Kiinalainen jäännöslause ripauksella kryptografiaa

Anne-Maria Ernvall-Hytönen
Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Johdanto

Kiinalaisen jäännöslauseen nimi vaatii ehkä hieman selvennystä. Lauseen alkuperäinen muotoilu löytyy Sun Zin kirjasta, johon englanniksi viitataan nimellä The Mathematical Classic of Sun Zi. Lauseen tarkka ajankohta lienee hieman hämärän peitossa: Wikipedia kertoo tämän kirjan olevan 300-luvulta. Toisaalta kirjoittajan elinajasta todetaan vain hänen eläneen 300–500 -luvulla. Kenneth Rosenin lukuteorian kirjassa [1] (Elementary number theory and its applications) annetaan ymmärtää, että lause on ehkäpä 100-luvulta. Tarkalla ajankohdalla ei varmasti ole väliä, oleellisempaa on tietää, että kyseessä on vanha ja kiinalainen lause. Yleistetty muotoilu puolestaan löytyy Qin Jiushaon kirjasta Da yan shu, joka on kirjoitettu 1247.

Lauseen muotoilu ja todistus

Lyhyesti sanottuna kiinalainen jäännöslause kertoo kongruenssiyhtälöryhmälle tietyin ehdoin löytyvän ratkaisun:

Kiinalainen jäännöslause. Olkoot $m_1, m_2, \ldots, m_r$ pareittain yhteistekijättömiä kokonaislukuja. Tällöin kongruenssiyhtälöryhmällä

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

on yksikäsitteinen ratkaisu modulossa

$$M = m_1 m_2 \cdots m_r.$$

Ennen kuin siirrytään todistukseen, todetaan, että ehto lukujen $m_1, m_2, \ldots, m_r$ pareittaisesta yhteistekijättömyydestä on paikallaan: Mikäli tätä ehtoa ei olisi, ei välttämättä olisi yhtään ratkaisua, kuten jos $x \equiv 1 \pmod 2$ ja $x \equiv 2 \pmod 6$, jolloin ensimmäinen ehto kertoo luvun x olevan pariton, ja toinen ehto kertoo luvun x olevan parillinen ja hieman muuta vielä lisäksi. Toisaalta ratkaisuja voisi olla useita. Esimerkkinä tarkastellaan vaikkapa tilannetta, jossa $x \equiv 3 \pmod 6$ ja $x \equiv 6 \pmod 9$, jolloin luvut $x \equiv 15 \pmod{18}$ toteuttavat ehdot, eli modulossa $54 = 9 \cdot 6$ on useita ratkaisuja.

Nyt voimme siirtyä todistukseen.

Todistus. Merkitään $M_k = \frac{M}{m_k}$ kaikilla $1 \leq k \leq r$. Nyt $\mathrm{syt}(m_k, M_k) = 1$, jolloin luvulla M_k on olemassa käänteisluku modulossa m_k (tämän löytää vaikkapa Diofantoksen yhtälön ratkaisemalla Eukleideksen algoritmia käyttäen), eli on olemassa sellainen s_k, että

$M_k s_k \equiv 1 \pmod{m_k}$. Muodostetaan luku

$$x_0 = a_1 M_1 s_1 + a_2 M_2 s_2 + \cdots a_r M_r s_r.$$

Huomataan, että

$$x_0 = a_1 M_1 s_1 + \cdots + a_r M_r s_r \equiv a_k \pmod{m_k},$$

sillä $m_k \mid M_j$, jos $j \neq k$. (Muista, miten luku M_j on muodostettu!) Lisäksi $a_k M_k s_k \equiv a_k \pmod{m_k}$, koska luku s_k on luvun M_k käänteisluku modulossa m_k. Selvästi siis x_0 on ratkaisu.

Osoitetaan nyt, että muita ratkaisuja ei modulossa M ole. Tarkastellaan lukuja x_0 ja x_1, jotka ovat yhtälöryhmän ratkaisuja. Tällöin

$$x_1 - x_0 \equiv a_k - a_k = 0 \pmod{m_k}$$

kaikilla $1 \leq k \leq r$, eli $m_k \mid (x_1 - x_0)$. Koska luvut m_k ovat yhteistekijättömiä, seuraa tästä $M \mid (x_1 - x_0)$, eli ratkaisu on yksikäsitteinen modulossa M. Todistus on valmis.

