# Lukuteorian alkeet

Anne-Maria Ernvall-Hytönen

15. helmikuuta 2013

# Sisältö

# Luku 1

# Johdanto

Lukuteoriasta voi rehellisesti sanoa, että jo muinaiset kreikkalaiset tutkivat sitä. Alkulukujen ääretöntä lukumäärää koskeva todistus löytyy jo Eukleidekseen Elementasta. Pythagoraan kolmion tuntevat kaikki (ja ennen kuin kukaan ehtii todeta, että sehän on geometriaa, niin todetaan, että kyllä, se on geometriaa, mutta liittyy se lukuteoriaankin, ja jos ei muuten usko, niin siitä voi tehdä harjoitustyönsä). Pythagoraan koulukunnan keskuudessa myös väitetään herättäneen suurta järkytystä havainnon, että $1 \times 1$-neliön halkaisija ei olekaan rationaaliluku, eli sitä ei voidakaan esittää kahden kokonaisluvun erotuksena. Tästä pitikin vaieta kuolemanrangaistuksen uhalla. (Ihan kuin asia olisi salaisuutena säilynyt...) Luultavasti pythagoraslaiset olisivat järkyttyneet vieläkin enemmän, jos he olisivat osanneet todistaa, että myös $\pi$ on irrationaalinen. Tämä säilyi kuitenkin vielä paljon pidempään avoimena ongelmana.

Vime vuosi(kymmeni)en aikana on päästy näkemään useita lukuteoreettisia menestystarinoita: Ensin Wiles ja Taylor todistivat Fermat'n viimeisen lauseen. Sitten Mihăilescu todisti Catalanin konjektuuri, eli että ainoat aidot potenssit, joiden erotus on vain yksi, ovat kahdeksan ja yhdeksän. Tämän jälkeen Green ja Tao osoittivat vielä, että alkulukujen joukossa on mielivaltaisen pitkiä aritmeettisia jonoja. Kuitenkin paljon on vielä todistamatta. Riemannin hypoteesi sinnittelee yhä. Lähes kaikki siihen uskovat (mutta ei kaikki), mutta todistusta ei vain löydy.

Tämän kurssin tavoitteena on antaa opiskelijalle perustiedot lukuteoriasta, hahmotus missä esimerkiksi lukuteoriaa käytetään, sekä jonkinlainen yleinen lukuteoreettinen yleissivistys.

Kurssi soveltuu kaikille matematiikan opiskelijoille. Kurssin suunnittelussa on erityisesti huomioitu lukiokurssin opetuksen tarpeet sekä sellaiset esimerkit, joilla olisi mahdollisimman paljon yleistä mielenkiintoa.

Monisteessa tulee olemaan materiaalia, jota ei luennoilla käydä läpi. Toisaalta luennoilla tullaan käsittelemään esimerkkejä, joita ei monisteesta löydy.

# Kirjallisuutta

[1] Paulo Ribenboim, *My Numbers, My Friends*

[2] Kenneth H. Rosen, *Elementary Number Theory and its Applications*

[3] Kalle Väisälä, *Lukuteorian ja korkeamman algebran alkeet*

# Luku 2

# Jaollisuus ja alkuluvut

## 2.1 Jaollisuus

Jaollisuus on perustavanlaatuinen käsite. Kaikki lukuteoriassa perustuu jossain mielessä jaollisuuteen. Kuitenkin määritelmä itsessään on suorastaan tylsän yksinkertainen:

**Määritelmä 1.** Luku $d$ *jakaa* luvun $n$, mikäli $\frac{n}{d}$ on kokonaisluku. Kirjoitetaan

$$d \mid n.$$

Lukua $d$ kutsutaan tällöin luvun $n$ jakajaksi tai tekijäksi. Mikäli taas $\frac{n}{d}$ ei ole kokonaisluku, sanotaan, että luku $d$ ei jaa lukua $n$. ja kirjoitetaan

$$d \nmid n.$$

Esimerkiksi siis $5 \mid 25$ (sillä $\frac{25}{5} = 5 \in \mathbb{Z}$), $1 \mid 100$ (sillä $\frac{100}{1} = 100 \in \mathbb{Z}$), mutta $6 \nmid 31$ (sillä $\frac{31}{6} \approx 5,167 \notin \mathbb{Z}$).

Luvun 24 jakajat ovat $1, 2, 3, 4, 6, 8, 12, 24$.

**Propositio 2.** Mikäli $d \mid a$ ja $d \mid b$, niin $d \mid an + bm$, missä $n$ ja $m$ ovat kokonaislukuja.

*Todistus.* Koska $d \mid a$, pätee $\frac{a}{d} = k \in \mathbb{Z}$, ja koska $d \mid b$. pätee $\frac{b}{d} = \ell \in \mathbb{Z}$. Nyt $\frac{an+bm}{d} = \frac{kd+\ell d}{d} = k + \ell \in \mathbb{Z}$. □

## 2.2 Alkuluvut

Alkuluvuksi kutsutaan positiivista kokonaislukua $p$, jolle pätee $p > 1$ ja luvun $p$ ainoat positiiviset tekijät ovat luku $p$ itse sekä luku yksi.

Ensimmäiset alkuluvut ovat $2, 3, 5, 7, 11, \ldots$.

Lukua, joka ei ole luku yksi, eikä alkuluku, kutsutaan *yhdistetyksi luvuksi.*

Induktiolla voi yksinkertaisesti todistaa, että jokainen lukua yksi suurempi positiivinen luku on jaollinen ainakin jollakin alkuluvulla (kannattaa huomata, että luku voi itse olla tämä alkuluku).

Seuraavalle tulokselle on olemassa paljon erilaisia todistuksia – jopa topologinenkin löytyy. Keskitytään nyt kuitenkin perinteiseen, suorastaan antiikkiseen todistukseen:

**Lause 3.** *Alkulukuja on äärettömän paljon.*

*Todistus.* Tehdään vastaoletus: Kaikki alkuluvut ovat $q_1, q_2, \cdots q_n$. Tarkastellaan lukua $m = q_1 q_2 \cdots q_n + 1$. Selvästi luku on suurempi kuin mikään luvuista $q_1, q_2, \ldots, q_n$, joten tähän rimpsuun se ei voi kuulua, joten se ei ole alkuluku. Edellä todetun nojalla sen on kuitenkin oltava jollakin alkuluvulla jaollinen. Olkoon tämä alkuluku $q_k$. Nyt $q_k \mid m$ ja selvästi $q_k \mid q_1 q_2 \cdots q_n$, joten $q_k \mid (m - q_1 q_2 \cdots q_n)$, eli $q_k \mid 1$. Tämä on ristiriita. Vastaoletus oli siis väärä ja alkuperäinen väite tosi. □

### 2.2.1 Alkutekijät ja alkutekijähajotelman yksikäsitteisyys

**Määritelmä 4.** Luvun $n$ *alkutekijäksi* kutsutaan sellaisia alkulukuja $p$, jotka jakavat luvun $n$.

Esimerkiksi luvun 30 alkutekijät ovat 2, 3 ja 5.

Nyt huijataan hiukan. Oikeasti meillä ei ole tässä vaiheessa kurssia vielä valmiuksia todistaa seuraavaa harvinaisen triviaalintuntuista lausetta (joka itse asiassa ei olekaan ihan triviaali, eli kaikissa lukujärjestelmissä se ei päde). Suhteellisen pian kurssilla on kuitenkin kasattu teoriaa, jotta lause voidaan todistaa.

**Lause 5** (Alkutekijähajotelman yksikäsitteisyys)**.** *Positiivisella kokonaisluvulla $n$ on järjestystä vaille yksikäsitteinen esitys alkulukujen tulona, eli luku $n$ voidaan esittää vain yhdellä tavalla muodossa*

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

*kun vaaditaan, että $\alpha_1, \alpha_2, \ldots, \alpha_k > 0$ (kokonaislukuja) ja luvut $p_j$ ovat alkulukuja, joille pätee $p_j \neq p_\ell$, kun $j \neq \ell$ ja tulontekijöiden järjestyksen vaihtaminen sallitaan.*

Ehkäpä yksinkertaisin esimerkki tilanteesta, jolloin alkutekijähajotelma ei ole yksikäsitteinen, on tarkastella muotoa $4k + 1$ olevia positiivisia kokonaislukuja. Tämä joukko on selvästi suljettu kertolaskun suhteen. Joukon alkuluvuiksi määritellään sellaiset luvut, jotka eivät tässä joukossa hajoa pienemmiksi tekijöiksi. Luku 1 on joukon yksikkö. Alkulukuja tässä joukossa ovat siis esimerkiksi $5, 9, 13, 17, 21, 29, \ldots$ Nyt tässä joukossa voidaan luku 441 jakaa seuraavasti alkutkeijöihin:

$$441 = 9 \times 49 = 21^2,$$

sillä mikään luvuista $9, 21, 49$ ei muotoa $4k + 1$ olevien lukujen joukossa hajoa.

