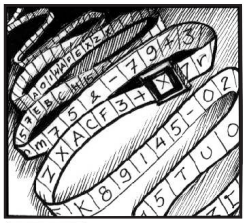

Lukuteoriaa ja salakirjoitusta, osa 1

Heikki Apiola
Dosentti
Matematiikan laitos, Teknillinen korkeakoulu

Johdanto

Lukuteoriaa on joskus pidetty esteettisesti kauniina, mutta käytännössä aika hyödyttömänä matematiikan alana. Kukaan ei asettane nykyäänkään tuota esteettistä puolta kyseenalaiseksi, mutta miten on sen käytännön hyödyn laita?

Nykyinen sähköiseen tiedonvälitykseen perustuva asioiden hoitaminen ei olisi mahdollista ilman tehokkaita salausmenetelmiä. Niiden kehittämisessä puolestaan on ollut ratkaisevan tärkeä osa juuri tuolla lukuteorian tarjoamalla "hyödyttömällä" estetiikalla.

Tässä kirjoituksessa esitetään lukuteorian perusasiat, joita tarvitaan osassa 2 esiteltävän ns. julkisen RSA-salakirjoitusmenetelmän johtamiseen, päteväksi osoittamiseen ja ohjelmoimiseen.

Lukuteoria on sikäli poikkeava matematiikan ala, että siitä voi kirjoittaa lukijalle, jolla on minimaaliset perustiedot matematiikassa. Itse asiassa tarvitaan vain ymmärrys kokonaislukujen perusominaisuuksista ja laskutoimituksista niillä. Näillä eväillä päästään aika nopeasti kiinnostaviin tuloksiin ja sovelluksiin käsiksi.

Kirjoitus toimii testinä yllä olevalle väitteelle. Toki on hyödyksi, jos lukijalla on oheislukemistona vaikkapa lukion lukuteorian syventävän kurssin 11 oppikirja, kuten [Lukio1] tai [Lukio2].

Kirjoitus ei ole lukuteorian alkeiden oppikirjan osa, keskityn välttämättömän (ja toivottavasti riittävän) osuuden esittelyyn päämääränä yllä mainitun julkisen salakirjoituksen RSA-salakirjoitusalgoritmina tunnetun menetelmän ymmärtäminen. Esitän asiat perusteellisesti, niin että yksityiskohtienkin ymmärtäminen olisi mahdollista. Jotta kirjoitus ei paisuisi liian laajaksi, esitän sen kahdessa osassa. Tässä ensimmäisessä keskityn lukuteorian perusteisiin ja toisessa tuohon salakirjoitussovellukseen.

Kokonaisluvut, jaollisuus

Merkintöjä: Käytän joukko-opin ja logiikan standardimerkintöjä:

$x \in A$ tarkoittaa: x kuuluu joukkoon A, eli x on A:n alkio.

Kokonaisluvut: $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3 \ldots\}$

Luonnolliset luvut: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Käsittelemme pelkästään kokonaislukuja, usein viittaamme kokonaislukuun lyhyesti sanalla *luku*.

Pienin ja suurin luku

Kokonaislukujen osajoukoilla on ominaisuus, jota ei ole rationaali- eikä reaaliluvuilla. Kyseessä on mahdollisuus valita osajoukosta pienin ja suurin luku.

Luonnollisten lukujen minimiominaisuus: *Jokaisessa $\mathbb{N}$:n epätyhjässä osajoukossa on* ***pienin luku***.

Tästä seuraa:

Kokonaislukujen minimi- ja maksimiominaisuus: *Jokaisessa $\mathbb{Z}$:n* ***ylhäältä rajoitetussa*** *epätyhjässä osajoukossa on* ***suurin*** *luku ja* ***alhaalta rajoitetussa*** *on* ***pienin*** *luku*

Jakoyhtälö

Jos vaikkapa luku $a = 55$ jaetaan luvulla $b = 8$ kokonaislukujakona, saadaan osamäärä $q = 6$ ja jakojäännös $r = 7$, sillä $55 = 6 \cdot 8 + 7$. Osamäärä q löydetään hakemalla suurin luku q, jolle $q \cdot 8 \leq 55$, jakojäännös on se, mitä jää yli. Jakojäännös r on jakajaa ($b = 8$) pienempi, muutenhan osamäärä $q = 6$ ei olisikaan suurin mahdollinen.

Yllä oleva esimerkki noudattaa sitä periaatetta, jolla olemme oppineet jakolaskun suorittamaan jo peruskoulussa. Sama periaate voidaan kirjoittaa yleisesti pelkillä kirjainsymboleilla:

Lause 1. *Olkoot a ja b luonnollisia lukuja, $a > 0$. Tällöin on olemassa yksikäsitteiset q ja r, $0 \leq r < b$ siten, että $a = q\,b + r$*

Tod. Toistamme siis vain yllä esimerkissä esitetyn juonen. Voidaan olettaa, että $a > b$, muutenhan voidaan ottaa $q = 0, r = a$.
No, ei muuta kuin valitaan maksimiominaisuuden perusteella suurin luku q niin, että $q\,b \leq a$. (Epäyhtälön $p\,b \leq a$ toteuttavia lukuja p varmasti on, ainakin $p = 0$, ja $p = 1$, joten puheena on epätyhjä joukko. Lisäksi kaikki tällaiset luvut p toteuttavat varmasti epäyhtälön $p \leq a$, joten niiden joukko on ylhäältä rajoitettu.)