Katsotaanpa nyt esimerkkiä kiinalaisen jäännöslauseen käytöstä, eli ratkaistaan yhtälöryhmä

$$x \equiv 2 \pmod{5}$$
$$x \equiv 3 \pmod{7}.$$

Koska $x \equiv 2 \pmod 5$, voidaan kirjoittaa $x = 5k + 2$. Sijoitetaan tämä jälkimmäiseen yhtälöön:

$$5k + 2 \equiv 3 \pmod{7},$$

eli $5k \equiv 1 \pmod 7$. Nyt voi tietenkin repiä hatusta luvun 5 käänteisluvun modulossa 7, tai sen voi selvittää yksinkertaisesti ratkaisemalla Diofantoksen yhtälön $5k - \ell 7 = 1$. Käytetään Eukleideksen algoritmia:

$$7 = 5 + 2$$
$$5 = 2 \cdot 2 + 1$$

eli $1 = 5 - 2 \cdot 2$, josta sijoittaen ensimmäisestä yhtälöstä ratkaistun kakkosen jälkimmäiseen:

$$1 = 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7.$$

Luvun 5 käänteisluku modulossa 7 on siis luku 3, eli voidaan valita $k = 7h + 3$. Sijoitetaan tämä lausekkeeseen $x = 5k + 2$:

$$\begin{aligned} x &= 5k + 2 = 5(7h + 3) + 2 \\ &= 35h + 15 + 2 = 35h + 17 \equiv 17 \pmod{35}. \end{aligned}$$

Yhtälöryhmän ratkaisu modulossa 35 on siis $x \equiv 17$. Halutessaan tämän voi myös helposti tarkistaa.

Yllä olevan yhtälöryhmän ratkaisun olisi toki voinut hakea kiinalaisen jäännöslauseen todistusta jäljitellenkin.

Luvun loppuun pohdintatehtävä: Mikäli yhtälöryhmässä

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

eivät luvut m_1 ja m_2 ole yhteistekijättömiä, niin milloin yhtälöryhmällä on kuitenkin ratkaisu? Missä modulossa se on yksikäsitteinen? Rosenin kirjan tehtävistä ([1], sivu 142) voi tässä olla apua, mutta tehtävä on kyllä ratkeava ilmankin sitä.

Hyödyllinen lukukokemus kiinalaisen jäännöslauseen käytöstä voi myös olla [2].

Hyödyt RSA:n käytössä

Jotta voimme järkevästi pohtia kiinalaisen jäännöslauseen hyödyistä RSA-kryptosysteemin käytössä, on syytä ensin käydä läpi RSA:n toimintaperiaate.

RSA on siis kryptosysteemi, eli salausjärjestelmä paremmalla suomella sanottuna. Sitä käytetään tiedon salaamiseen. Kriittistä on, että lähettäjä pystyy tiedon salaamaan, vastaanottaja puolestaan salauksen purkamaan, ja että ulkopuoliset eivät salausta voi purkaa. Käytännössä on lisäksi toivottavaa, että mikään operaatio ei kestä tuhottoman kauan.

RSA:ssa on julkinen avain (n, e) ja salainen avain $(\varphi(n), d)$, missä $\varphi(n)$ on Eulerin funktio (eli jos

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

on luvun n alkutekijähajotelma, niin

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1)).$$

Tiedetään myös, että n on muotoa pq, missä p ja q ovat kaksi eri alkulukua. On syytä huomata, että vaikka luku n tunnetaan, ei lukua $\varphi(n)$ ole helppo laskea, koska se edellyttää luvun n alkutekijöiden tuntemista, ja tämä taas on yleisessä tilanteessa hyvin hankalaa.

Käytännössähän luvun $\varphi(n)$ pystyy laskemaan, mikäli luvut p ja q on tiedossa. Homma toimii myös toisinpäin: jos luvun $\varphi(n)$ tietää, niin luvut p ja q on helppo selvittää. Jätetään tämän toteaminen aktiivisille lukijoille harjoitustehtäväksi.