## 2.3 Erastostheneen seula

Alkulukujen etsiminen on eräs ongelma. On suhteellisen hidasta selvittää yksittäisestä luvusta varmasti, onko se alkuluku vai ei. Eräs mahdollisuus on tietenkin n.s. brute force -menetelmä: jaetaan yksitellen kaikkia lukua pienemmilla luvuilla (tai alkuluvuilla), ja jos jako ei koskaan mene tasan, on pakko olla kyseessä alkuluvun. Tarkasti ottaen tässä riittäisi luvun neliöjuurta pienemmillä luvuilla jakaminen, eli luku $n$ on alkuluku jos ja vain jos

$$\forall d \in \mathbb{Z},\ 1 < d < \sqrt{n} : \frac{n}{d} \notin \mathbb{Z}$$

Tehokkaampiakin tapoja on olemassa, jopa polynoamiajassa toimiva, ja näistä aiheista innostuessaan voi toisen harjoitustyön tehdä alkulukutestauksesta.

Keskitytään nyt kuitenkin alkulukujen etsintään isosta joukosta: Halutaan löytää kaikki alkuluvut, jotka ovat korkeintaan luvun $n$ kokoisia. Tähän eräs hyvin yksinkertainen menetelmä on Erastostheneen seula. Seulan pääperiaate on tämä: Listataan kokonaisluvut väliltä $[2, n]$. Havaitaan, että luku 2 on alkuluku. Viivataan tämän jälkeen yli kaikki luvulla 2 jaolliset luvut. Seuraava yliviivaamaton luku taulukossa on alkuluku (tässä tapauksessa siis luku 3). Viivataan nyt yli kaikki luvulla 3 jaolliset luvut, paitsi luku 3 itse. Seuraava taulukossa yliviivaamaton luku on taas alkuluku, ja viivataan yli kaikki sillä jaolliset luvut, paitsi luku itse. Jatketaan näin. Kuitenkin riittää yliviivata vain korkeintaan luvun $\sqrt{n}$ suuruisilla luvuilla, koska kuten aiemmin todettu, mikäli luku ei ole alkuluku, on sillä oltava korkeintaan neliöjuurensa kokoinen tekijä.

Otetaan esimerkki valottamaan miten homma oikeasti toimii.

**Esimerkki 6.** Halutaan listata kaikki alkuluvut väliltä $[2, 40]$. Lasketaan ensin $\sqrt{40} \approx 6,3$, joten kaikilla korkeintaan luvun 40 suuruisilla yhdistetyillä luvuilla on tekijä, joka on korkeintaan kuusi. Listataan nyt luvut:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | |

Luku 2 on alkuluku. Vedetään siis yli kaikki sillä jaolliset luvut paitsi luku kaksi itse:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | |

Luku kolme on seuraava yliviivaamaton luku. Se on siis alkuluku. Viivataan nyt yli sillä jaolliset luvut, paitsi luku kolme itse:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | |

Seuraava yliviivaamaton luku on viisi. Se on siis alkuluku. Viivataan nyt yli sillä jaoliset luvut, paitsi luku viisi itse:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ | 11 |
| ~~12~~ | 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ | ~~21~~ |
| ~~22~~ | 23 | ~~24~~ | ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ | 31 |
| ~~32~~ | ~~33~~ | ~~34~~ | ~~35~~ | ~~36~~ | 37 | ~~38~~ | ~~39~~ | ~~40~~ | |

Seuraava yliviivaamaton luku on seitsemän. Kuitenkin $7 > 6,3 \approx \sqrt{40}$, jolloin kaikilla joukon $\{2, 3, \ldots, 40\}$ yhdistetyillä luvuilla on lukua seitsemän pienempi alkutekijä. Täten kaikki tarkistukset on tehty, ja kaikki yliviivaamattomat luvut ovat alkulukuja. Joukon $\{2, 3, \ldots, 40\}$ alkuluvut ovat siis $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$.

### 2.3.1 Mersennen alkuluvut ja GIMPS

Mersennen alkuluvuksi kutsutaan alkulukua, joka on muotoa

$$2^b - 1.$$

On varsin helppo nähdä, että luvun $b$ on tällöin oltava alkuluku. (Miksi?) Merkitään siis

$$M(p) = 2^p - 1.$$

Kuitenkaan kaikki tällaiset luvut eivät alkulukuja ole, vaan esimerkiksi

$$M(11) = 2^{11} - 1 = 2047 = 23 \cdot 89.$$

Verkossa toimii GIMPS-projekti (Great Internet Mersenne Prime Search) osoitteessa

`http://www.mersenne.org/`

Projektin tarkoituksena on tarkastella valtavia Mersennen lukuja, ja selvittää ovatko ne alkulukuja vai ei.

Tällä hetkellä ainoastaan 47 Mersennen alkulukua on löytynyt. Pienin näistä on (luonnollisestikin) $M(2) = 3$ ja suurin $M(43112609)$, jossa on huimaavat 12978189 numeroa kymmenjärjestelmäesityksessä.

Kysymys onko Mersennen alkulukuja äärellinen vai ääretön määrä on avoin. Äärettömään määrään yleisesti uskotaan.

## 2.4 Alkulukujen jakaumasta

### 2.4.1 Bertrandin postulaatti

Eräs mielenkiintoinen kysymys lukuteoriassa on alkulukujen jakauma. Kuinka lähellä annettua lukua on jonkin alkuluvun oltava?

Niin kutsutun alkulukukaksoskonjektuurin mukaan on äärettömän paljon alkulukukaksosia, eli sellaisia alkulukuja, joiden etäisyys on vain kaksi. Tämä ongelma on kuitenkin avoin. Toinen äärilaita ongelmaa on mahdollisimman pitkän etäisyyden saavuttaminen: Voiko alkulukua $p$ seuraava alkuluku olla vaikkapa suuruusluokkaa $3p$? Entä $p^2$? Vastaus molempiin kysymyksiin on: Ei. Ei missään nimessä. Konjekturoitu on, että välillä $[x, x+cx^{\varepsilon}]$ on alkuluku, ja tässä $c$ on vakio, joka riippuu luvusta $\varepsilon$, joka puolestaan voidaan valita mielivaltaisen pieneksi positiiviseksi luvuksi. Tämä ongelma on vielä auki. Seuraava Bertrandin postulaatin nimellä tunnettu tulos antaa erään rajan:

**Lause 7.** *Olkoon $n \geq 2$. Luvun $n$ ja $2n$ välissä on aina alkuluku.*

Tämän lauseen todistuksesta on harjoitustehtäväsarja niille, jotka suorittavat kurssin syventävinä opintoina.

### 2.4.2 Alkulukulause

Alkulukulause on matematiikan historiankin kannalta merkittävä. Sen todistus oli avoin hyvin pitkään, ja lopulta Riemann tarjosi hahmotelman todistukselle. Tämän todistuksen eräänä lemmana olisi pitänyt osoittaa, että funktion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

joka voidaan ns. *analyyttisesti jatkaa* koko kompleksitasoon, epätriviaalit nollakohdat ovat suoralla $\Re s = \frac{1}{2}$. Tämä väite tunnetaan nykyään Riemannin hypoteesina, ja se on lukuteorian tunnetuin avoin ongelma, ehkäpä jopa koko matematiikan tunnetuin avoin ongelma.

Alkulukulause tuli kuitenkin todistettua. Todistukseen ei lopulta tarvittukaan koko Riemannin hypoteesia, vaan riitti tieto, että suoralla $\Re s = 1$ ei nollakohtia ole. Lauseen todistivat yhtä aikaa ja toisistaan riippumattomasti Hadamard ja de la Vallée Poussin. Lauseen mukaan

$$|\{n \leq x : \ n \text{ alkuluku}\}| \sim \ \frac{x}{\log x},$$

missä $\sim$ tarkoittaa sitä, että tulos ei ole tarkka, mutta virhetermi on (tietyssä mielessä) merkittävästi pienempi kuin päätermi. Virhetermin tarkka arvo riippuu Riemannin hypoteesista.

## 2.5 Erilaisia tekijäfunktioita

Luvun tekijöiden avulla voidaan muodostaa kaikenlaisia funktioita. Tarkastellaan nyt kahta hyvin yksinkertaista funktiota:

$$\tau(n) = \sum_{d|n, d>0} 1$$

ja

$$\sigma(n) = \sum_{d|n, d>0} d.$$

On helppo nähdä, että mikäli luvun $n$ alkutekijähajotelma on

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

niin

$$\tau(n) = \prod_{j=1}^{k} (\alpha_j + 1)$$

ja

$$\sigma(n) = \prod_{j=1}^{k} \frac{p_j^{\alpha_j+1} - 1}{p_j - 1}.$$

### 2.5.1 Täydelliset luvut

*Täydelliseksi luvuksi* kutsutaan sellaista lukua, jonka kaikkien positiivisten tekijöiden summa on kaksi kertaa luvun oma arvo. Esimerkiksi luvun 6 tekijät ovat $1, 2, 3, 6$, ja niiden summa on $1 + 2 + 3 + 6 = 12 = 2 \cdot 6$, joten luku 6 on täydellinen. Toisaalta taas esimerkiksi luvun 7 positiiviset tekijät ovat 1 ja 7. Koska $1 + 7 = 8 \neq 14 = 2 \cdot 7$, eli luku 7 ole täydellinen.

Laskuharjoituksissa tullaan osoittamaan seuraava yhteys Mersennen alkulukujen ja täydellisten lukujen välillä: Mersennen alkuluvun avulla voidaan konstruioida parillinen täydellinen luku. Itse asiassa pätee myös, että jokaista parillista täydellistä lukua vastaa Mersennen alkuluku. On siis yhtäpitävää väittää, että Mersennen alkulukuja on äärettömästi kuin että parillisia täydellisiä lukuja on äärettömästi, mutta kumpaakaan ei ole todistettu.