Merkitään r:llä erotusta $r = a - b\,q$, jolloin $r \geq 0$. Jos olisi $r \geq b$, niin voitaisiin kirjoittaa $r = b + c$, missä $c \geq 0$.
Tällöin olisi $a = q\,b + b + c = (q + 1)\,b + c$, joten q ei olisikaan yllä olevan joukon suurin luku.

Yksikäsitteisyys: Olkoon kaksi esitystä: $a = q_1\,b + r_1$, ja $a = q_2\,b + r_2$, missä $0 \leq r_i < b, \quad i = 1, 2$.
Tällöin $|r_2 - r_1| < b$, joten $|q_1 - q_2|\,b < b$.
Koska $b > 0$, sillä voidaan jakaa ja saadaan $|q_1 - q_2| < 1$.
Kokonaisluvuille tämä on mahdollista vain siten, että $q_1 = q_2$. Siitäpä heti seuraa, että myös $r_1 = r_2$. □

Määritelmä 1 (Jaollisuus)**.** *Luku a on jaollinen luvulla b, jos on olemassa luku n siten, että $a = n\,b$. Tällöin sanotaan, että b on a:n* ***tekijä*** *ja a on b:n* ***monikerta***. *Merkitään: $b \,|\, a$, joka voidaan lukea: "b on tekijänä a:ssa" tai "b jakaa a:n"*

Huomautus 1. *Jos $b \,|\, a$, niin $-b \,|\, a$. Jokaisella luvulla a on triviaalit tekijät ± 1 ja $\pm a$.*
Luku 0 on jaollinen kaikilla luvuilla b, koska $0 = 0 \cdot b$, toisaalta 0 on tekijänä 0:ssa, mutta ei missään luvussa $a \neq 0$.

Esimerkki 1. *Jaollisuusesimerkkejä*
1) $7 \,|\, 56, \quad -3 \,|\, 12.$
2) Luvun 12 ei-triviaalit tekijät: $\pm 2, \pm 3, \pm 4, \pm 6$
3) Luvulla 6 jaollisten lukujen joukko:
$\{n \cdot 6 | n \in \mathbb{Z}\} = \{0, \pm 6, \pm 12, \pm 18 \ldots\}$

Kootaanpa yhteen yleiset jaollisuuden perusominaisuudet.

Lause 2. *Yleiset jaollisuusominaisuudet*
1) Jos $x \,|\, a$ ja $x \,|\, b$, niin $x \,|\, (a \pm b)$
Yleisemmin:
1') Jos $x \,|\, a$ ja $x \,|\, b$, niin $x \,|\, (a\,m + b\,n)$ mielivaltaisille (kokonais)luvuille $m, \quad n$
2) Jos $x \,|\, a$ tai $x \,|\, b$, niin $x \,|\, (a\,b)$
3) Jos $a \,|\, b, \quad b \neq 0$, niin $|a| \leq |b|$,

Tod. Todistetaan malliksi kohta 1). Yleistys 1') on aivan vastaavanlainen. Kohdat 2) ja 3) ovat suorastaan itsestäänselvyyksiä. Mieti kuitenkin.
Kohta 1): Oletuksen mukaan on olemassa (kokonais)luvut s ja t siten, että $a = s\,x$ ja $b = t\,x$. Niinpä $a + b = s\,x + t\,x = \underbrace{(s + t)}_{\in \mathbb{Z}}\,x$, joten $x \,|\, (a + b)$.

□

Kannattaa huomata, että käänteinen suunta kohdalle 2) ei päde yleisesti.

Esim: $12 = 3 \cdot 4$. Luku 6 on tekijänä luvussa 12, mutta 6 ei ole tekijänä kummassakaan tulontekijässä 3 tai 4.

No, kysehän on siitä, että 6 :lla on yhteinen tekijä sekä 3 :n että 4 :n kanssa. Tähän tärkeään havaintoon palataan, ja muotoillaan lisäehto, jolla käänteinen johtopäätös on voimassa.

Kun puhutaan positiivisten kokonaislukujen a jaollisuudesta, voidaan rajoittua puhumaan positiivisista tekijöistä b, sillä jos b on tekijä, niin $-b$ on aina myös tekijä, joten sen mainitseminen erikseen on turhaa sanahelinää. (Matemaatikon hyveisiin kuuluu sanojen säästäminen.)

