LUKUTEORIA – johdantoa

Lukuteorian tehtävä: Lukuteoria tutkii *kokonaislukuja, niiden ominaisuuksia ja niiden välisiä suhteita*. Kokonaislukujen maailma näyttää yksinkertaiselta, mutta siellä matka yksinkertaisista havainnoista vaikeasti ratkaistaviin ongelmiin on lyhyempi kuin millään muulla matematiikan alueella:

Esimerkki Pikku-Pekka laskee piparkakkuja: $1, 2, 3, 4, \ldots$. Hän huomaa, että 8 piparkakkua voidaan jakaa tasan 3 pikkuveljen kanssa, mutta seitsemää ei. Pekka on löytänyt *jaollisuuden* käsitteen.

Opittuaan kertotaulun Pekka saattaa huomata, että esim. luvut 13 ja 19 eivät ole jaollisia millään muulla ykköstä suuremmalla kokonaisluvulla kuin itsellään. Pekka on löytänyt *alkuluvut*.

Jos Pekka oikein innostuu tutkimaan alkulukuja, hän ehkä huomaa, että $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7$, $12 = 5 + 7$ … Pekka on havainnut kokonaislukujen ominaisuuden, jonka arvellaan olevan tosi, mutta jota kukaan ei ole vielä todistanut oikeaksi.

Lukuteorian juuret ulottuvat aina 4000 vuoden päähän. Alkuperäisessä muodossaan lukuteoria tutki luonnollisia lukuja, mutta nykyään lukuteoria keskittyy laajempiin lukujoukkojen tutkimiseen.

Lukuteorian lähtökohta on kokonaislukujen jakolasku, josta saadaan *jakoyhtälö* käyttöön. Jakoyhtälöön taas perustuu *Eukleideen algoritmi*, menetelmä, jolla saadaan kahden kokonaisluvun suurin yhteinen tekijä selville. Algoritmille läheistä sukua on *Diofantoksen yhtälöt*.
Alkulukuja sekä *kongruenssi*-käsitteestä saatavia *jakojäännösluokkia* (ns. *moduloita*) tarvitaan mm. salakirjoituksessa ja esim. *Kiinalaisen jäännöslauseen* ratkaisemisessa (ei tällä kurssilla).

C.F. Gauss on todennut: *”Matematiikka on tieteiden kuningatar ja lukuteoria on matematiikan kuningas.”*

Jaollisuus

Määritelmä, kokonaislukujen jaollisuus:
Kokonaisluku a on jaollinen kokonaisluvulla $b(\neq 0)$, jos on olemassa sellainen kokonaisluku c, että $a = bc$. Tällöin b on a:n tekijä **eli** b jakaa a:n **eli** a on b:n monikerta. Tätä merkitään $b|a$. Muutoin $b \nmid a$.

Esimerkki **a)** $7 \mid 42$, $(-5) \mid 30$, $7 \nmid 51$.
b) Luvun 6 tekijät ovat $\pm 1, \pm 2, \pm 3$ ja ± 6.
c) Luvulla 7 jaollisten lukujen joukko on $\{0, \pm 7, \pm 14, \pm 21, \dots\} = \{7n | \ n \in \mathbb{Z}\}$.

Huomautus Tästä eteenpäin sanalla luku tarkoitetaan kokonaislukua!

Se, onko a jaollinen b:llä, voidaan aina selvittää suorittamalla jakolasku $a : b$ ja katsomalla, onko tulos kokonaisluku.
Jos luku b on $2, 3, 4, 5, 6, 8$ tai 9, niin on mukavampi käyttää *jaollisuussääntöjä*, jolloin ei tarvitse tehdä jakolaskua. Myös luvuille 7 ja 11 on olemassa jaollisuussäännöt, mutta ne ovat hieman konstikkaita.
Luvun 10 jaollisuus opeteltu ala-asteen 3.luokalla, 10-kertotaulu.

Lause, jaollisuussääntöjä (todistetaan myöhemmin…ehkä):
Kokonaisluku on jaollinen

- **2:lla**, jos ja vain jos sen viimeinen numero on $2,4,6,8$ tai 0.
- **3:lla**, jos ja vain jos sen numeroiden summa on jaollinen 3:lla.
- **4:llä**, jos ja vain jos sen kahden viimeisen numeron muodostama luku on jaollinen 4:llä.
- **5:llä**, jos ja vain jos sen viimeinen numero on 0 tai 5.
- **6:lla**, jos ja vain jos se on jaollinen sekä 2:lla että 3:lla.
- **7:lla**, jos ja vain jos viimeinen numero poistetaan ja jäljelle jäävästä luvusta vähennetään alkuperäinen viimeinen numero kerrottuna kahdella ja jos näin saatu luku on jaollinen 7:lla, on alkuperäinenkin luku jaollinen 7:lla.
- **8:lla**, jos ja vain jos sen kolmen viimeisen numeron muodostama luku on jaollinen 8:lla.
- **9:llä**, jos ja vain jos sen numeroiden summa on jaollinen 9:llä.
- **10:llä**, jos ja vain jos sen viimeinen numero on 0.
- **11:sta**, jos ja vain jos sen numeroista vuorotellen yhteen- ja vähennyslaskulla saatu luku on jaollinen 11:sta.