Parittomien täydellisten lukujen kohdalla tilanne on vielä heikompi: Niitä ei ole yhtään löydetty, eikä niiden olemassaoloon myöskään uskota.

# Luku 3

# Ensimmäisen asteen Diofantoksen yhtälöt

Tämän luvun tarkoituksena on tarkastella yksinkertaisia ensimmäisen asteen Diofantoksen yhtälöitä, eli etsiä kokonaislukuratkaisuja $(x, y)$ yhtälölle

$$ax + by = c,$$

missä $a$, $b$ ja $c$ ovat kokonaislukuja. Ennen yhtälöihin siirtymistä tarvitsemme hieman teoriaa.

Lukijalle varoituksena, että teoria saattaa näyttää kaoottiselta tai karmealta aluksi, mutta asiaa avataan luennoilla, ja menetelmät aukeavat parin esimerkin jälkeen paremmin. Toisin sanoen, asia ei ole niin raskasta kuin miltä näyttää.

## 3.1 Suurin yhteinen tekijä

Aloitetaan määrittelemällä suurin yhteinen tekijä:

**Määritelmä 8.** Lukujen $a$ ja $b$ suurin yhteinen tekijä (eli syt) on suurin positiivinen $d \in \mathbb{Z}$, joka jakaa sekä luvun $a$ että luvun $b$.

Huomataan ensin, että suurimman yhteisen tekijän laskeminen voidaan siirtää pienemmille luvuille:

**Lause 9.** *Pätee* $syt(a, b) = syt(a - b, b)$.

*Todistus.* Jos $d \mid a$ ja $d \mid b$, niin $d \mid (a - b)$. Täten $d \mid \text{syt}(a - b, b)$e, eli $\text{syt}(a.b) \mid \text{syt}(a - b, b)$Toisaalta, jos $d' \mid a - b$ ja $d' \mid b$, niin $d' \mid (a - b) + b = a$, joten $\text{syt}(a - b, b) \mid \text{syt}(a, b)$. Lause on todistettu. □

## 3.2 Eukleideksen algoritmi

Eukleideksen algoritmi on hyvin tehokas tapa laskea suurin yhteinen tekijä. Se toimii seuraavasti:

Oletetaan, että $a > b$. Kirjoitetaan nyt $a = bq_1 + r_1$, missä $0 \leq r_1 < b$. Mikäli $r_1 = 0$, on homma valmis. Jos ei ole, niin kirjoitetaan $b = r_1q_2 + r_2$, missä $0 \leq r_2 < r_1$. Mikäli $r_2 = 0$, on homma valmis. Jos näin ei ole, niin jatketaan kirjoittamalla $r_1 = r_2q_3 + r_3$, missä $0 \leq r_3 < r_2$, ja näin jatketaan, kunnes jokin $r_k = 0$. Tällöin $\text{syt}(a, b) = r_{k-1}$.

**Perustelu:** $\text{syt}(a, b) = \text{syt}(a-b, b) = \text{syt}(a-2b-b) = \cdots = \text{syt}(a-q_1b, b) = \text{syt}(r_1, b)$. Vastaavasti $\text{syt}(r_1, b) = \text{syt}(r_1, r_2)$. Näin voidaan jatkaa, ja saadaan lopulta $\text{syt}(a, b) = \text{syt}(r_{k-1}, r_{k-2}) = r_{k-1}$. Algoritmi päättyy, kun jako menee tasan, eli $r_k = 0$ silloin ja vain silloin, kun $r_{k-1} \mid r_{k-2}$, josta syystä $\text{syt}(r_{k-1}, r_{k-2}) = r_{k-1}$.

**Esimerkki 10.** Tarkastellaan nyt esimerkin luontoisesti lukujen 56 ja 44 suurimman yhteisen tekijän laskemista:

$$56 = 1 \cdot 44 + 12,$$

joten $\text{syt}(56, 44) = \text{syt}(44, 12)$. Vastaavasti voidaan tehdä seuraavat

$$\begin{aligned} 44 &= 3 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 + 0, \end{aligned}$$

joten $\text{syt}(56, 44) = 4$.

## 3.3 Ensimmäisen asteen Diofantoksen yhtälöt (vihdoinkin)

Tarkoituksemme on nyt tarkastella milloin yhtälöllä $ax + by = c$ on kokonaislukuratkaisu, sekä lisäksi selvittää miten nämä kokonaislukuratkaisut voi löytää.

Aloitetaan tilanteella, jossa Diofantoksen yhtälöllä ei ole ratkaisua

**Lause 11.** *Mikäli $\text{syt}(a, b) \nmid c$, ei Diofantoksen yhtälöllä*

$$ax + by = c$$

*ole ratkaisua.*

*Todistus.* Tällöin $\text{syt}(a, b) \mid a, b$, eli $\text{syt}(a, b) \mid ax + by$ kaikilla kokonaisluvuilla $x$ ja $y$. Toisaalta luku $c$ ei ole luvulla $\text{syt}(a, b)$ jaollinen, joten yhtälö on mahdoton. □

Osoitetaan seuraavaksi, että aina muulloin ratkaisu on olemassa, sekä samalla konstruoidaan tapa löytää yksi ratkaisu.

**Lause 12.** *Yhtälöllä $ax + by = \text{syt}(a, b)$ on ratkaisu.*

*Todistus.* Voidaan olettaa, että $a > b$. Kirjoitetaan Eukleideksen algoritmi luvuille $a$ ja $b$:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\dots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k, \end{aligned}$$

jolloin $\text{syt}(a, b) = r_k$. Ratkaistaan nyt ylläolevista yhtälöistä jäännökset (paitsi viimeisestä, jossa jäännöstä ei ole):

$$\begin{aligned} r_1 &= a - q_1 b \\ r_2 &= b - q_2 r_1 \\ r_3 &= r_1 - q_3 r_2 \\ &\dots \\ r_{k-1} &= r_{k-3} - q_{k-1} r_{k-2} \\ r_k &= r_{k-2} - q_k r_{k-1}. \end{aligned}$$

Viimeinen yhtälö esittää luvun $r_k$ lukujen $r_{k-1}$ ja $r_{k-2}$ avulla. Toiseksi viimeinen yhtälö taas esittää luvun $r_{k-1}$ lukujen $r_{k-2}$ ja $r_{k-3}$ avulla. Yleisesti yhtälöt ovat muotoa $r_j = r_{j-2} - q_j r_{j-1}$. Sijoitetaan luvun $r_{k-1}$ tilalle viimeisessä yhtälössä toiseksi viimeisen yhtälön antama lauseke luvulle $r_{k-1}$:

$$r_k = r_{k-2} - q_k r_{k-1} = r_{k-2} - q_k \left(r_{k-3} - q_{k-1} r_{k-2}\right) = (1 + q_k q_{k-1}) r_{k-2} - q_{k-1} r_{k-3}$$

Sijoitetaan tähän termin $r_{k-2}$ paikalle yhtälön $r_{k-2} = r_{k-4} - q_{k-2} r_{k-3}$ antama lauseke:

$$\begin{aligned} r_k = (1 + q_k q_{k-1}) r_{k-2} - q_{k-1} r_{k-3} &= (1 + q_k q_{k-1})(r_{k-4} - q_{k-2} r_{k-3}) - q_{k-1} r_{k-3} \\ &= (1 + q_k q_{k-1}) r_{k-4} - (q_{k-2} + q_k q_{k-1} q_{k-2} - q_{k-1}) r_{k-3}, \end{aligned}$$

ja seuraavaksi taas korvataan luku $r_{k-3}$ vastaavasti lausekkeellaan, sitten $r_{k-4}$, kunnes lopulta olemme saaneet esitettyä luvun $r_k = \text{syt}(a, b)$ lausekkeena

$$r_k = a c_1 + b c_2,$$

missä kertoimet $c_1$ ja $c_2$ riippuvat luvuista $q_j$. Tämä todistaa väitteen. Ratkaisuksi käyvät kertoimet $c_1$ ja $c_2$. □

**Lause 13.** *Mikäli* $\text{syt}(a, b) \mid c$, *on yhtälöllä* $ax + by = c$ *ratkaisu*

*Todistus.* Mikäli $\text{syt}(a, b) = c$, on tämä ratkaisu löydetty jo edellisessä lauseessa. Oletetaan siis, että $c = d\text{syt}(a, b)$. Olkoon $(x_0, y_0)$ yhtälön $ax + by = \text{syt}(a, b)$ ratkaisu. Tällöin $(dx_0, dy_0)$ on yhtälön $ax + by = c$ ratkaisu, sillä $adx_0 + bdy_0 = d\text{syt}(a, b) = c$. □

**Lause 14.** *Homogeenisen yhtälön $ax + by = 0$ yleinen ratkaisu on $x = \frac{b}{syt(a,b))}k$ ja $y = -\frac{a}{syt(a,b))}k$.*