Alkuluvut

Määritelmä 2. *Kokonaisluku $a > 1$ on **alkuluku**, jos se on jaollinen vain 1:llä ja itsellään. Muuten puhutaan **yhdistetystä luvusta**.*

Jokainen luku a on jaollinen myös -1 :llä ja $-a$:lla. Noudatamme edellä mainittua "turhan sanahelinän välttämisperiaatetta " ja pitäydymme positiivisissa tekijöissä.

Alkulukujen alkupää näyttää tältä: $2, 3, 5, 7, 11, 13, 17$. Yksinkertainen algoritmi alkulukujen laskemiseen on jo antiikin Kreikassa tunnettu *Eratostheneen seula*. Lukujoukosta $1, \ldots, n$ seulotaan pois kaikki yhdistetyt luvut poistamalla ensin 2:n monikerrat (parilliset luvut), sitten 3:n monikerrat (3:lla jaolliset luvut), jne. Kts. [Lukio1]

Symbolilaskentaohjelmissa on valmiita alkulukualgoritmeja ohjelmoituna. MAPLE:lla voitaisiin 100 ensimmäistä alkulukua laskea näin:

```
>     N := [$(2 .. 100)]
[2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13,14 ...
  ...   99, 100]
>     map(ithprime, N)
[3, 5, 7, 11, 13, 17, 19,23,29,31,37,41,43 ..
  ...   523, 541]
```

Eratostheneen seula on helppo ymmärtää ja ohjelmoida, mutta se on varsin tehoton. Tehokkaiden alkulukualgoritmien kehittely on tärkeä osa mm. kryptologista (salakirjoitusmenetelmiin liittyvää) tutkimusta.

Lause 3 (Alkulukuhajotelma)**.** *Jokainen luonnollinen luku $a > 1$ voidaan esittää alkulukujen tulona.*

Tod. Jos a on alkuluku, se on (yksiterminen) alkulukutulo. Jos taas a on yhdistetty luku, se on muotoa $a = a_1\, a_2, \quad a_i > 1, i = 1, 2$. Jos kumpikin on alkuluku, olemme perillä. Ellei, niin ainakin toinen on yhdistetty luku. Esitetään kaikki (toinen tai molemmat) tekijät kahden luvun tulona. Näin jatketaan, kunnes päädytään tuloon, jonka mitään tekijää ei voida jakaa. Tämä tapahtuu viimeistään $\log_2(a)$ askeleen jälkeen, koska yhdistetyn luvun kumpikin tekijä ≥ 2. □

Tuntuisi uskomattomalta, jos alkuluvut loppuisivat jostain alkaen, ts. niitä olisi vain äärellinen määrä. *Eukleides* todisti jo v. 300 eKr. kirjassaan Elementa (Kirja IX, propositio 20), että niitä todella on äärettömän paljon. Tämä 2300 vuotta vanha todistus on edelleenkin voimissaan. Näin se menee:

Lause 4 (Eukleides)**.** *Alkulukuja on ääretön määrä.*

Tod. Olkoon p mielivaltainen alkuluku. Osoitetaan, että on olemassa sitä suurempi alkuluku. Tällöinhän äärellinen alkulukujen määrä johtaisi heti ristiriitaan.

Olkoot $p_1, p_2, \ldots, p_n = p$ kaikki alkuluvut, jotka ovat $\leq p$. Olkoon $P = (p_1 \cdot p_2 \cdot \ldots \cdot p_n) + 1$. Jos P jaetaan millä tahansa luvuista $p_j, j = 1, \ldots, n$, niin jakojäännös $= 1$ (ajattele $P : n$ kaavaa jakoyhtälönä). Jako ei siis mene tasan, eli mikään p :tä pienempi alkuluku ei ole tekijänä P :ssä. Mutta alkulukuhajotelmalauseen 3 mukaan P :llä on tekijänä alkuluku (P itse, jos se sattuu olemaan alkuluku). Tämä tekijä ei ole mikään p :tä pienempi tai sen suuruinen (alku)luku, joten sen on oltava p :tä suurempi. □

Myöhemmin on esitetty monia muitakin todistuksia, kts. esim.
`http://en.wikipedia.org/wiki/Prime_numbers`

Suurin yhteinen tekijä

Lukujen a ja b **suurin yhteinen tekijä**, $\text{syt}(a, b)$ on nimensä mukaisesti suurin luku s, joka on tekijänä sekä a:ssa että b:ssä.
Esimerkiksi $\text{syt}(24, 30) = 6, \quad \text{syt}(5, 7) = 1$. Systemaattinen tapa $\text{syt}(a, b)$:n määräämiseksi on muodostaa alkulukuhajotelmat ja poimia kummastakin yhteiset alkutekijät. Edellisessä esimerkissä: $24 = 2 \cdot 2 \cdot 2 \cdot 3$, $30 = 2 \cdot 3 \cdot 5$. Yksi kakkonen ja yksi kolmonen voidaan poimia kummastakin, eikä mitään muuta, joten todellakin saadaan 6.
Tehokkaampi menetelmä on ns. *Eukleideen algoritmi*, joka esitellään kohta.
Sitä ennen johdetaan suurimmalle yhteiselle tekijälle kaava, josta saadaan kätevästi koko joukko ominaisuuksia. Sitä voidaan pitää tämän kirjoituksen yhtenä tärkeimpänä työkaluna.