Esimerkki 1 Onko luku $21\,624$ jaollinen luvulla **a)** 2, **b)** 3, **c)** 4, **d)** 5, **e)** 6, **f)** 8, **g)** 9?

a) On, koska viimeinen numero 4 on parillinen.
b) On, koska numeroiden summa $2+1+6+2+4=15$ on jaollinen 3:lla.
c) On, koska kahden viimeisen numeron muodostama luku 24 on jaollinen 4:llä.
d) Ei ole, koska viimeinen numero 4 ei ole 0 tai 5.
e) On, koska tämä luku on jaollinen 2:lla ja 3:lla, kts. **b)** ja **c)** – kohdat.
f) On, koska kolmen viimeisen numeron muodostama luku 624 on jaollinen luvulla 8:lla, sillä $8 \cdot 78 = 624$.
g) Ei ole, koska numeroiden summa 15 ei ole jaollinen 9:llä.

Entäpä 7:llä tai 11:sta jaollisuus?
Ei ole 7:llä jaollinen, koska: $2162|4 \rightarrow 2162 - 2 \cdot 4 = 2154$ ja edelleen $215|4 \rightarrow 215 - 2 \cdot 4 = 207$ ja $20|7 \rightarrow 20 - 2 \cdot 7 = 6$ ja $7 \nmid 6$.
Ei ole myöskään 11:sta jaollinen, koska $+2-1+6-2+4=9$ ja pätee $11 \nmid 9$.

Tarkastellaan kokonaislukujen jaollisuuden säilymistä eri laskutoimituksissa, jolloin automaattisesti oletetaan, että merkintä $b \nmid a$ pitää sisällään tiedon $b \neq 0$.

Lause, summan jaollisuus:
Kahden luvun summa on jaollinen tietyllä luvulla, jos *kumpikin* yhteenlaskettava on jaollinen tällä luvulla. Toisin sanoen;

Jos $k|a$ ja $k|b$, niin $k|(a+b)$.

Todistus Jos $k|a$ ja $k|b$, niin on olemassa sellaiset p ja q, että $a = kp$ ja $b = kq$. Tällöin $a + b = kp + kq = k(q+p)$, mistä väite seuraa.
Huomautus Koska erotus on negatiivisen luvun summaamista, säilyy jaollisuus myös erotuksessa, siis jos $k|a$ ja $k|a$, niin $k|(a-b)$.

Lause, tulon jaollisuus:
Kahden luvun tulo on jaollinen tietyllä luvulla, jos *ainakin* toinen tekijä on jaollinen tällä luvulla. Toisin sanoen;

Jos $k|a$, niin $k|ab$ TAI Jos $k|b$, niin $k|ab$.

Todistus Jos $k|a$, niin on olemassa sellainen p, että $a = kp$. Tällöin $ab = kpb$, mistä väite seuraa.

Edelliset lauseet voidaan yhdistää (tosin vaatisi hieman perusteluja), saadaan

Jos $k|a$ ja $k|b$, niin $k|(ra + sb)$

Lause, kokonaislukujen yleiset jaollisuussäännöt:

1. $1|a$,
2. Jos $a \neq 0$, niin $a|a$ ja $a|0$,
3. Jos $a|b$ ja $b|a$, niin $a = \pm b$,
4. Jos $a|b$ ja $b|c$, niin $a|c$,
5. Jos $a|b$, niin $a|kb$ kaikilla $k \in \mathbb{Z}$,
6. Jos $c|a$ ja $c|b$, niin $c|(a \pm b)$
7. Jos $c|a$ ja $c|b$, niin $c|(ra \pm sb)$

Todistus (7): Koska $c|a$ ja $c|b$, niin on olemassa kokonaisluvut x, y siten, että

$$a = cx, \qquad b = cy.$$

Tällöin

$$ra \pm sb = rcx \pm scy = c(rx \pm sy).$$

Siis $c|(ra \pm sb)$.

Todistus Harjoitustehtävä.

