvun 118 monikerrat yhdistetty.
h): Yhtälöstä (4) on saatu esitys luvulle 118.
i): Sulut on laskettu auki ja luvun 150 monikerrat yhdistetty.
j): Yhtälöstä (3) on saatu esitys luvulle 150.
k): Sulut on laskettu auki ja luvun 268 monikerrat yhdistetty.
l): Yhtälöstä (2) on saatu esitys luvulle 268.
m): Sulut on laskettu auki ja luvun 418 monikerrat yhdistetty.
n): Yhtälöstä (1) on saatu esitys luvulle 418.
o): Sulut on laskettu auki ja luvun 1104 monikerrat yhdistetty.

Tällaisissa laskelmissa kannattaa muistaa, että laskun vaiheet voi aina tarkistaa: näppäilee laskimeen ja katsoo, onko tulos lasketun suurimman yhteisen tekijän (tässä 2) suuruinen.

2.6. Juoruajat voidaan numeroida; olkoot he $1, \ldots, n$. Koska jokainen juoruaja tietää skandaalin, jota kukaan muu ei tiedä, määrää skandaali yksikäsitteisesti juoruajan, ja skandaaleista voidaan näin ollen käyttää samaa numerointia kuin juoruajista, jolloin skandaalien joukkoa voidaan merkitä

$$\{1, 2, \ldots, n\}\,.$$

a) Jos $n = 1$, niin on vain yksi juoruaja ja yksi skandaali, joten nolla soittoa riittää ja $S(1) = 0$.

Jos $n = 2$, niin yksi soitto, jonka aikana juoruajat 1 ja 2 kertovat toisilleen skandaalinsa,

riittää. Siispä $S(2) = 1$.

Jos $n = 3$, niin juoruajia ja skandaaleja on kolme. Jos 1 soittaa 2:lle, tietävät he skandaalit 1 ja 2. Tämä ei riitä, sillä kolmosskandaalikin pitäisi tietää. Siispä jomman kumman, olkoon vaikka 2, on soitettava 3:lle. Tällöin juoruaja 1 tietää skandaalit 1 ja 2, juoruaja 2 tietää skandaalit 1,2 ja 3 ja samoin juoruaja 3 tietää skandaalit 1, 2 ja 3. Kolmas soitto vielä vaaditaan, jotta juoruaja 1 saa tietouden skandaalista 3, joten $S(3) = 3$.

Oletetaan sitten, että $n = 4$. Nyt $S(n) = 4$. Nimittäin selvästi $S(n) \geq 4$, neljä skandaalia kun pitää neljän juoruajan välillä jakaa. Toisaalta myös ketju: "1 soittaa 4:lle, 2 soittaa 3:lle, 3 soittaa 1:lle ja 4 soittaa 2:lle" hoitelee homman, joten $S(n) \leq 4$ ja väite seuraa.

b) Todistetaan induktiolla, että $S(n) \leq 2n - 4$ kaikille $n \geq 4$.

Induktion alkuaskel seuraa a)-kohdasta, koska $2 \cdot 4 - 4 = 4$ ja $4 \leq 4$. Tehdään sitten induktio-oletus: oletetaan, että $n \geq 4$ ja että väite pätee n:lle. On osoitettava, että väite pätee $n + 1$:lle eli että

$$S(n + 1) \leq 2(n + 1) - 4 = 2n - 4 + 2\,.$$

Riittää osoittaa, että jos n:n juoruajan joukkoon tulee yksi lisää ja soittokierros alkaa, saadaan skandaalit hoidettua $2n - 4 + 2$:lla soitolla eli – induktio-oletuksen nojalla – kahdella soitolla enemmän kuin n:n juoruajan kerhossa. Tämä hoituu seuraavasti: induktio-oletuksen nojalla olisi olemassa soittoketju, jossa on enintään $2n-4$ soittoa ja jossa juorut $1, \ldots, n$ käydään läpi. Jos juoruaja $n + 1$ soittaa ensimmäisenä (ennen "alkuperäisen" ketjun aloitusta) alkuperäisen ketjun ensimmäiselle soittajalle ja kertoo juorunsa, tulee se kaikkien tietoon. Sitten alkuperäisen ketjun viimeinen soittaja soittaa vielä juoruajalle $n+1$, jolloin $n+1$ saa kaikki juorut $1, \ldots, n$ tietoonsa ja ollaan valmiit. Lisäsoittoja tuli täsmälleen kaksi, joten väite on (epämuodollisesti) todistettu. □

2.7. Olkoon $n \in \mathbb{Z}$.

Väite: n on pariton jos ja vain, jos n^2 on pariton.

Todistus: Oletetaan ensin, että n on pariton. On osoitettava, että n^2 on pariton. Oletuksen nojalla on olemassa $k \in \mathbb{Z}$ siten, että $n = 2k + 1$. Tällöin

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1\,,$$

joten n^2 on pariton ja väitteen tämä suunta pätee.