Lause 5 (SYTlause)**.** *Olkoot a ja b positiivisia kokonaislukuja.*

$$syt(a, b) = min\{s > 0 | s = a\, x + b\, y, \quad x, y \in \mathbb{Z}\}$$

Tod. Oikealla puolella oleva joukko koostuu positiivisista kokonaisluvuista. Luonnollisten lukujen minimiominaisuuden mukaan tässä joukossa on pienin luku

$$s_0 = a\, x_0 + b\, y_0,$$

missä x_0 ja y_0 ovat sellaiset kokonaisluvut, joilla tuo minimi saavutetaan.

Todistuksen juoni on osoittaa, että

$$\begin{cases} (1) & \text{syt}(a, b) \leq s_0, \\ (2) & \text{syt}(a, b) \geq s_0. \end{cases}$$

Epäyhtälö (1) : Koska syt(a,b) on tekijänä sekä a:ssa että b:ssä, niin se on tekijänä jokaisessa muotoa $a\,x+b\,y$ olevassa lausekkeessa, siis myös s_0 :ssa. Niinpä on oltava syt$(a,b) \leq s_0$.

Epäyhtälö (2) : Jos onnistumme osoittamaan, että $s_0 \mid a$ ja $s_0 \mid b$, niin tiedämme, että s_0 on a :n ja b :n yhteinen tekijä ja siten pienempi tai yhtäsuuri kuin suurin yhteinen tekijä syt(a,b).

Aloitetaan a :sta. Jakoyhtälön mukaan $a = q\,s_0 + r$, missä $0 \leq r < s_0$. Osoitetaan, että $r = 0$, jolloin väitteemme on a :n osalta todistettu.

Kirjoitetaan $r = a - q\,s_0 = a - q(a\,x_0 + b\,y_0) = a(1 - q\,x_0) + b(-q\,y_0)$.

Siis r on "muotoa s_0". Lisäksi $0 \leq r < s_0$. Koska s_0 on pienin positiivinen tuota muotoa oleva luku, on oltava $r = 0$. Siten $a = q\,s_0$, ts. $s_0 \mid a$.

Aivan samoin voimme menetellä b:n suhteen, ja päätellä, että $s_0 \mid b$. (Suoritapa tämä lasku ja päättely!) Siispä s_0 on a :n ja b :n yhteinen tekijä, ja niin ollen $s_0 \leq$ syt(a,b).

Niin olemme todistaneet epäyhtälöt (1) ja (2), joten todellakin syt$(a,b) = s_0$.

□

Ennenkuin ryhdymme nautiskelemaan tämän lauseen seurauksista, otamme käyttöön merkinnän ja nimityksen:
Keskenään jaottomat luvut: Luvut a ja b ovat keskenään jaottomat, jos syt$(a,b) = 1$. Käytämme myös sanontaa *yhteistekijättömät* ja puhetapaa: "a :lla ja b :llä ei ole yhteisiä tekijöitä" tarkoittaen: ei *yhteisiä epätriviaaleja tekijöitä*.

Aloitetaan edellä luvatulla käänteisellä puolella tulon jaollisuusominaisuuteen (Lause 2)

Lause 6. *Oletetaan, että syt$(a,n) = 1$. Jos $n \mid a\,b$, niin $n \mid b$*

Tod. Koska syt$(a,n) = 1$, on $1 = x_1\,a + y_1\,b$ joillakin kokonaisluvuilla x_1 ja y_1 (SYTlause (Lause 5)). Kun tämä kerrotaan puolittain b :llä, saadaan

$$b = x_1\,a\,b + y_1\,b\,n.$$

Koska $n \mid a\,b$, on $a\,b = k\,n$ jollain $k \in \mathbb{Z}$. Kun yllä b :n lausekkeessa sijoitetaan $a\,b$:n paikalle $k\,n$, saadan:

$$b = x_1\,k\,n + y_1\,b\,n = n\underbrace{(x_1\,k + y_1\,b)}_{\in\mathbb{Z}}.$$

Siispä todellakin n on tekijänä b : ssä. □

Erityisesti saadaan nyt:

Seuraus 7. *Olkoon p alkuluku ja a ja b mielivaltaisia kokonaislukuja. Jos p on tekijänä tulossa $a\,b$, niin p on tekijänä a :ssa tai p on tekijänä b :ssä. Loogisena lauseena ilmaistuna:*

$$p \ \ \textit{alkuluku}, \ \ p \mid a\,b \implies p \mid a \vee p \mid b.$$

Tod. Oletetaan siis, että p on tekijänä $a\,b$:ssä. Jos p ei ole tekijänä a :ssa, niin syt$(p,a) = 1$, koska p on alkuluku. Edellisen mukaan p :n täytyy siten olla tekijänä b :ssä. □

Tehtävä 1. *Osoita esimerkillä, että edellinen ei päde yleisesti, jos p ei ole alkuluku.*

Eukleideen algoritmi

Kyseessä on menettely, jolla voidaan rekursiivisesti määrittää syt(a,b) annetuille kokonaisluvuille a ja b . Se on peräisin samasta Elementa-teoksesta n. 300 v. eKr kuin lause 4.