*Todistus.* Tarkastellaan yhtälöä $ax + by = 0$. Nyt $ax = -by$, eli $\frac{a}{\text{syt}(a,b)}x = -\frac{b}{\text{syt}(a,b)}y$. Koska $\text{syt}(\frac{a}{\text{syt}(a.b)}, \frac{b}{\text{syt}(a,b)}) = 1$, pätee $\frac{b}{\text{syt}(a.b)} \mid x$ ja $\frac{a}{\text{syt}(a.b)} \mid y$. Kirjoitetaan $x = \frac{b}{\text{syt}(a.b)}x'$ ja $y = \frac{a}{\text{syt}(a.b)}y'$, jolloin yhtälö muuttuu muotoon $\frac{a}{\text{syt}(a,b)} \cdot \frac{b}{\text{syt}(a,b)}x' = -\frac{b}{\text{syt}(a,b)} \cdot \frac{a}{\text{syt}(a,b)}y'$, eli $x' = -y'$. Täten luvuille $x'$ ja $y'$ ei ole muita rajoituksia kuin että ne ovat kokonaislukuja ja toistensa vastalukuja. Parametrisoidaan $x' = y' = k$, jolloin ratkaisut ovat $(\frac{b}{\text{syt}(a,b))}k, -\frac{a}{\text{syt}(a,b)}k)$. □

**Lause 15.** *Mikäli Diofantoksen yhtälöllä $ax + by = c$ on yksi ratkaisu, on sillä äärettömän monta ratkaisua, ja ne saadaan summaamalla mikä tahansa yksittäisratkaisu homogeenisen yhtälön $ax + by = 0$ yleiseen ratkaisuun.*

*Todistus.* Olkoot $(x_1, y_1)$ ja $(x_2, y_2)$ yhtälön $ax + by = c$ ratkaisu. Tällöin $a(x_1 - x_2) + b(y_1 - y_2) = 0$, joten $(x_1 - x_2, y_1 - y_2)$ on homogeenisen yhtälön jokin ratkaisu. Väite on todistettu. □

Päätetään tämä luku esimerkkiin.

**Esimerkki 16.** Ratkaistaan Diofantoksen yhtälö $44x + 56y = 4$. Aiemmin tässä luvussa laskettiin $\text{syt}(56, 44)$. Laskuketju uudelleen kirjoittaen saadaan

$$\begin{aligned} 12 &= 56 - 1 \cdot 44 \\ 8 &= 44 - 3 \cdot 12 \\ 4 &= 12 - 1 \cdot 8, \end{aligned}$$

joten sijoittaen saadaan

$$4 = 12 - 8 = 12 - (44 - 3 \cdot 12) = 4 \cdot 12 - 44 = 4(56 - 44) - 44 = 4 \cdot 56 - 5 \cdot 44.$$

Yksi ratkaisu on siis $x = -5$ ja $y = 4$. Homogeenisen yhtälön $44x + 56y = 0$ ratkaisut taas ovat $x = 14k$ ja $y = -11k$. Yhtälön $44x + 56y = 4$ kaikki kokonaislukuratkaisut siis ovat $x = -5 + 14k$ ja $y = 4 - 11k$.

## 3.4 Alkutekijähajotelman yksikäsitteisyyden todistus

Tarvitaan vielä seuraava lemma ennen varsinaista todistusta:

**Lemma 17.** *Olkoon $p$ alkuluku. Mikäli $p \mid ab$, ja $p \nmid b$, niin $p \mid a$.*

*Todistus.* Koska $p$ on alkuluku ja $p \nmid b$, on pädettävä $\text{syt}(p, b) = 1$. Tällöin on olemassa kertoimet $x$ ja $y$, joilla $px + by = 1$. Koska $p \mid ab$, erityisesti pätee $p \mid aby$, eli $p \mid a(1 - px)$. Koska pätee myös $p \mid apx$, pätee siis $p \mid apx + a(1 - px) = a$. Väite on todistettu. □

Tämän jälkeen alkutekijähajotelman yksikäsitteisyyden todistus tipahtaa yksinkertaisesti: Tehdään vastaoletus: Luvulla $n$ on kaksi erilaista alkutekijähajotelmaa, eli pätee yhtälö,

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}.$$

Voidaan lisäksi olettaa, että alkuluvut $p_1, p_2, \ldots, p_k$ ovat kaikki erisuuria kuin luvut $q_1, q_2, \ldots, q_\ell$, sillä mikäli jotkin alkuluvut olisivat samat, voisimme sieventää vastaavan tekijän pois yhtälöstä.

Nyt $p_1 \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$. Koska $p_1 \neq q_1, q_2, \ldots, q_\ell$, pätee $p_1 \nmid q_1^{\beta_1}, q_2^{\beta_2}, \ldots, q_\ell^{\beta_\ell}$. Erityisesti, koska $p_1 \nmid q_1^{\beta_1}$, on pädettävä edellisen lemman nojalla $p_1 \mid q_2^{\beta_2} q_3^{\beta_3} \cdots q_\ell^{\beta_\ell}$. Kuitenkin, koska $p_1 \nmid q_2^{\beta_2}$, on jälleen edellisen lemman nojalla pädettävä $p_1 \mid q_3^{\beta_3} q_4^{\beta_4} \cdots q_\ell^{\beta_\ell}$. Voidaan näin jatkaa, kunnes on lopulta pädettävä $p_1 \mid q_\ell^{\beta_\ell}$, mikä on ristiriita. Näin saatiin todistettua alkutekijähajotelman yksikäsitteisyys.

# Luku 4

# Kongruenssit

Lukujen $a$ ja $b$ sanotaan olevan kongruentit keskenään modulossa $n$ (tai "luku $a$ on kongruentti luvun $b$ kanssa modulo $n$), mikäli

$$n \mid (a - b).$$

Tätä merkitään

$$a \equiv b \pmod{n}.$$

Tämä siis tarkoittaa, että $a-b = kn$ jollain kokonaisluvulla $k$. Jos näin ei ole, niin merkitään

$$a \not\equiv b \pmod{n}$$

Esimerkiksi siis $3 \equiv 7 \pmod{4}$ ja $105 \equiv 55 \pmod{25}$.

**Lause 18.** *Kongruensseille pätevät seuraavat laskusäännöt: Jos*

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

*niin*

$$a \pm c \equiv b \pm d \pmod{n} \quad ja \quad ac \equiv bd \pmod{n}.$$

*Todistus.* Todistus on helppo tehdä jaollisuuden ominaisuuksilla: Oletuksista saadaan $n \mid (a - b)$ ja $n \mid (c - d)$, eli $n \mid ((a - b) + (c - d)) = (a + c) - (b + d)$ ja $n \mid (a - b) - (c - d) = ((a - c) - (b - d))$, mitkä ovatkin yhtäpitäviä kahden ensimmäisen väitteen kanssa.

Kertolaskun todistus on suurinpiirtein yhtä yksinkertainen: $n \mid a - b$ ja $n \mid c - d$, joten

$$n \mid (c(a - b) + b(c - d)) = ac - bd.$$

□

Kertolaskusta seuraavat erikostapauksena potenssit:

**Lause 19.** *Jos* $a \equiv b \pmod{n}$, *niin* $a^m \equiv b^m \pmod{n}$ *kaikilla epänegatiivisilla kokonaisluvuilla* $m$.

On syytä huomata, että jakolasku ei toimi näin yksinkertaisesti, vaan jakolaskun suhteen on syytä olla varsin varovainen. Esimerkiksi yhtälö

$$2 \equiv 6 \pmod 4$$

on tosi, mutta jos yhtälö jaetaan puolittain luvulla 2, saadaan paikkansapitämätön $1 \equiv 3 \pmod 4$. Tämä johtuu siitä, että luku 2 jakaa luvun 4, eli modulon. Sen sijaan, jos myös modulo jaettaisiin luvulla 2, menisi kaikki hyvin. Toisaalta, jos ylläoleva yhtälö haluttaisiin jakaa luvulla 3, ei välttämättä olisi mitenkään selvää, mitä tällä oikein tarkoitetaan. Järkevää siis onkin ajatella jakaminen tarkoittamaan käänteisluvulla kertomista, ja käytännössä seuraava menetelmä toimii jakolaskuille oikein hyvin:

Halutaan jakaa yhtälö $a \equiv b \pmod n$ luvulla $d$. Kerrotaan siis luvun $d$ käänteisluvulla, eli sellaisella luvulla $d'$. että

$$dd' \equiv 1 (\text{mod } n).$$

Tämä on yhtäpitävää sen kanssa, että $n \mid dd' - 1$, eli $dd' - 1 = xn$, eli $dd' - xn = 1$. Tämä on ensimmäisen asteen Diofantoksen yhtälö, jonka yleinen ratkaisu voidaan kirjoittaa muodossa $d' = d_0 + nk$ ja $x = x_0 + dk$, missä $(d_0, x_0)$ on yksittäistapauksen ratkaisu. Ennen kaikkea huomaamme, että $d' \equiv d_0 \pmod n$. Täten siis jakaminen luvulla $d$ voidaan suorittaa kertomalla yhtälö puolittain luvulla $d_0$, joka on Diofantoksen yhtälön yksittäisratkaisu.

Erikoistapauksena voimme nähdä, että mikäli tarkastelemme kongruenssia muotoa $da \equiv db \pmod n$, ja mikäli $\text{syt}(n, d) = 1$, niin tällöin myös $a \equiv b \pmod n$.