Lisäksi luvut e ja d on valittu niin, että $ed \equiv 1 \pmod{\varphi(n)}$. Tämä valinta on helppo tehdä, mikäli $\varphi(n)$ on tiedossa, valitsemalla ensin e tai d ja ratkaisemalla sitten Diofantoksen yhtälö $ed - \ell\varphi(n) = 1$.

RSA toimii seuraavasti:

1. Alice saa päähänsä, että hän haluaa ottaa vastaan viestejä salattuna. Hän valitsee alkuluvut p ja q, laskee luvut $n = pq$ ja $\varphi(n) = (p - 1)(q - 1)$. Hän valitsee vielä luvun e ja laskee luvun d ratkaisemalla Diofantoksen yhtälön $ed - \ell\varphi(n) = 1$.

2. Hän julistaa lukuparin (n, e) kaikelle kansalle.
3. Bob päättää lähettää salaisen viestin Alicelle. Viesti on luku w.
4. Bob laskee luvun w^e modulossa n ja lähettää lopputuloksen Alicelle.
5. Alice ottaa vastaan Bobin lähettämän luvun, jota merkitään tässä kirjaimella v ja laskee:

$$v^d \equiv w^{ed} = w^{1+\ell\varphi(n)} \equiv w \pmod{n},$$

eli hän saa modulossa n Bobin lähettämän luvun w. Kunhan n on riittävän suuri (käytännössä se valitaan olemaan joitakin tuhansia bittejä, jotta systeemi on turvallinen), voi Bob lähettää varsin isojakin lukuja tietäen, että Alice saa ne oikein.

Salaus perustuu siis sille, että luvun d selvittäminen on hirvittävän hankalaa, ja brute force -ratkaisu kestäisi liian pitkään.

Yleisesti ottaen RSA on hyvin turvallinen: Mikäli RSA murtuu, niin myös lukujen tekijöihinjako-ongelma on ratkeava, ainakin kahden alkutekijän tapauksessa. Tämä ongelma taas on hyvin vanha, ja hyvin hankalaksi todettu. Kuitenkin joitakin rajoituksia on: luku d ei saa olla kovin pieni, eikä myöskään liian lähellä lukua $\varphi(n)$. Ei myöskään ole turvallista, jos luvut p ja q ovat liian lähellä toisiaan. Turvallisuuden nojalla toisaalta yleensä vaaditaan, että $p < q < 2p$. Nämä rajoitukset ovat melko kosmeettisia, vaikka toisinaan joitakin niistä kovin mielellään rikkoisikin nopeuden nimissä.

Jotain kuitenkin nopeudenkin kanssa on tehtävissä. Sen sijaan, että Alice laskisi luvun v^d suoraan modulossa n, voi hän laskea sen moduloissa p ja q, mikä on nopeampaa, sillä hän voi redusoida paitsi välituloksia moduloissa p ja q, voi hän redusoida eksponentin moduloissa p ja q, jolloin potenssiinkorotuksia täytyy tehdä paljon vähemmän. Laskettuaan luvut $w_p \equiv v^d \pmod{p}$ ja $w_q \equiv v^d \pmod{q}$, laskee hän luvun w käyttäen kiinalaista jäännöslausetta, sillä $w \equiv w_p \pmod{p}$ ja $w \equiv w_q \pmod{q}$.

Laitetaan loppuun pohdiskelutehtävä (jolla ei ole mitään tekemistä kiinalaisen jäännöslauseen kanssa): Määritä mahdollisimman suuri h (riippuen luonnollisestikin luvusta n) niin, että tietäen vain luvun n pystyt löytämään sen alkutekijät p ja q, jos $n = pq$ ja $|p - q| < h$. (Vihje: neliöiden jakauma on mielenkiintoinen asia.)

Viitteet

[1] K. H. Rosen, *Elementary number theory and its applications.* Addison Wesley, 3rd Edition, 1993.

[2] J. Herman, R. Kučera and J. Šimša, Equations and Inequalities: Elementary Problems and Theorems in Algebra and Number Theory, Canadian Mathematical Society Books in Mathematics 1, Springer-Verlag, New York, 2000.

Uutta Verkko-Solmun matematiikkadiplomisivulla

Diplomi VII tehtävineen sekä diplomin VIII tehtävät ovat ilmestyneet osoitteessa

`http://solmu.math.helsinki.fi/2008/diplomi/diplomi.html`