Algoritmi pohjautuu havainnolle:

Lause 8. *Olkoot a ja b luonnollisia lukuja, $a > b$. Jos r on jakojäännös jakolaskussa a/b, niin syt$(a,b) =$ syt(b,r).*

Tod. Kirjoitetaan jakoyhtälön mukaan $a = q\,b + r$. Jos s on a :n ja b :n yhteinen tekijä, niin s on tekijänä r :ssä, koska $r = a - q\,b$ (Lause 2, kohta 1). Siispä s on b:n ja r:n yhteinen tekijä. Kääntäen, jos s on b:n ja r:n yhteinen tekijä, niin se on a:n tekijä, koska $a = q\,b + r$. Kaikki yhteiset tekijät ovat samat, joten erityisesti suurin yhteinen tekijä on sama. □

Esimerkki 2. *Määrättävä syt*$(576, 168)$.
$576 = 3 \cdot 168 + 72$.
Lause 8: syt$(576, 168) =$ *syt*$(168, 72)$.
Jakoyhtälö: $168 = 2 \cdot 72 + 24$.
Lause 8: syt$(168, 72) =$ *syt*$(72, 24)$.
Jakoyhtälö: $72 = 3 \cdot 24 + 0$.
Lause 8: syt$(72, 24) =$ *syt*$(24, 0) = 24$.
Alkuperäisen tehtävän ratkaisu: syt$(576, 168) = 24$.

Kirjoitetaan algoritmi rekursiiviseksi (itseään kutsuvaksi) ohjelmaksi symbolilaskentaohjelman MAPLE ohjelmointikielellä. Kyseessä on varmasti kaikkien rekursiivisten algoritmien äiti!
(Solmukirjoitus Maplen-käytöstä:
`http://solmu.math.helsinki.fi/1999/5/apiola/`,
rekursiota käsitellään kirjoituksessa:
`http://solmu.math.helsinki.fi/1998/2/seppanen/`.
Eräs kuulemani tietosanakirjamääritelmä: *Rekursio, kts. rekursio*)

```
Eukleides := proc (a, b)
print(a, b); # seurantaa varten
if b = 0 then a else
  Eukleides(b, a mod b) end if
  # a mod b on jakojäännös.
end proc:
```

Suoritetaan esimerkkiajo vaikkapa määrittämällä syt$(145, 75)$. Oikean sarakkeen b siirtyy seuraavalla rivillä vasemmalle jakajaksi ja saman rivin oikean puolen luku on vastaava jakojäännös.

```
> Eukleides(145, 75)
            145, 75
             75, 70   ( 145 = 1x75 + 70 )
              70, 5   (  75 = 1x70 + 5  )
              5, 0    (  70 = 14x5 + 0 )
                5     ( syt(5,0) = 5 )
```

Siis syt$(145, 75) = 5$.

Aritmetiikkaa jakojäännöksillä

Meihin on "sisäänrakennettu" laskenta jakojäännöksillä erityisesti tapauksissa $n = 12$ ja 24. Jokainen tietää, että kellonajat 5 (i.p.) ja 17 tarkoittavat samaa, ja jos yöjuna lähtee klo 20 ja on perillä klo 9, niin matkaan on kulunut aikaa 13 tuntia. Matemaattisesti nämä voidaan ilmaista kaavoilla:

$$5 \equiv 17 \pmod{12} \quad \text{ja} \quad 20 + 13 \equiv 9 \pmod{24}$$

Yleisesti määritellään käsite *kongruenssi modulo n*:

Määritelmä 3. *Olkoon $n > 1$. Luvut a ja b ovat* ***kongruentteja modulo n****, jos $n \mid (a-b)$. Tällöin merkitään*

$$a \equiv b \mod n.$$

Määritelmä tarkoittaa sitä, että a ja b saadaan toisistaan lisäämällä sopiva "modulin" n monikerta: $a - b = k\,n$ jollain kokonaisluvulla k. Tämä merkitsee, että jakolaskuissa a/n ja b/n on sama jakojäännös.

