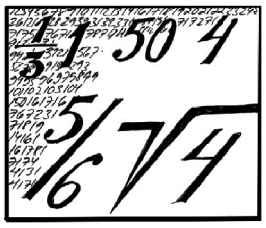

Ketjumurtoluvut: mitä ne ovat ja mitä hyötyä niistä on?

Anne-Maria Ernvall-Hytönen
Helsingin yliopisto

Yksinkertaiseksi ketjumurtoesitykseksi kutsutaan positiivisen luvun esittämistä muodossa

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots}}}}},$$

missä luvut $a_1, \ldots$ ovat positiivisia kokonaislukuja ja a_0 on epänegatiivinen kokonaisluku. Lisäksi sovitaan, että viimeinen luvuista a_i (jos siis kehitelmä on päättyvä) on suurempi kuin 1.

Esimerkiksi siis ei kirjoiteta

$$\frac{37}{16} = 2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{1}}},$$

vaan

$$\frac{37}{16} = 2 + \cfrac{1}{3 + \cfrac{1}{5}}.$$

Käytännössä tilanne on tämä: Jos kyseessä on rationaaliluku, päättyy tämä esitys joskus (eli kolmen pisteen tilalle ei tule äärettömän pitkää jonoa). Jos kyseessä on irrationaaliluku, ei tämä esitys pääty koskaan. Jälkimmäinen on helppo nähdä. Ensimmäinen ei ole niin triviaali. Se on luultavasti helpoin perustella sillä, että ketjumurtokehitelmä tehdään käytännössä Eukleideen algoritmilla, joka vain kirjoitetaan toisin. Innostunut lukija voi perustella tämän itselleen. Jos Eukleideen algoritmi kuulostaa täysin vieraalta, ei tarvitse pelästyä: ketjumurtokehitelmiä voi tehdä, vaikkei olisi Eukleideesta tai hänen algoritmistaan koskaan kuullutkaan.

Luvun kehittäminen ketjumurtoluvuksi

Otetaan nyt pari esimerkkiä siitä, miten luku kehitetään yksinkertaiseen ketjumurtoesitykseen. Käsitellään ensin rationaaliluku. Verrataan sen jälkeen ketjumurtokehitelmää Eukleideen algoritmiin osoittajalle ja nimittäjälle.

Esimerkki. Kirjoitetaan $\frac{27}{8}$ ketjumurtolukuna. Huomataan ensin, että esityksessä

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ddots}}}}}$$

on osan

$$\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}}}}}$$

pakko olla ykköstä pienempi, sillä $a_1 \geq 1$ ja vähintään toinen seuraavista ehdoista toteutuu: $a_1 \geq 2$ tai nimittäjässä on muutakin kuin a_1. Luvun a_0 on siis vastattava luvun kokonaisosaa. Koska $\frac{27}{8} = 3 + \frac{3}{8}$, on oltava $a_0 = 3$. Nyt

$$\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}}}}} = \frac{3}{8},$$

joten

$$a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}}}} = \frac{8}{3}.$$

Ihan vastaavasti kuin edellä huomataan, että luvun a_1 on oltava luvun $\frac{8}{3}$ kokonaisosa. Koska $\frac{8}{3} = 2 + \frac{2}{3}$, on $a_1 = 2$. Nyt

$$\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}}}} = \frac{2}{3},$$

joten

$$a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}}} = \frac{3}{2} = 1 + \frac{1}{2}.$$

Siispä $a_2 = 1$ ja $a_3 = 2$. On siis saatu

$$\frac{27}{8} = 3 + \cfrac{1}{2+\cfrac{1}{1+\frac{1}{2}}}.$$

Jos lukujen 27 ja 8 suurin yhteinen tekijä määritettäisiin Eukleideen algoritmilla, näyttäisi se tältä:

$$\begin{aligned} 27 &= 3 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1. \end{aligned}$$

Eukleideen algoritmin kertoimet (ensimmäiset luvut yhtäsuuruusmerkkien oikealla puolella) ovat samat kuin ketjumurtoesityksen kertoimet. Tämän perusteleminen itselle on siis se innokkaan lukijan harjoitustehtävä.