Luvut $a_1, a_2, \ldots a_n$ muodostavat *jäännössysteemin* modulo $n$, mikäli $a_j \not\equiv a_i \pmod n$, kun $i \neq j$. Esimerkiksi siis luvut $0, 1, 2, \ldots, n-1$ muodostavat jäännössysteemin modulo $n$, eli jäännössysteemissä on jokainen jäännösluokka edustettuna. Mikäli jäännössysteemistä poistetaan ne luvut, joilla on yhteisiä tekijöitä luvun $n$ kanssa, saadaan lukujoukko, jota voidaan kutsua *redusoiduksi jäännössysteemiksi.*

**Esimerkki 20.** Luvut $3, 4, 5, 6, 7$ muodostavat jäännössysteemin modulo 5. Myös esimerkiksi luvut $100, 101, 102, 103, 104$ muodostavat jäännössysteemin modulo 5. Luvut $3, 4, 6, 7$ puolestaan muodostavat redusoidun jäännössysteemin modulo 5.

Otetaan luvun loppuun esimerkki kongruensseilla laskemisesta.

**Esimerkki 21.** Todistetaan luvun 9 jaollisuussääntö, eli että luku on yhdeksällä jaollinen jos ja vain jos sen kymmenjärjestelmäesityksen numeroiden summa on jaollinen yhdeksällä.

Luvun $n$ kymmenjärjestelmäesitys voidaan kirjoittaa muodossa

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots a_1 10 + a_0.$$

Nyt $10 \equiv 1 \pmod 9$, joten $10^k \equiv 1^k \equiv 1 \pmod 9$. Siispä

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots a_1 10 + a_0 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 9.$$

## 4.1 Fermat'n pieni lause ja yleistys

Fermat'n pieni lause helpottaa huomattavasti potenssien sieventämistä kongruensseilla laskettaessa:

**Lause 22.** *Olkoon $p$ alkuluku ja $\text{syt}(a,p)=1$. Nyt*

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Todistus.* Luvut $a, 2a, 3a, \ldots, (p-1)a$ muodostavat redusoidun jäännössysteemin, sillä jos $aj \equiv ak \pmod{p}$, niin $j \equiv k \pmod{p}$, eli $j = k$, koska $0 < j, k \leq p-1$. Täten

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1),$$

sillä molemmilla puolilla yhtälöä ovat samojen jäännösluokkien edustajat. Siispä

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

Tällainen yhtälö voidaan jakaa puolittain, sillä $\text{syt}((p-1)!, p) = 1$, joten

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Valotetaan nyt Fermat'n pienen lauseen käyttöä esimerkillä:

**Esimerkki 23.** Halutaan osoittaa, että $7 \mid 5^{600} - 1$. Huomataan aluksi, että $\text{syt}(7,5) = 1$. Siispä

$$5^6 \equiv 1 \pmod{7}.$$

Kongruenssien laskusäännöillä pätee myös

$$5^{600} = \left(5^6\right)^{100} \equiv 1^{100} = 1 \pmod{7}.$$

Täten $5^{600} - 1 \equiv 0 \pmod{7}$, eli $7 \mid 5^{600} - 1$.

### 4.1.1 Eulerin $\varphi$-funktio ja Eulerin lause

Eulerin $\varphi$-funktio kertoo kuinka moni korkeintaan luvun $n$ suuruinen luku on yhteistekijätön luvun $n$ kanssa, eli

$$\varphi(n) = \left|\{1 \leq m < n : \ \text{syt}(n,m) = 1\}\right|.$$

Esimerkiksi siis $\varphi(8) = 4$ ja $\varphi(30) = 8$.

Mikäli $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (luvun $n$ alkutekijähajotelma), niin

$$\varphi(n) = \prod_{j=1}^{k} p_j^{\alpha_j - 1}(p_j - 1).$$

Tämän todistus on laskuharjoituksissa.

Eulerin lause on Fermat'n pienen lauseen yleistys, ja todistuskin on itse asiassa samanlainen.

**Lause 24.** *Olkoon syt*$(a, n) = 1$. *Tällöin*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

## 4.2 Kongruenssiyhtälöt

Kongruenssiyhtälöksi kutsutaan yhtälöä, jolle yritetään löytää ratkaisuja jossain modulossa, esimerkiksi siis yhtälö

$$m^2 \equiv 1 \pmod{8}$$

on kongruenssiyhtälö. Tämän ratkaisuja ovat kaikki parittomat $m$, eli kaikki sellaiset $m$, joilla pätee $m \equiv 1, 3, 5, 7 \pmod{8}$ (ks. ekat laskarit).

Toinen esimerkki kongruenssiyhtälöstä on yhden muuttujan lineaarinen kongruenssiyhtälö

$$4x + 3 \equiv 5 \pmod{7}$$

Tämä on yhtäpitävää sen kanssa, että $4x \equiv 2 \pmod{7}$. Näin pienillä luvuilla ratkaisun voi löytää kokeilemallakin. Yleispätevämpi menetelmä on kuitenkin muuttaa yhtälö Diofantoksen yhtälöksi:

$$4x + 7y = 2.$$

Tämän yhtälön yleinen ratkaisu on $x = 4 + 7k$ ja $y = -2 - 4k$. Luvulle $x$ pätee siis $x \equiv 4 \pmod{7}$.

Luonnollisestikin voi tarkastella myös useamman muuttujan kongruenssiyhtälöitä. Esimerkiksi yhtälöllä

$$x^2 + y^2 \equiv 3 \pmod{4}$$

ei ole ratkaisuja, sillä parillisten lukujen neliöt ovat neljällä jaollisia, eli $\equiv 0 \pmod{4}$ ja parittomien lukujen neliöt taas $\equiv 1 \pmod{4}$.

Palataan nyt vielä lineaarisiin yhden muuttujan kongruenssiyhtälöihin: Olkoon syt$(a, n) = 1$ Yhtälö

$$ax + b \equiv c \pmod{n}$$

ratkaistaan vaikkapa seuraavasti:

1. Siirrä $b$ toiselle puolelle yhtälöä: $ax \equiv c - b \pmod{n}$
2. Määritetään luvun $a$ käänteisluku modulo $n$ etsimällä Diofantoksen yhtälölle $ax - ny = 1$ yksi ratkaisu. Olkoon tämä ratkaisu $(a', n')$
3. Kerrotaan yhtälön puolittain luvulla $a'$, jolloin

$$x \equiv a'(c - b) \pmod{n}.$$

Vaiheet 2) ja 3) voi myös tehdä kokeilemalla tai suosiolla etsimällä suoraan Diofantoksen yhtälölle $ax - ny = c - b$ yhden ratkaisun.

## 4.3 Kiinalainen jäännöslause

Kiinalainen jäännöslause kertoo, että tietyntyyppisillä kongruenssiyhtälöryhmillä on ratkaisu:

**Lause 25.** *Olkoot luvut $m_1, m_2, \ldots, m_k$ pareittain yhteistekijättömiä. Tällöin kongruenssiyhtälöryhmällä*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

*on yksikäsitteinen ratkaisu modulossa $M = m_1 m_2 \cdots m_k$.*

*Todistus.* Laskuharjoitustehtävänä on todistaa, että

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots a_k M_k y_k \pmod{M}$$

toteuttaa yhtälöryhmän, kun luvut $y_j$ on määritelty seuraavasti: Kirjoitetaan $M_j = \frac{M}{m_j}$. Tällöin $\text{syt}(m_j, M_j) = 1$, jolloin luvulla $M_j$ on olemassa käänteisluku modulossa $m_j$, ja olkoon $y_j$ tämä käänteisluku, eli $y_j$ on määritelty kongruenssiyhtälöllä $M_j y_j \equiv 1 \pmod{m_j}$.

Osoitetaan nyt ratkaisujen yksikäsitteisyys. Oletetaan, että $x_0$ ja $x_1$ ovat kongruenssiyhtälöryhmän ratkaisuja. Tällöin $x_0 - x_1 \equiv 0 \pmod{m_1}$, $x_0 - x_1 \equiv 0 \pmod{m_2}$, ja niin edelleen, joten $m_1 \mid x_0 - x_1$, $m_2 \mid x_0 - x_1$, ja niin edelleen, joten $M \mid x_0 - x_1$ (sillä luvut $m_1, x_2, \ldots, m_k$ ovat pareittain yhteistekijättömiä). □

Käytännön elämässä seuraava tapa ratkaista kongruenssiyhtälöryhmiä on kuitenkin harvinaisen toimiva. Valaistaan sitä esimerkin avulla.

**Esimerkki 26.** Ratkaistaan kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

Aloitetaan kirjoittamalla ensimmäinen yhtälö uusiksi. Koska $x \equiv 2 \pmod{5}$, niin $x = 5y + 2$. Sijoitetaan tämä toiseen yhtälöön:

$$5y + 2 \equiv 3 (\text{mod } 7),$$

eli $5y \equiv 1 \pmod{7}$. On siis ratkaistava Diofantoksen yhtälö $5y + 7t = 1$. Tämän yleinen ratkaisu on $y = 3 + 7k$ ja $t = -2 - 5k$. Sijoitetaan nyt luvun $y$ lauseke $y = 3 + 7k$ luvun $x$ lausekkeeseen $x = 5y + 2$:

$$x = 5y + 2 = 5(3 + 7k) + 2 = 15 + 35k + 2 = 35k + 17 \equiv 17 \pmod{35},$$

eli ratkaisu on $x \equiv 17 \pmod{35}$.

# Luku 5

# Primitiiviset juuret

Tässä luvussa luku $p$ on alkuluku, vaikkei mitään mainittaisi.