Tehtävä 2. *Jos tänään on maanantai, niin mikä viikonpäivä on* 100 *:n päivän kuluttua?*
Ratkaisu: Numeroidaan viikonpäivät $0, \ldots, 6$ *antaen arvo* 0 *vaikka sunnuntaille. Tehtävänä on selvittää jakojäännös jakolaskussa* 100/7. *Jakoyhtälö on* $100 = 7 \cdot 14 + 2$. *Kun siis kierrämme "viikkokellotaulua"* 14 *kertaa (=* 98 *päivää), tulemme samaan, mistä lähdimme, mennään vielä kahdella yli, joten päivä on* $1 + 2 = 3$, *eli keskiviikko.*

Voidaan ajatella, että $1 + 100$:sta vähennetään sellainen 7 :n monikerta, että päästään välille $0, \cdots, 6$. Sanonta: *Redusoidaan luku* 101 *modulo 7*. Tämä juhlalliselta kalskahtava sanonta tarkoittaa siis arkikielellä vain sitä, että määritämme jakojäännöksen jakolaskussa 101/7. Kaiken aikaa vaan siis pyörittelemme samaa jakoyhtälöä.

Modulaariaritmetiikkaa

Havainnollisesti ajatellen modulaariaritmetiikka, eli "jakojäännöslaskenta" voidaan ajatella niin, että lukusuoran sijasta kuljetaan pitkin ympyrän kehää. Kellotaulu on tästä havainnollinen esimerkki, siinä jakovälejä on 12 ja kyseessä siis laskenta modulo 12.

Voidaan ajatella, että kokonaislukusuora on kierretty rullalle, joka kiertää samaa kehää äärettömän monta kertaa. Kehä on jaettu 12 :een osaan, yleisesti modulin eli jakajan ilmaisemaan määrään osia. Useimmiten emme ole kiinnostuneita siitä, montako täyttä kierrosta kehän ympäri tehdään, vaan siitä, mille kohdalle "onnenpyörää" lopulta pysähdytään.

Käytännön laskutoimitukset $(+ - \cdot)$, kun modulina on n, suoritetaan niin, että lasketaan luvuilla $0, \ldots, n-1$. Lopputulos "redusoidaan modulo n", ts. lisätään tai vähennetään n:n monikertoja niin, että päästään välille $0, \ldots n-1$, eli kerran vielä: lasketaan jakojäännös, kun jakajana on n.

Formaalimpi ja matemaattisesti kauemmas kantava tapa on tarkastella ns. jäännösluokkia modulo n, jolloin "samaistetaan" kaikki luvut, joilla on sama jakojäännös jaettaessa luvulla n. Viittaan koulukirjoihin [Lukio2] Kongruenssi, s. 126, tai [Lukio1] Kappale 5 s. 82. Koska pyrin pitämään koneiston minimaalisena salakirjoitustavoitteitamme ajatellen, vältän ylimääräisiä uusia abstraktioita, niin elegantteja ja keskeisiä matemaattisen käsitteenrakennuksen välineitä kuin ovatkin.

Kongruensseilla laskeminen

Kongruenssi näyttää yhtälöltä ja monessa suhteessa käyttäytyy samoin.

Lause 9.

$$\textit{Jos} \quad a \equiv b \pmod{n} \quad \textit{ja} \quad c \equiv d \pmod{n}, \quad \textit{niin}$$

$$a \pm c \equiv b \pm d \pmod{n} \quad \textit{ja} \quad a\,c \equiv b\,d \pmod{n}.$$

Tod. Tyydytään todistamaan vain summan tapaus. Erotus on aivan samanlainen. Tulo on hiukan pitempi, mutta periaate on sama, eikä siinä voi mitenkään johtua harhateille (eihän!). (Yritä itse, mutta voit myös katsoa [Lukio1] s. 85).

No niin, olkoon siis $n \,|\, (a-b)$ ja $n \,|\, (c-d)$, ts.

$a-b = j\,n$ ja $c-d = k\,n$ joillakin luvuilla $j,\ \ k$. Nyt

$(a+c)-(b+d) = j\,n - k\,n = (j-k)\,n$, joten todellakin

$a+c = (b+d) + K\,n$, missä $K = j-k \in \mathbb{Z}$, eli väite on tosi. □

Erityisesti valitsemalla $c = d(= m)$ nähdään, että kongruenssiin voidaan lisätä puolittain luku, se voidaan kertoa puolittain luvulla ja korottaa potenssiin:

Lause 10. *Jos* $a \equiv b\,(mod\ \ n)$ *ja* $k \in \mathbb{Z},\ \ m \in \mathbb{N}$, *niin*

(1.) $a + k \equiv b + k\,(mod\ \ n)$,

(2.) $a\,k \equiv b\,k\,(mod\ \ n)$,

(3.) $a^m \equiv b^m\,(mod\ \ n)$.

Kongruenssiyhtälön supistaminen

Kyseessä on oikeastaan vain lauseen 6 yhteydessä esitettyjen asioiden pukeminen modulaariaritmetiikan kielelle.