Otetaan toinen esimerkki. Ennen esimerkkiä palautetaan mieleen (tai johdetaan) eräs muistikaava:

$$(a-b)(a+b) = a^2 + ab - ba - b^2 = a^2 - b^2.$$

Tämän avulla voi muokata joskus lukuja helpommin käsiteltävään muotoon. Esimerkiksi:

$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{(\sqrt{3}-1)(\sqrt{3}+1)} = \frac{\sqrt{3}+1}{2}.$$

Esimerkki. Kirjoitetaan $\sqrt{3}$ ketjumurtolukuna. Kuten aiemminkin, huomataan, että luvun a_0 on vastattava luvun $\sqrt{3}$ kokonaisosaa. Koska $1 \leq \sqrt{3} < 2$, niin kokonaisosa on 1. Siispä $a_0 = 1$. Nyt

$$\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}}}}} = \sqrt{3}-1,$$

eli

$$a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}}}} = \frac{1}{\sqrt{3}-1}.$$

Yllä olevan laskun perusteella

$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}.$$

Tämän muotoilun etu on se, että sitä on helppo arvioida. Koska $1 \leq \sqrt{3} < 2$, niin

$$1 = \frac{1+1}{2} \leq \frac{\sqrt{3}+1}{2} \leq \frac{2+1}{2} = \frac{3}{2}.$$

Siispä $a_1 = 1$, sillä se on luvun $\frac{1}{\sqrt{3}-1}$ kokonaisosa. Koska $a_1 = 1$, pätee

$$1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}}}} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2},$$

joten

$$\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}}}} = \frac{\sqrt{3}+1}{2} - 1 = \frac{\sqrt{3}+1-2}{2} = \frac{\sqrt{3}-1}{2}.$$

Nyt siis

$$a_2+\cfrac{1}{a_3+\cfrac{1}{\ddots}} = \frac{2}{\sqrt{3}-1} = \frac{2(\sqrt{3}+1)}{(\sqrt{3}-1)(\sqrt{3}+1)} = \sqrt{3}+1.$$

Koska $2 \leq \sqrt{3}+1 \leq 3$, on $a_2 = 2$. Siispä

$$\cfrac{1}{a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}}} = \sqrt{3}+1-2 = \sqrt{3}-1,$$

joten

$$a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}.$$

Tämän tilanteen olemme kuitenkin nähneet jo aiemmin, eli laskiessamme lukua a_1. Siispä $a_3 = a_1 = 1$. Nyt tilanne alkaa toistamaan itseään, eli $a_4 = a_2 = 2$. Tämä tulee jatkumaan vastaavasti, eli luvuissa a_i vuorottelevat luvut 1 ja 2. Jos alaindeksi i on pariton, on $a_i = 1$, ja jos alaindeksi i on parillinen, on $a_i = 2$. Nyt siis

$$\sqrt{3} = 1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{\ddots}}}}}.$$

Ketjumurtoluvut ja arviointi

Tässä luvussa joudun vain antamaan tuloksia todistamatta niitä. Perusteellisesti kaiken todistamalla tämä artikkeli muuttuisi melko pitkäksi, eikä enää tarjoaisi sitä nopeaa johdattelua ketjumurtolukuihin, joka oli tarkoitukseni.

Luvun ketjumurtokehitelmää voidaan katkaista. Esimerkiksi luvun

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\cfrac{1}{\ddots}}}}},$$

ketjumurtokehitelmä voidaan katkaista esimerkiksi seuraavilla tavoilla:

$$a_0, \quad a_0+\frac{1}{a_1}, \quad a_0+\cfrac{1}{a_1+\cfrac{1}{a_2}},$$

jne. Vastaavasti kuin katkaisemalla desimaalikehitelmä, näinkin saadaan arvioita luvulle. Näitä kutsutaan luvun *konvergenteiksi*.