Fermat'n pienen lauseen nojalla

$$a^{p-1} \equiv 1 \pmod{p},$$

kun $p$ on alkuluku ja $\text{syt}(a, p) = 1$. Toisaalta voidaan kysyä, milloin $a^s \not\equiv 1 \pmod{p}$ kaikilla positiivisilla $s < p - 1$. Tämä johtaa seuraavaan määritelmään

**Määritelmä 27.** Primitiiviseksi juureksi modulo $p$, kun $p$ on alkuluku kutsutaan sellaista lukua $g$, jolle pätee $\text{syt}(p, g) = 1$ ja $g^s \not\equiv 1 \pmod{p}$, kun $1 \leq s < p - 1$.

Esimerkiksi siis luku 2 on primitiivinen juuri modulo 5, sillä $2^1 \equiv 2 \pmod{5}$, $2^2 \equiv 4 \pmod{5}$ ja $2^3 \equiv 3 \pmod{5}$.

Primitiiviset juuret ovat mielenkiintoisia, sillä niiden avulla voidaan esittää koko redusoitu jäännössysteemi:

**Lause 28.** *Olkoon $g$ primitiivinen juuri modulo $p$. Nyt luvut $g^0, g^1, g^2, \ldots, g^{p-2}$ muodostavat redusoidun jäännössysteemin modulo $p$.*

*Todistus.* Luvun $p$ redusoidussa jäännössysteemissä on $p - 1$ alkiota, sillä ainoa jäännösluokka, joka täydestä jäännössysteemistä joudutaan poistamaan, on se jäännösluokka, jossa on luvun 0 jäännösluokan edustaja.

Lukuja $g^0, g^1, g^2, \ldots, d^{p-2}$ on $p - 1$ kappaletta, eli täysin oikea määrä. Riittää siis todistaa, että mitkään kaksi eivät ole kongruentteja keskenään modulo $p$. Jos nyt

$$g^s \equiv g^r,$$

kun $s > r$, niin $g^{s-r} \equiv 1 \pmod{p}$. Oletimme kuitenkin, että $g$ on primitiivinen juuri, joten koska $s - r$ on positiivinen, on pädettävä $s - r \geq p - 1$. Tämä on ristiriita ja väite on todistettu. □

Seuraava lause on hyvin tärkeä. Sen todistus kuitenkin vaatii jonkin verran lemmoja, eli esitetään ensin lause, sitten tarpeelliset lemmat ja lopulta lauseen todistus.

**Lause 29.** *Jokaisella alkuluvulla on primitiivinen juuri.*

## 5.1 Lemmoja polynomeista

Tämän osion tarkoitus on osoittaa, että modulo $p$ voidaan polynomeilla operoida kuten reaalilukujenkin joukossa. (Muista, että $p$ on alkuluku!)

**Lause 30** (Lagrangen lause)**.** *Modulo $p$ on $n$–asteisella polynomilla korkeintaan $n$ epäkongruenttia juurta.*

*Todistus.* Todistetaan tämä induktiolla. Alkuaskel: polynomilla $ax+b$ on korkeintaan yksi juuri modulo $p$, eli $x \equiv -ba^{-1} \pmod{p}$.

Tehdään nyt induktio-oletus, että astetta $k-1$ olevalla polynomilla on korkeintaan $k-1$ epäkongruenttia juurta.

Tarkastellaan nyt astetta $k$ olevaa polynomia $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$. Tehdään vastaoletus, että tällä on $k+1$ epäkongruenttia juurta, ja olkoot nämä juuret $c_0, c_1, \ldots, c_k$. Tarkastellaan nyt lauseketta

$$\begin{aligned} f(c_0) - f(x) = a_k c_0^k + a_{k-1}c_0^{k-1} + \cdots + a_1 c_0 + a_0 - a_k x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_0 = \\ a_k(c_0^k - x^k) + a_{k-1}(c_0^{k-1} - x^{k-1}) + \cdots + a_1(c_0 - x) = (c_0 - x)g(x), \end{aligned}$$

missä $g$ on astetta $k-1$ oleva polynomi. Väitetään nyt, että lukujen $c_1, c_2, \ldots, c_k$ on oltava polynomin $g(x)$ juuria. Selvästi

$$f(c_0) - f(c_j) \equiv 0 \pmod{p},$$

joten lukujen $c_j$ on oltava polynomin $f(c_0) - f(x)$ juuria. Nyt

$$f(c_0) - f(c_j) = (c_0 - c_j)g(c_j) \equiv 0 \pmod{p}.$$

Koska luvut $c_j$ ja $c_0$ ovat keskenään epäkongruentteja modulo $p$, pätee $\operatorname{syt}(p, c_0 - c_j) = 1$, joten $p \mid g(c_j)$ kaikilla $1 \leq j \leq k$. Tämä on ristiriita. Väite on todistettu. □

**Lause 31.** *Kun $d \mid p-1$, niin polynomilla $x^d - 1$ on modulo $p$ täsmälleen $d$ epäkongruenttia juurta.*

*Todistus.* Huomataan ensin, että Fermat'n pienen lauseen nojalla polynomilla $x^{p-1} - 1$ on $p-1$ epäkongruenttia juurta modulo $p$. Kirjoitetaan $p - 1 = rd$. Nyt

$$x^{p-1} - 1 = (x^d - 1)(x^{(r-1)d} + x^{(r-2)d} + \cdots + x^d + 1).$$

Koska polynomilla $x^{(r-1)d} + x^{(r-2)d} + \cdots x^d + 1$ on korkeintaan $(r-1)d$ epäkongruenttia juurta, ja polynomilla, joka on tämän ja $d$-asteisen polynomin tulo on $p - 1 = rd$ epäkongruenttia juurta, on polynomilla $x^d - 1$ oltava $d$ epäkongruenttia juurta. □

## 5.2 Lemma Eulerin $\varphi$-funktiolle

Eulerin $\varphi$-funktio on määritelty olemaan niiden korkeintaan luvun $n$ suuruisten lukujen lukumäärä, joiden suurin yhteinen tekijä luvun $n$ kanssa on yksi.

$$\varphi(n) = |\{1 \leq m \leq n : \ \mathrm{syt}(n, m) = 1\}| .$$

Huom! Aiemmassa monisteen versiossa oli "lukua $n$ pienempien"eikä siis "korkeintaan luvun $n$ suuruisten". Tämä on nyt muutettu multiplikatiivisuusominaisuuksien vuoksi – ainoa ero on siis $\varphi(1)$, joka näin määrittelemällä on 1, kun se muutoin olisi 0.

Mikäli $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (luvun $n$ alkutekijähajotelma), niin

$$\varphi(n) = \prod_{j=1}^{k} p_j^{\alpha_j - 1}(p_j - 1).$$

Tästä on selvää, että $\varphi$-funktio on multiplikatiivinen, eli mikäli $\mathrm{syt}(n, m) = 1$, niin

$$\varphi(n)\varphi(m) = \varphi(nm).$$

Todistetaan nyt seuraava, ehkäpä hieman omituisen näköinen lause:

**Lause 32.** *Pätee*

$$\sum_{d|n} \varphi(d) = n.$$

*Todistus.* Todistetaan tämä ensin suoralla laskulla alkulukupotensseille, ja tämän jälkeen induktiolla kaikille yhdistetyille luvuille.

Aloitetaan kuitenkin tapauksesta $n = 1$. Nyt

$$\sum_{d|1} \varphi(d) = 1,$$

kuten pitäisikin.

Kun $n = p^k$, pätee

$$\sum_{d|p^k} = \varphi(1) + \sum_{1 \leq \ell \leq k} \varphi(p^\ell) = 1 + \sum_{1 \leq \ell \leq k} (p-1)p^{\ell-1} = 1 + (p-1)\frac{p^k - 1}{p-1} = p^k.$$

Tehdään nyt induktio eri alkutekijöiden lukumäärän suhteen. Edellinen toimii induktion alkuaskeleena. Tehdään siis induktio-oletus, että

$$\sum_{d|p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}} \varphi(d) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Tarkastellaan nyt lukua $n = p_1^{\alpha_1} p_2^{/alpha_2} \cdots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}}$. Kaikki tämän luvun tekijät ovat joko luvun $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ tekijöitä tai niillä on tekijänä jokin luvun $p$ potenssi $p^\ell$. Siispä

$$\sum_{d|p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k+1}^{\alpha_k+1}} \varphi(d) = \sum_{0 \le \ell \le \alpha_{k+1}} \sum_{d|p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}} \varphi(p^\ell d)$$

$$= \sum_{1 \le \ell \le \alpha_{k+1}} \sum_{d|p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}} \varphi(p^\ell d) + \sum_{d|p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}} \varphi(d) = \sum_{1 \le \ell \le \alpha_{k+1}} \sum_{d|p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}} \varphi(p^\ell)\varphi(d) + p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

$$= \sum_{1 \le \ell \le \alpha_{k+1}} (p-1)p^{\ell-1} p_1^{\alpha_1} \cdots p_k^{\alpha_k} + p_1^{\alpha_1} \cdots p_k^{\alpha_k} = (p-1)\frac{p^{\alpha_{k+1}} - 1}{p-1} p_1^{\alpha_1} \cdots p_k^{\alpha_k} + p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

$$= p_1^{\alpha_1} \cdots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}},$$

ja väite on todistettu. □

## 5.3 Lemmoja primitiivisistä juurista

**Määritelmä 33.** Määritellään luvun $n$ *kertaluku* $\mathrm{ord}_p(n)$ modulo $p$ seuraavasti, kun $\mathrm{syt}(p, n) = 1$:

$$n^{\mathrm{ord}_p(n)} \equiv 1 \pmod{p},$$

ja jos $s < \mathrm{ord}_p(n)$, niin $n^s \not\equiv 1 \pmod{p}$. Siis primitiivisille juurille $g$ pätee $\mathrm{ord}_p(g) = p - 1$.