Jakoyhtälö

Lause, jakoyhtälö:

Olkoon $a \geq 0$ ja $b > 0$. Tällöin on olemassa sellaiset *yksikäsitteiset* luvut q ja r siten, että $a = qb + r$ ja $0 \leq r < b$.

Nimityksiä: a on *jaettava*, b on *jakaja*, q on *osamäärä* ja r on *jakojäännös*. (Oletus $a \geq 0$ on oikeastaan tarpeeton, mutta tapauksessa $a < 0$ olisi parempi rajata $b < r \leq 0$, siksi oletus $a \geq 0$.)

Esimerkki Suorita jakolasku $123 : 45$. Saadaan osamäärän kokonaisosaksi 2 ja jakojäännökseksi 33, siis $123 = 2 \cdot 45 + 33$.

Jakoyhtälö vaikuttaa itsestään selvältä, mutta sen todistamiseksi tarvitaan pieni lemma.

Lemma, peräkkäiset luvut:

Jos $b > 0$, niin b:n peräkkäisen luvun joukossa on täsmälleen yksi b:llä jaollinen. (vertaa tehtävä: Osoita, että luku $n^3 - n$ on 3:lla jaollinen.)

Todistus Induktio. TAI Havaitaan, että kaikkien b:llä jaollisten lukujen joukko on $B = \{0, \pm b, \pm 2b, \dots\}$, joten jokaiseen b:n peräkkäisen luvun joukkoon kuuluu täsmälleen yksi B:n alkio.

Todistus (jakoyhtälölause)
Tarkastellaan peräkkäisiä lukuja $a, a+1, a+2, \ldots, a-(b-1)$. Näitä on b kappaletta, joten edellisen lemman nojalla täsmälleen yksi niistä, merkitään sitä $a-r$, on b:llä jaollinen. Tällöin on olemassa täsmälleen yksi sellainen q, että $a-r=qb$, eli toisin sanoen $a=qb+r$.

Jakoyhtälöstä tehdään havainto, että jokainen kokonaisluku a voidaan esittää annetun b:n avulla. Mahdolliset a:n esitysmuodot ovat:

$$qb, \quad qb+1, \quad qb+2, \quad \ldots \text{ , tai } \quad qb+(b-1).$$

Esimerkki Olkoon $b=5$. Tällöin jokainen luku a on jotain seuraavaa muotoa

$$a=5q, \quad a=5q+1, \quad a=5q+2,$$
$$a=5q+3 \text{ tai } a=5q+4, \quad q \in \mathbb{Z}.$$

Esimerkki Osoita, että jos n on kokonaisluku, niin luku

$$n(n+1)(n+5)$$

on jaollinen kuudella.

Ratkaisu *Oletus:* n on kokonaisluku,
Väite: $6 \mid n(n+1)(n+5)$
Todistus: Jakoyhtälön nojalla jokainen kokonaisluku a on jotain seuraavaa muotoa:

$$a=6q, \quad a=6q+1, \quad a=6q+2,$$
$$a=6q+3, \quad a=6q+4 \quad \text{tai} \quad a=6q+5, \quad q \in \mathbb{Z}.$$

Näin ollen myös luku $n(n+1)(n+5)$. Tutkitaan jokainen vaihtoehto sijoittamalla tarkasteltavaan lausekkeeseen $n(n+1)(n+5)$ ensin $n=6q$, sitten $n=6q+1$ jne. Pitää löytyä tekijä 6 kaikista vaihtoehd.

Kun $n=6q$: $n(n+1)(n+5)=6q(6q+1)(6q+5)$ ja asia selvä.

Kun $n=6q+1$:
$$n(n+1)(n+5)=(6q+1)(6q+2)(6q+6)$$
$$=(6q+1)(6q+2)\cdot 6(q+1), \text{OK}$$

Kun $n=6q+2$:
$$n(n+1)(n+5)=(6q+2)(6q+3)(6q+7)$$
$$=2(3q+1)\cdot 3(2q+1)(6q+7), \text{OK}$$

Kun $n = 6q + 3$:

$$n(n+1)(n+5) = (6q+3)(6q+4)(6q+8)$$
$$= 3(2q+1) \cdot 2(3q+2)(6q+8), \text{OK}$$

Kun $n = 6q + 4$:

$$n(n+1)(n+5) = (6q+4)(6q+5)(6q+9)$$
$$= 2(3q+2)(6q+5) \cdot 3(2q+3), \text{OK}$$

Kun $n = 6q + 5$:

$$n(n+1)(n+5) = (6q+5)(6q+6)(6q+10)$$
$$= (6q+5) \cdot 6(q+1)(6q+10), \text{OK}$$

Siis luku $n(n+1)(n+5)$ on aina jaollinen kuudella.