Aloitetaan luvun π arvioinnista kymmenjärjestelmän avulla. Tiedetään, että

$$\pi = 3{,}14159265\ldots$$

Arvioita luvulle π saadaan siis suoraan sen desimaalikehitelmää katkaisemalla ja normaalien pyöristyssääntöjen mukaan ylös tai alas pyöristämällä:

desimaalit	arvio	virhe
0	3	$< 0{,}2 = \frac{2}{10}$
1	$3{,}1 = \frac{31}{10}$	$< 0{,}04 = \frac{4}{100}$
2	$3{,}14 = \frac{314}{100}$	$< 0{,}002 = \frac{2}{1000}$
3	$3{,}142 = \frac{3142}{1000}$	$< 0{,}0005 = \frac{5}{10000}$.

Virheet ovat selvästi pienempiä kuin luvun suuruus. Lisäksi virhe pienenee, kun otetaan desimaaleja lisää (eli kasvatetaan arviossa nimittäjää). Tämä on hyvä, mutta käytännössä virhe pienenee melko hitaasti. Otetaan vertailun vuoksi luvun π ketjumurtokehitelmä

$$3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1+\cfrac{1}{292+\cfrac{1}{\ddots}}}}}$$

ja siitä saatavat arviot

$$\pi \approx 3, \quad \pi \approx 3+\frac{1}{7} = \frac{22}{7}, \quad \pi \approx 3+\cfrac{1}{7+\cfrac{1}{15}} = \frac{333}{106}, \ldots$$

Nyt virheet ovatkin

arvio	virhe
3	$< 0{,}2 = \frac{2}{10}$
$\frac{22}{7}$	$< \frac{2}{1000}$
$\frac{333}{106}$	$< \frac{1}{10000}$
$\frac{103993}{33102}$	$< 10^{-9}$

Virheet pienenevät nyt huomattavaa vauhtia verrattuna nimittäjän kasvuvauhtiin. Yleisesti voidaan todistaa, että jos ξ on jokin luku ja $\frac{r}{s}$ joku sen konvergentti, niin

$$\left|\xi - \frac{r}{s}\right| \leq \frac{1}{s^2}.$$

Toinen suunta on puolestaan tällainen: Jos ξ on jokin luku ja $\frac{r}{s}$ joku arvio, joka toteuttaa ehdon

$$\left|\xi - \frac{r}{s}\right| \leq \frac{1}{2s^2},$$

niin $\frac{r}{s}$ on väistämättä luvun ξ konvergentti.

Sovellus yhtälönratkaisuun ja kryptografiaan

RSA-salausjärjestelmässä on julkinen avain, joka on lukupari (n, e) sekä salauksen purkamiseen tarvittava salainen eksponentti d. Luku n on kahden eri alkuluvun tulo $n = pq$. Tämä alkutekijähajotelma on salainen. Luvut toteuttavat ehdon

$$ed \equiv 1 \pmod{\varphi(n)},$$

jolloin $w^{ed} \equiv w$ kaikilla w. Tällöin siis viesti voidaan salata korottamalla se potenssiin e ja redusoimalla modulo n ja salaus voidaan purkaa korottamalla salattu viesti potenssiin d ja redusoimalla modulo n.

Otetaan esimerkki, joka on tehty hyvin pienillä luvuilla:

Esimerkki. Jos $n = 7 \cdot 11 = 77$, niin $\varphi(n) = 6 \cdot 10 = 60$. Valitaan luvuksi e esimerkiksi 13. Tällöin viesti 8 salataan seuraavasti: Lasketaan 8^{13} ja lasketaan jakojäännös luvulla 77 jaettaessa. Saadaan 50.

Viestin purkamiseksi tarvitaan d. Tämä luku toteuttaa siis ehdon

$$13d \equiv 1 \pmod{60}.$$

Nyt $d = 37$. Viesti saadaan siis purettua korottamalla se potenssiin 37 ja redusoimalla modulo 77. Jos esimerkiksi on vastaanotettu viesti 50, tapahtuu purku laskemalla 50^{37} ja ottamalla jakojäännös luvulla 77 jaettaessa. Saadaan 8, kuten pitikin, eli kun viesti 8 salattiin ja salaus purettiin, saatiin alkuperäinen viesti.