Todistetaan nyt muutama lemma kertaluvuille:

**Lemma 34.** *Pätee*

$$ord_p(n) \mid p - 1.$$

*Todistus.* Olkoon nyt $s$ pienin kertaluku, joka ei jaa lukua $p - 1$. Kirjoitetaan jakoyhtälö:

$$p - 1 = qs + r,$$

missä $0 \le r < s$.Nyt kuitenkin $n^r = n^{p-1-qs} \equiv 1 \pmod{p}$, mikä on ristiriita. □

**Lemma 35.** *Jos* $n^s \equiv 1 \pmod{p}$*, niin* $ord_p(n) \mid s$.

*Todistus.* Tehdään vastaoletus: $\mathrm{ord}_p(n) \nmid s$. Määritelmän nojalla $\mathrm{ord}_p(n) < s$, joten kirjoitetaan jakoyhtälö:

$$s = q\mathrm{ord}_p(n) + r,$$

missä $r < \mathrm{ord}_p(n)$. Nyt

$$n^r = n^{s - q\mathrm{ord}_p(n)} \equiv 1 \pmod{p},$$

mikä on ristiriita, sillä nyt kertaluvun määritelmän nojalla pitäisi luvun $r$ olla luvun $n$ kertaluku. □

Tarvitsemme vielä yhden lemman, joka mahdollistaa jäännöksestä toiseen siirtymisen ja kertaluvun laskemisen:

**Lemma 36.** *Luvun $n^j$ kertaluku on $\frac{ord_p(n)}{syt(j,ord_p(n))}$.*

*Todistus.* Olkoon $s = \mathrm{ord}_p(n^j)$. Kirjoitetaan $\mathrm{syt}(j, \mathrm{ord}_(n)) = d$, ja $j = j_0 d$ sekä $\mathrm{ord}_p(n) = kd$, missä $\mathrm{syt}(j,k) = 1$. Nyt

$$\left(n^j\right)^{\frac{\mathrm{ord}_p(n)}{\mathrm{syt}(j,\mathrm{ord}_p(n))}} = n^{j_0 d \frac{\mathrm{ord}_p(n)}{d}} = n^{j_0 \mathrm{ord}_p(n)} \equiv 1 \pmod{p}.$$

Toisaalta on osoitettava, että millään lukua $\frac{\mathrm{ord}_p(n)}{\mathrm{syt}(j,\mathrm{ord}_p(n))}$ pienemmällä luvulla $s$ ei päde, että $(n^j)^s \equiv 1 \pmod{p}$. Edellisen lemman nojalla $s \mid \frac{\mathrm{ord}_p(n)}{\mathrm{syt}(j,\mathrm{ord}_p(n))}$. Toisaalta,

$$(n^j)^s = n^{js} \equiv 1 \pmod{p},$$

joten $\mathrm{ord}_(n) \mid js$, eli $kd \mid j_0 ds$, eli $k \mid j_0 s$. Koska $\mathrm{syt}(j_0, k) = 1$, niin $k \mid s$, eli $\frac{\mathrm{ord}_p(n)}{\mathrm{syt}(\mathrm{ord}_p(n),j)} \mid s$. Väite on todistettu. □

Nyt voimme siirtyä varsinaiseen todistukseen.

## 5.4 Todistus, että primitiivisiä juuria on olemassa

Lauseen todistus on itse asiassa harvinaisen mukava. Paitsi, että saamme sillä osoitettua, että primitiivisiä juuria on olemassa, saamme myös määritettyä niiden tarkan määrän.

Merkitään $f(k)$ niiden lukujen $1, 2, \ldots, p-1$ lukumäärää, joiden kertaluku modulossa $p$ on k, eli

$$f(k) = \left|\{1 \le m \le p-1 : \ \mathrm{ord}_p(m) = k\}\right|.$$

Aiemmin todistetun nojalla tiedämme, että jos $k \nmid p-1$, niin $f(k) = 0$. Toisaalta kaikkien lukujen $\{1, 2, \ldots, p-1\}$ täytyy kuulua jollakin luvulla $k$ joukkoon $\{1 \le m \le p-1 : \mathrm{ord}_p(m) = k\}$. Siispä

$$p - 1 = \sum_{1 \le m \le p-1} f(k) = \sum_{d \mid p-1} f(d).$$

Tarkastellaan nyt lukuja, joiden kertaluku on $d$. Mikäli tällaisia lukuja ei ole olemassakaan, pätee $f(d) = 0$. Jos taas tällaisia lukuja on olemassa, niin olkoon $a$ tällainen luku. Nyt $a$ on polynomin $x^d - 1$ juuri. Itse asiassa luvut $a, a^2, \ldots, a^d$ ovat tämän polynomin juuria. Lisäksi tiedämme, että tällä polynomilla on tasan $d$ epäkongruenttia juurta. Luvut $a^j$ ovat epäkongruentteja keskenään, sillä mikäli $a^j \equiv a^i \pmod{p}$, niin $a^{j-i} \equiv 1 \pmod{p}$, jolloin luvun $a$ kertaluku on korkeintaan $|j - i| < p - 1$. Toisaalta näiden kaikkien lukujen kertaluku ei ole $d$, vaan luvun $a^j$ kertaluku on $\frac{d}{\mathrm{syt}(d,j)}$, eli se on $d$ vain, jos $\mathrm{syt}(j,d) = 1$. Koska $1 \le j \le d$, niin tällaisia lukuja on $\varphi(d)$ kappaletta. Olemme siis osoittaneet, että $0 \le f(d) \le \varphi(d)$. Nyt kuitenkin

$$\sum_{d \mid p-1} f(d) = \sum_{d \mid p-1} \varphi(d),$$

joten $f(d) = \varphi(d)$, sillä summat ovat samat, ja $f(d) \le \varphi(d)$.

## 5.5 Wilsonin lause

Seuraava lause tunnetaan Wilsonin lauseena, ja sen voi todistaa primitiivisten juurten avulla. Todistus on laskuharjoitustehtävänä. Sen voisi todistaa myös esimerkiksi polynomien ominaisuuksilla.

**Lause 37** (Wilsonin lause)**.** *Pätee*

$$(p-1)! \equiv -1 \pmod{p}.$$

Toisaalta voidaan osoittaa myös käänteinen tulos: Mikäli $(n-1)! \equiv -1 \pmod{n}$, niin $n$ on alkuluku. Tämänkin todistus on laskuharjoitustehtävänä.

# Luku 6

# Irrationaalisuus

Lukua $a$ kutsutaan *rationaaliseksi*, mikäli $a$ voidaan esittää muodossa

$$a = \frac{r}{s},$$

missä $r$ ja $s$ ovat kokonaislukuja ja $s \neq 0$. Mikäli lukua $a$ ei voida esittää tällaisessa muodossa, kutsutaan sitä *irrationaaliseksi*.

Seuraava lause on tunnettu klassikko. Sen todistusta käytetään usein esimerkkinä vastaoletustodistuksesta. Lause oleellisesti ottaen kertoo sen, että yksikköneliön lävistäjä on irrationaalinen. Tämän tuloksen väitetään aiheuttaneen suurta järkytystä Pythagoraan koulukunnassa, jopa siinä mittakaavassa, että tästä tuloksesta ei olisi ollut syytä puhua, ja tiedon vuotajia uhattiin kuolemanrangaistuksella. Tämä ei kuitenkaan juoruilua hillinnyt, vaan neliön lävistäjän irrationaalisuus levisi muidenkin tietoisuuteen.

**Lause 38.** *Luku $\sqrt{2}$ on irrationaalinen.*

*Todistus.* Tehdään vastaoletus: Voidaan kirjoittaa $\sqrt{2} = \frac{r}{s}$, missä luvut $r$ ja $s$ ovat positiivisia ja yhteistekijättömiä. Nyt

$$2 = \frac{r^2}{s^2},$$

joten $2s^2 = r^2$. Siispä $2 \mid r^2$, joten $2 \mid r$. Kirjoitetaan $r = 2r_1$. Nyt $2s^2 = r^2 = 4r_1^2$, joten $s^2 = 2r_1^2$, eli $2 \mid s^2$, ja siis $2 \mid s$. Tämä on ristiriita, koska oletimme, että luvut $r$ ja $s$ ovat yhteistekijättömiä. □

Pohdittavaksi (tätä pohditaan luennoilla): Missä ylläoleva todistus kosahtaisi esimerkiksi luvun 4 neliöjuurelle. Tiedämme siis, että $\sqrt{4} = 2$, joka on rationaalinen, joten ylläoleva todistus ei voi mennä läpi. Missä se menisi metsään?

