■ Sisältö
■ Hakemisto

Alkuluvut

■ luonnollinen luku

Alkuluvuiksi sanotaan jaottomia luonnollisia lukuja ($\neq 1$):

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53,\ 59,$$
$$61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97,\ 101,\ 103,\ 107,\ 109,\ 113,\ 127,$$
$$131,\ 137,\ 139,\ 149,\ 151,\ 157,\ 163,\ 167,\ 173,\ 179,\ 181,\ 191,$$
$$193,\ 197,\ 199,\ 211,\ 223,\ 227,\ 229,\ 233,\ 239,\ 241,\ 251,\ \ldots\ .$$

Voidaan helposti osoittaa, että näitä on äärettömän paljon, ts. suurinta alkulukua ei ole. Tästä huolimatta ei ole helppoa konstruoida uusia alkulukuja, vaan näiden etsiminen edellyttää pitkiä tietokoneajoja. Vuoden 1999 tilanteen mukaan suurin tunnettu alkuluku on $2^{6972593}-1$; tässä on 2 098 960 numeroa.

Jokainen luku voidaan yksikäsitteisellä tavalla esittää alkulukujen tulona; näitä sanotaan luvun *alkutekijöiksi*. Esimerkiksi

$$123456789 = 3^2 \cdot 3607 \cdot 3803, \qquad 90642552 = 2^3 \cdot 3 \cdot 7^4 \cdot 11^2 \cdot 13.$$

Luonnollisen luvun n jakaminen alkutekijöihin voidaan alkeellisesti tehdä kokeilemalla: Tutkitaan, onko luku jaollinen alkuluvuilla, jotka ovat $\leq \sqrt{n}$. Tällöin on apua seuraavassa esitettävistä jaollisuussäännöistä.

Jaollisuussäännöt

Tärkeimmät *jaollisuussäänöt* ovat seuraavat:

- Luku on kahdella jaollinen, jos sen viimeinen numero on 2, 4, 6, 8 tai 0.
- Luku on kolmella jaollinen, jos sen numeroiden summa on kolmella jaollinen. Esimerkiksi 573 on kolmella jaollinen, koska $5+7+3=15$ on kolmella jaollinen.
- Luku on neljällä jaollinen, jos sen kahden viimeisen numeron muodostama luku on neljällä jaollinen. Esimerkiksi 123498724 on neljällä jaollinen, koska 24 on neljällä jaollinen.
- Luku on viidellä jaollinen, jos sen viimeinen numero on 0 tai 5.
- Luku on yhdeksällä jaollinen, jos sen numeroiden summa on yhdeksällä jaollinen.
- Luku on yhdellätoista jaollinen, jos sen numeroista vuorotellen yhteen- ja vähennyslaskuilla saatu luku on yhdellätoista jaollinen. Esimerkiksi 45859 on yhdellätoista jaollinen, koska $4-5+8-5+9=11$ on yhdellätoista jaollinen; samoin 4169, koska $4-1+6-9=0$.

Parillisia lukuja ovat kahdella jaolliset luvut, so. muotoa $2n$ olevat luvut, missä n on kokonaisluku. *Parittomat luvut* ovat vastaavasti muotoa $2n+1$.

■ Sisältö
■ Hakemisto

Suurin yhteinen tekijä ja pienin yhteinen jaettava

■ luonnollinen luku

Kahden luonnollisen luvun *yhteinen tekijä* on luku, jolla molemmat luvut ovat jaollisia (ts. jako menee tasan). *Suurin yhteinen tekijä* (syt) on suurin tällainen luku.

Suurin yhteinen tekijä voidaan määrittää jakamalla luvut alkutekijöihin: yhteisten alkutekijöiden tulo on suurin yhteinen tekijä. Esimerkiksi: Lukujen $156 = 2 \cdot 2 \cdot 3 \cdot 13$ ja $104 = 2 \cdot 2 \cdot 2 \cdot 13$ suurin yhteinen tekijä on $2 \cdot 2 \cdot 13 = 52$.

■ Eukleides

Suurin yhteinen tekijä voidaan hakea myös ns. *Eukleideen algoritmilla*, jolloin alkutekijöihin jakoa ei tarvita.

Kahden luonnollisen luvun *yhteinen jaettava* on luku, joka on jaollinen kummallakin luvulla. *Pienin yhteinen jaettava* (pyj) on pienin tällainen luku.

■ potenssi (kokonaisluku-)

Pienin yhteinen jaettava voidaan määrittää lukujen alkutekijäesityksen perusteella: Kun jokainen esiintyvä alkutekijä otetaan korotettuna korkeimpaan esiintyvään potenssiin, saadaan näiden tulona pienin yhteinen jaettava. Esimerkiksi: Lukujen $156 = 2 \cdot 2 \cdot 3 \cdot 13$ ja $104 = 2 \cdot 2 \cdot 2 \cdot 13$ pienin yhteinen jaettava on $2^3 \cdot 3 \cdot 13 = 312$.

Lukujen n ja p suurimmalle yhteiselle tekijälle ja pienimmälle yhteiselle jaettavalle pätee

$$n \cdot p = \text{syt}(n, p) \cdot \text{pyj}(n, p).$$

Salakirjoitus

Suurten lukujen jakaminen alkutekijöihin merkitsee yleensä suurta työtä, samoin sen selvittäminen, onko annettu luku alkuluku vai ei. Tehtävä on hankala myös käytettäessä nopeita tietokoneita, koska laskenta-aika kasvaa erittäin nopeasti luvun suurentuessa, vaikka käytössä ovat alkeellista kokeilumenetelmää paljonkin tehokkaammat algoritmit.

Alkutekijöihin jaon vaikeuteen perustuvat ns. *julkisen salakirjoituksen* järjestelmät, joissa viestien vastaanottaja voi julkisesti ilmoittaa hänelle lähetettävien viestien kirjoitusavaimen, so. menettelyn, jolla viestit on salakirjoitettava. Tämä ei merkitse, että salakirjoitetut viestit pystyttäisiin julkisesti lukemaan: lukuavaimen tietää vain viestien saaja.

Periaate on seuraava: Kirjoitusavaimena on kahden suuren alkuluvun tulo, mutta ei tekijöitä erikseen. Tämä on julkinen. Lukuavain edellyttää tekijöiden tuntemista. Sen konstruoiminen vaatii siis ison luvun tekijöihin jakoa. Valitsemalla kyllin suuret alkuluvut, päästään tilanteeseen, missä tämä parhaillakin tietokoneohjelmilla vie vuosikausia. Tehtävän vaikeutta kuvaa seuraava: Vuonna 1990 tehdyssä kokeessa onnistuttiin 155-numeroinen luku jakamaan kolmeen alkutekijäänsä viiden viikon tietokoneajolla, kun käytössä oli 1000 verkkoon kytkettyä konetta.