Nyt huomionarvoista on se, että luvun d määrittämiseen tarvitaan luvun n alkutekijähajotelma. Jos sitä ei ole käytettävissä, on luvun d määrittäminen hyvin hankala tehtävä. Itse asiassa on todistettu, että jos pystytään määrittämään d, niin saadaan selville luvun n alkutekijähajotelma (eli implikaatio kulkee myös toiseen suuntaan). Luvun alkutekijähajotelman löytäminen on tunnetusti vaikeana pidetty ongelma. Sitä on mietitty jo vuosisatoja. Kuitenkin jos d on pieni, tarkasti ottaen $d < \frac{n^{1/4}}{3}$, niin ongelma voidaan kiertää. Tämä menetelmä tunnetaan Wienerin hyökkäyksenä [2] ja tästä on erinomainen kuvaus Bonehin artikkelissa [1].

Yhtälö $ed \equiv 1 \pmod{\varphi(n)}$ nimittäin muuttuu muotoon

$$ed - k\varphi(n) = 1,$$

joka on kolmen tuntemattoman Diofantoksen yhtälö. Oletetaan lisäksi, että $e < \varphi(n)$, jolloin $k < d$, ja että $p < q < 2p$ (eli luvun n alkutekijät ovat samaa kertaluokkaa). Nyt myös $p < \sqrt{n}$ ja $q < 2\sqrt{n}$. Tällöin

$$n - \varphi(n) = pq - (p-1)(q-1) = p + q - 1 < p + q < 3\sqrt{n}.$$

Kirjoitetaan yllä oleva yhtälö muotoon

$$ed - kn = 1 + k\varphi(n) - kn.$$

Jaetaan tämä yhtälö puolittain luvuilla d ja n, ja tarkastellaan vasemman puolen erotusta arvioimalla oikeaa puolta:

$$\left| \frac{e}{n} - \frac{k}{d} \right| = \left| \frac{1 + k(\varphi(n) - n)}{dn} \right| \leq \frac{k(n - \varphi(n))}{dn}.$$

Koska $n - \varphi(n) < 3\sqrt{n}$ ja $k < d$, voidaan arvioida

$$\frac{k(n - \varphi(n))}{dn} < \frac{3\sqrt{n}}{n} = \frac{3}{\sqrt{n}} < \frac{1}{2d^2},$$

sillä epäyhtälö $\frac{3}{\sqrt{n}} < \frac{1}{2d^2}$ on yhtäpitävä epäyhtälön $6d^2 < \sqrt{n}$ kanssa, joka varmasti toteutuu, kun $d < \frac{n^{1/4}}{3}$. Edellä kerrotun perusteella $\frac{k}{d}$ on varmasti luvun $\frac{e}{n}$ konvergentti. Luvun konvergentit pystytään laskemaan tehokkaasti, jolloin myös luvut k ja d pystytään löytämään ja RSA murtamaan.

Harjoitustehtäviä

Tehtävä 1. Esitä ketjumurtolukuna $\frac{13}{5}$.

Tehtävä 2. Esitä ketjumurtolukuna $\frac{89}{25}$.

Tehtävä 3. Esitä ketjumurtolukuna $\sqrt{2}$.

Tehtävä 4. Esitä ketjumurtolukuna $\sqrt{5}$.

Tehtävä 5. Esitä ketjumurtolukuna $\sqrt{13}$.

Kirjoittajan kommentit ja tunnustukset

Tätä tekstiä kirjoitettaessa on hyödynnetty MAOL:n ja matematiikan olympiavalmennuksen yhteiskerhoon tuottamaani kerhomateriaalia. Jos siis koet nähneesi osan tekstistä joskus aiemmin, luultavasti oletkin nähnyt.

Viitteet

[1] Boneh, Dan (1999). Twenty Years of attacks on the RSA Cryptosystem. Notices of the American Mathematical Society (AMS) 46 (2).

[2] M. J. Wiener (1990). Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, vol. 36, no. 3, pp. 553–558, May 1990, doi: 10.1109/18.54902.