Esimerkki 3.

$$2 \cdot 2 \equiv 2 \cdot 5 (mod\ \ 6).$$

Voidaanko tekijällä 2 *supistaa? Ts, päteekö* $2 \equiv 5(mod\ \ 6)$ *? No eipä tietenkään, sillä* $5-2 = 3$, *joka ei taatusti ole* 6*:n kokonaismonikerta.*

Ehto, jolla supistaminen on sallittua, ei yllättäne ketään.

Lause 11 (Modsupistus)**.** *Jos* $syt(k,n) = 1$, *niin* $a\,k \equiv b\,k\,(mod\ \ n) \implies a \equiv b\,(mod\ \ n)$.
Sanallisesti: Kongruenssiyhtälö voidaan supistaa yhteisellä kertoimella k, *mikäli kerroin* k *ja moduuli* n *ovat yhteistekijättömät.*

Tod. Oletetaan siis, että $\mathrm{syt}(k,n) = 1$ ja $a\,k \equiv b\,k\,(\mathrm{mod}\ \ n)$. Tällöin $(a-b)\,k \equiv 0\,(\mathrm{mod}\, n)$, joten $n|(a-b)\,k$. Koska $\mathrm{syt}(k,n) = 1$, niin lauseen 6 mukaan $n|(a-b)$, ts. $a \equiv b\,(\mathrm{mod}\, n)$. □

Kongruenssiyhtälö, käänteisalkio

Tarkastelemme yksinomaan muotoa $a\,x \equiv b\,(\mathrm{mod}\ \ n)$ olevia yhtälöitä. Yleisesti kokonaislukukertoimisia yhtälöitä sanotaan *Diofantoksen yhtälöiksi* ja niihin liittyvä teoria on osa lukuteorian perusoppia. Salakirjoituksen kannalta tarvitaan vain yllä olevaa muotoa, vieläpä sillä lisärajoituksella, että $b = 1$.

Lause 12. *Olkoon* $n > 1$ *ja* $syt(a,n) = 1$. *Tällöin yhtälöllä* $a\,x \equiv 1(mod\ \ n)$ *on yksikäsitteinen ratkaisu* x.

Tod. 1. Ratkaisun olemassaolo: Todistus seuraa suoraan Lauseesta 5 näin: Koska $\mathrm{syt}(a,n) = 1$, on olemassa kokonaisluvut x ja y siten, että $a\,x + n\,y = 1$, ts. $a\,x = 1 + n\,y$. Mutta tämähän tarkoittaa, että $a\,x \equiv 1(\mathrm{mod}\ \ n)$.

2. Ratkaisun yksikäsitteisyys seuraa suoraan *Modsupistus*-lauseesta 11. (Mieti kuitenkin!) □

Yllä olevan yhtälön ratkaisu voidaan ajatella käänteisalkion etsimistehtäväksi annetulle a :lle. Tyydyttävämmin sanottuna kyse on a :n määräämän "jäänösluokan" modulo n käänteisalkiosta, josta kuitenkin lupasimme olla puhumatta enempää tällä kertaa. Ratkaisua x merkitään usein symbolilla $x = a^{-1}(\mathrm{mod}\ \ n)$. Yksikäsitteinen käänteisalkio $(\mathrm{mod}\ \ n)$ on siis olemassa jokaiselle a :lle, joka on yhteistekijätön modulin n kanssa.

Käänteisalkion määrittämiseen tarvitaan menetelmä lauseen 5 kertoimen x (siellä merkittiin x_0) laskemiseksi. Se voidaan tehdä ns. laajennetulla Eukleideen algoritmilla. Palataan tähän kirjoituksen osassa 2.

Fermat'n pieni lause

Kaikkihan ovat kuulleet legendaarisia tarinoita *Fermat'n* suuresta lauseesta *"Fermat's last theorem"*. Kuinka "olen löytänyt ihmeellisen todistuksen, joka ei mahdu muistikirjani marginaaliin", ja kuinka englantilainen *Andrew Wiles*, 7 vuotta yksinäisessä vinttikamarissa työskenneltyään todisti tuon vuodesta 1630 matemaattista maailmaa kiusanneen lauseen. Kuinka siitä löytyi puutteita, jotka *Wiles* myöhemmin onnistui paikkaamaan. Ja kuinka tuo todistus ei mahtuisi sataankaan marginaaliin.

No, nyt emme puhu siitä enempää, vaan "pienestä" lauseesta, joka on yksi keskeinen osa salakirjoitusmenetelmän oikeellisuuden todistusta.

Lause 13 (Fermat'n pieni lause)**.** *Jos* p *on alkuluku ja* a *ei ole jaollinen* p *:llä, niin*

$$a^{p-1} \equiv 1(mod p).$$

Tod. Lauseen 10 kohdan (3.) perusteella a voidaan redusoida välille $[0, p-1]$. Koska p ei ole tekijänä a :ssa, ei a ole kongruentti 0 :n kanssa modulo p. Niinpä riittää osoittaa väite oletuksella $0 < a \leq p-1$.