Oletetaan sitten, että n^2 on pariton. On osoitettava, että n on pariton. Tehdään antiteesi: oletetaan vastoin väitettä, että n on parillinen. Tällöin on olemassa $k \in \mathbb{Z}$ siten, että $n = 2k$. Siten

$$n^2 = (2k)^2 = 4k^2 = 2 \cdot (2k^2)\,,$$

joten n^2 on parillinen. Tämä on kuitenkin vastoin oletusta luvun n^2 parittomuudesta. Syntynyt ristiriita kaataa antiteesin ja todistaa väitteen. □

Tehtävänä oli vielä tarkastella väitettä siinä tapauksessa, että n on parillinen. Kuten edellä olevassa antiteesitodistuksessa nähtiin, seuraa ehdosta "n on parillinen" ehto "n^2 on parillinen". Mutta päteekö sama kääntäen? Kyllä se pätee. Tämän todistamiseksi oletetaan, että n on parillinen. On osoitettava, että n^2 on parillinen. Jos n^2 olisi pariton, olisi tämän tehtävän alkuosan perusteella myös n pariton vastoin oletusta. Luvun n^2 parillisuus seuraa tästä.

Sellainen väite, että mielivaltaisen parillisen luvun neliöjuuri olisi parillinen, ei tietenkään päde – eihän parillisen luvun neliöjuuri ole välttämättä edes kokonaisluku (esimerkkinä vaikka $n = 6$). Mutta tässä tehtävässä nimenomaan oletettiin, että n on kokonaisluku ja siten n^2 on kokonaisluvun neliö.

2.8. Olkoot $a, b, m, n, p \in \mathbb{Z}$ siten, että

$$p \mid m \quad \text{ja} \quad p \mid n\,. \tag{1}$$

Väite:

$$p \mid (am + bn)\,. \tag{2}$$

Todistus: Oletuksesta $p \mid m$ seuraa, että on olemassa $k \in \mathbb{Z}$ siten, että $m = kp$. Vastaavasti oletuksesta $p \mid n$ seuraa, että on olemassa $l \in \mathbb{Z}$ siten, että $n = lp$. Näiden avulla saadaan

$$am + bn = akp + blp = (ak + bl)p\,,$$

mistä väite (1) seuraa. □

2.9. Olkoon $n \in \mathbb{N}$ siten, että luku $2n + 1$ on jonkin kokonaisluvun neliö.

Väite: $n + 1$ on kahden kokonaisluvun neliön summa.

Todistus: Oletuksen mukaan on olemassa luku $m \in \mathbb{Z}$ siten, että

$$2n + 1 = m^2\,, \tag{1}$$

Koska $2n + 1$ on pariton, on esityksen (1) ja tehtävän 2.7 nojalla myös m pariton. On siis olemassa $k \in \mathbb{Z}$ siten, että $m = 2k + 1$. Tällöin

$$m^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k^2 + 4k\,,$$

mistä seuraa esityksen (1) kanssa, että

$$n = \frac{1}{2}(m^2 - 1) = 2k^2 + 2k\,.$$

Tässä kohtaa kannattaa muistaa binomin neliön kaava. Nimittäin sen avulla saadaan yllä olevasta esityksestä:

$$n + 1 = 2k^2 + 2k + 1 = k^2 + 2k + 1 + k^2 = (k + 1)^2 + k^2\,,$$

mistä väite seuraa. □

2.10. Olkoot $m, n \in \mathbb{Z}$. Olkoon lisäksi d aidosti positiivinen kokonaisluku.

Väite: Ehdot

$$syt(m,n) = d \quad \text{ja} \tag{1}$$
$$d \mid m \text{ ja } d \mid n \text{ ,ja jos } e \text{ on lukujen } m \text{ ja } n \text{ tekijä, niin } e \mid d \tag{2}$$

ovat yhtäpitäviä.

Todistus: Oletetaan ensin, että ehto (1) on voimassa. On todistettava ehto (2). Ensinnäkin, koska lukujen m ja n suurin yhteinen tekijä on selvästi lukujen m ja n tekijä, pätee $d \mid m$ ja $d \mid n$. Ehdon (2) toisen osan todistamiseta varten olkoon e lukujen m ja n yhteinen tekijä, jolloin siis $e|m$ ja $e|n$. Riittää osoittaa, että

$$e \mid syt(m,n)\,. \tag{3}$$

Luennoilta tiedetään, että on olemassa kokonaisluvut a ja b siten, että $am + bn = syt(m,n)$. Tämän esityksen avulla väite (3) tulee muotoon

$$e \mid am + bn\,. \tag{4}$$

Ehto (4) seuraa tehtävän 2.8 nojalla oletuksista $e|m$ ja $e|n$, joten väitteen tämä suunta on todistettu.

Toisen suunnan todistamiseksi oletetaan, että ehto (2) on voimassa. On todistettava ehto (1). Mutta tämä seuraa suoraan suurimman yhteisen tekijän määritelmästä, joten väite on kokonaisuudessaan todistettu. □