Muodostetaan jono

$$(A) : a, 2\,a, 3\,a, \ldots, (p-1)\,a \ \ (\mathrm{mod}\ \ p).$$

Nämä ovat siis jakojäännöksiä, kun jakajana on p, siis lukuja välillä $[0, p-1]$.
Osoitetaan, että luvut ovat > 0, ja että tässä on jokainen luku välillä $1, \ldots, p-1$ täsmälleen kerran. Toisin sanoen jono (A) antaa luvut $1, \ldots, p-1$ jossain järjestykseesä.

Jotta juonen seuraaminen olisi miellyttävämpää, jätämme tämän yksityiskohdan erikseen osoitettavaksi.

Kun se on tehty, tiedetään siis, että

$$a \cdot 2\,a \cdot 3\,a \cdot \ldots \cdot (p-1)\,a \equiv 1 \cdot \ldots \cdot (p-1) = (p-1)! \pmod{p}.$$

Toisin sanoen $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$.

Palamme halusta jakaa yhtälö puolittain $(p-1)!$:lla, mutta onko lupa? No eipä muuta kuin sydämen kyllyydestä sovellamme lausetta 11, jonka oletus on voimassa, sillä mikään luvuista $2, \ldots, p-1$ ei voi olla alkuluvun p tekijä.

Lause on todistettu, kunhan selvitämme tuon edellä mainitun puuttuvan yksityiskohdan.

Tiedämme jo, että $a \neq 0$. Voisiko olla $k\,a \equiv 0 \pmod{p}$ jollain $k = 1, \ldots p-1$? No tämähän merkitsisi, että p olisi tekijänä $k\,a$:ssa.

Seuraus 7 vaatisi, että p on tekijänä k :ssa tai a :ssa, mutta kumpikaan ei päde. Tiedämmehän, että $\mathrm{syt}(p, a) = 1$ ja $\mathrm{syt}(p, k) = 1$, kun $k = 1, \ldots, p-1$, koska kerran p on alkuluku. Jonon (A) luvut ovat siis joukossa $\{1, \ldots, p-1\}$.

Lisäksi ne ovat kaikki erillisiä, sillä jos j ja k ovat joukossa $\{1, \ldots, p-1\}$ ja $j\,a \equiv k\,a \pmod{p}$, niin modsupistuslauseen 11 mukaan $j = k$.

Siinä kaikki. □

Huomaamme, että oikeastaan ainoa työkalu oli Modsupistuslause 11. Todistuksen juonen keksiminen on sitten aivan toinen juttu.

Pierre de Fermat esitti väitteen ystävälleen 18.10.1640 päivätyssä kirjeessään. Kuten miehen tapoihin kuului, hän ei tällekään väitteelle esittänyt todistusta. ("Lähettäisin myös todistuksen, ellen pelkäisi sen olevan liian pitkän.") Ensimmäinen tunnettu todistus on *Leibniz'n* julkaisemattomassa käsikirjoituksessa vuodelta 1683 ja ensimmäinen julkaistu on peräisin *Eulerilta* vuodelta 1736. Nämä ovat keskenään periaatteessa samanlaisia, binomikaavaan perustuvia, kokonaan toisenlaisia kuin yllä annettu.

Lauseelle on myöhemmin keksitty useita kiintoisia todistuksia. Kts. `http://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_little_theorem`. Uusimpien joukkoon kuuluu hollantilaisen tietojenkäsittelytieteen gurun ja vuoden 1972 *Turingin palkinnon* saajan *Edsger Dijkstra*'n vuonna 1980 keksimä kombinatorinen todistus. Sekin on yllä mainitussa viitteessä esitettynä.

Salakirjoitus tulee

Näillä pohjatiedoilla päästään käsiksi johdannossa mainittuun salakirjoitusmenetelmään, joka on aiheena seuraavassa Solmun numerossa ilmestyvässä osassa 2, toistaiseksi vain omien arkistojeni uumenissa piileskelevänä ja muotoaan hakevana salakirjoituksena.

Viitteet

[Algo] T.H. Cormen, C.E. Leiserson, R.L. Rivest: *Introduction to Algorithms*, The MIT Press, McGraw-Hill, 1998.

[Lukio1] Halmetoja, Häkkinen, Merikoski, Pippola, Silfverberg, Tossavainen, Laurinolli, Väänänen: *Lukuteoria ja logiikka, Matematiikan taito, syventävä kurssi 11*, WSOY

[Lukio2] Kangasaho, Mäkinen, Oikkonen, Paasonen, Salmela: *Logiikka ja lukuteoria*, Pitkä matematiikka, syventävä kurssi, WSOY

[NumberTH] Humphreys, Prest: *Numbers, groups and codes*, Cambridge U.P. 1989.

[Wiki] `http://en.wikipedia.org/wiki/Fermat's_little_theorem`

Kirjat [Lukio1] ja [Lukio2] ovat saman syventävän kurssin 11 keskenään vaihtoehtoisia kirjoja. Edellinen käsittelee tätä aihetta hiukan laajemmin.