Rationaalilukujen lukumäärää on aina hyvä pohtia. Selvästi niitä on äärettömän paljon. Voidaan toisaalta osoittaa, että jossain mielessä niitä ei ole enempää kuin kokonaislukuja:

**Lause 39.** *Rationaalilukujen joukko on numeroituva.*

*Todistus.* Riittää tarkastella positiivisia rationaalilukuja, koska negatiiviset voidaan vastaavasti liittää negatiivisille kokonaisluvuille, ja nolla nollalle. Olkoon $\frac{r}{s}$ rationaaliluvun sievennetty muoto, eli $\text{syt}(r, s) = 1$. Määritellään

$$h\left(\frac{r}{s}\right) = r + s.$$

Nyt numeroidaan luvut ensinnäkin funktion $h$ osoittamassa järjestyksessä, ja lisäksi funktion $h$ arvojen ollessa sama, aina pienimmästä nimittäjästä suurimpaan. □

Edellinen todistus voi tarvita hieman selvitystä vielä. Mikäli $\frac{r}{s}$ on positiivinen, niin $r, s > 0$, joten $h\left(\frac{r}{s}\right) \geq 2$. Ainoa rationaaliluku, jolle funktio saa arvon 2, on luku 2, joten se pääsee ensimmäiseksi. Funktio saa arvon 3 luvuilla $\frac{1}{2}$ ja $\frac{2}{1}$, ja näistä pienempi nimittäjä on luvulla $\frac{2}{1}$, joten se listataan seuraavaksi, sitten $\frac{1}{2}$. Tämän jälkeen vuorossa on ne luvut, joille funktio $h$ antaa arvon 4, eli $\frac{1}{3}$ ja $\frac{3}{1}$ (lukua $\frac{2}{2}$ ei huomioida, koska se ei ole sievennetty, ja näin olen se on jo listattu). Näistä ensin listataan $\frac{3}{1}$, ja sitten vasta $\frac{1}{3}$. Näin käydään selvästi läpi kaikki rationaaliluvut, ja lisäksi voi arvioida, että luvun $\frac{r}{s}$ saavuttaminen vaatii alle $(r + s)^2$ askelta.

## 6.1 Luvun $e$ irrationaalisuus

Luvun $e$ osoittaminen irrationaaliseksi on suhteellisen helppoa, vaikka se onkin selvästi hankalampaa kuin esimerkiksi luvun $\sqrt{2}$ osoittaminen irrationaaliseksi. Intuitiivisesti todistus perustuu siihen, että luvun $e$ sarjakehitelmän nimittäjät kasvavat nopeasti.

**Lause 40.** *Luku $e$ on irrationaalinen.*

*Todistus.* Tehdään vastaoletus: $e$ on rationaalinen, eli se voidaan kirjoittaa muodossa $e = \frac{a}{b}$, missä $a, b \in \mathbb{Z}0$, $a, b > 0$ ja $\text{syt}(a, b) = 1$, jolloin

$$eb = a.$$

ja ennen kaikkea

$$n!eb = n!a$$

kaikilla $n$. Käytetään luvun $e$ sarjakehitelmää

$$e = \sum_{k \geq 0} \frac{1}{k!}.$$

(Tämä on siis funktion $e^x$ Taylorin sarja, kun $x = 1$.) Nyt

$$bn!\left(\left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}\right) + \left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \cdots\right)\right) = n!a.$$

Yhtälön oikea puoli on selvästi kokonaisluku. Myös termi

$$bn!\left(1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}\right)=b\left(n!+n!+\frac{n!}{2!}+\cdots+1\right)$$

on kokonaisluku. Täten luvun

$$bn!\left(\frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\cdots\right)$$

on oltava kokonaisluku. Arvioidaan tätä lukua.

$$\begin{aligned}bn!\left(\frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\cdots\right)&=b\left(\frac{1}{n+1}+\frac{1}{(n+1)(n+2)}+\cdots\right)\\&<b\left(\frac{1}{n+1}+\frac{1}{(n+1)^2}+\frac{1}{(n+1)^3}+\cdots\right)=b\cdot\frac{1}{n+1}\cdot\frac{1}{1-\frac{1}{n+1}}=\frac{b}{n}.\end{aligned}$$

Nyt siis tiedämme tästä kokonaisluvusta, että se on varmasti pienempi kuin $\frac{b}{n}$, ja kun $n>b$, se tarkoittaa sitä, että tämä kokonaisluku on korkeintaan 0. Toisaalta näemme, että

$$bn!\left(\frac{1}{(n+1)!}+\frac{1}{(n+2)!}+\cdots\right)>bn!\cdot\frac{1}{(n+1)!}=\frac{b}{n+1}>0.$$

Nyt toisaalta tiedämme, että tämä kokonaisluku on aidosti suurempi kuin 0. Koska mikään luku ei voi olla yhtä aikaa korkeintaan 0 ja aidosti suurempi kuin 0, ei tällaista lukua ole olemassakaan. Tämä on ristiriita. □

## 6.2 Algebralliset luvut

*Algebrallisiksi luvuiksi* kutsutaan lukuja, jotka ovat jonkin kokonaislukukertoimisen polynomin juuria. Esimerkiksi siis

$$\sqrt{2}$$

on algebrallinen, sillä se on polynomin $x^2-2$ juuri.

Sellaisia lukuja, jotka eivät ole algebrallisia, kutsutaan *transkendenttisiksi*. Tunnettuja transkendenttisia lukuja ovat $\pi$ ja $e$.

Annettu luku on tyypillisesti hyvin hankala osoittaa transkendenttiseksi. Joitakin poikkeuksia toki on. Toinen huomattava asia on, että jossain mielessä transkendenttisiin lukuihin on hyvin hankala päästä käsiksi: Ne eivät ole kokonaislukukertoimisten polynomien juuria, joten ne eivät aina ikäänkuin esiinny automaattisesti. Kuitenkin suurin osa luvuista on transkendenttisia siinä mielessä, että algebrallisia lukuja on vain numeroituvan paljon, transkendenttisia taas ylinumeroituvan paljon, sillä reaalilukujakin on ylinumeroituvan paljon.

Kannattaa huomata, että polynomilla ei välttämättä ole ratkaisukaavaa, vaan itse asiassa Galois ja Abel ovat riippumattomasti todistaneet, että viidennen ja korkeamman asteen polynomiyhtälöillä ei yleisesti ole ratkaisukaavaa. Toisin sanoen, algebrallisia lukujakaan ei ole aina helppo esittää, mutta ne voidaan kuitenkin aina antaa esimerkiksi sanomalla "tämän polynomin ratkaisut"tai "tämän polynomin ratkaisuista se, joka on.."

# Luku 7

# Kryptografiaa

Kuuluisa lukuteoreetikko Hardy totesi joskus lukuteoriasta:

*"No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity, and it seems unlikely that anyone will do so for many years."*

Kryptografialla eli salauksella tarkoitetaan niitä matemaattisia menetelmiä, joilla esimerkiksi viesti muutetaan sellaiseen muotoon, että väärät ihmiset eivät sitä pysty lukemaan. Käytännössä useat näistä menetelmistä nojaavat lukuteoriaan.

## 7.1 RSA

RSA perustuu siihen, että tekijöihinjako on hankalaa isoilla luvuilla. (Voidaan itse asiassa todistaa, että jos RSA murtuu yleisessä tilanteessa, niin myös tekijöihinjako-ongelma on ratkeava polynomiaalisessa ajassa.)

RSA:ssa on julkinen avain (julkinen avain on siis sellainen, joka voidaan levittää kaiken kansan tietoisuuteen), $(n, e)$, missä $n = pq$ sekä $p$ ja $q$ ovat parittomia alkulukuja, keskenään erisuuria. Kriittistä on kuitenkin se, että käytetään vain lukua $n$, eikä anneta sen alkutekijähajotelmaa. Pointti on se, että isoa lukua on hankala jakaa tekijöihin, jolloin jos alkuluvut $p$ ja $q$ ovat molemmat isoja, voidaan olettaa, että alkutekijöhajotelmaa ei tunneta.

Salainen avain puolestaan on $(p, q, \varphi(n), d)$, missä $ed \equiv 1 \pmod{\varphi(n)}$. Huomaa, että luku $e$ pitää valita niin, että käänteisluku on olemassa, eli että $\text{syt}(e, \varphi(n)) = 1$. Luku $d$ on siis helppo määrittää (käänteislukuja erilaisissa moduloissa on aiemminkin laskettu), jos tunnetaan $e$ ja $\varphi(n)$ (ja tämän funktion arvon laskemiseksi tarvitaan tieto luvuista $p$ ja $q$).

**Tiivistettynä siis:** Julkinen avain $(n, e)$, salainen avain $(p, q, \varphi(n), d)$, ja näistä oletetaan $pq = n$, $p \neq q$, $p$ ja $q$ parittomia alkulukuja, $ed \equiv 1 \pmod{\varphi(n)}$, ja $\varphi(n)$ on Eulerin funktio. Sisäänrakennettu oletus on siis, että $\text{syt}(e, \varphi(n)) = \text{syt}(d, \varphi(n)) = 1$.

Nyt luvun $1 \leq w \leq n$ salaaminen tapahtuu seuraavasti:

$$w' \equiv w^e \pmod{n}$$

ja purkaminen seuraavasti:

$$w'' \equiv w'^d \pmod{n}.$$

Nyt $w \equiv w'' \pmod{n}$, sillä

$$w'' \equiv w'^d \equiv w^{ed} \pmod{n},$$

ja Eulerin lauseen nojalla

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

jolloin $w^{ed} = w^{1+k\varphi(n)} \pmod{n}$, kunhan $\text{syt}(w, n) = 1$.

Valotetaan RSA:n toimintaa esimerkillä:

**Esimerkki 41.** Olkoon $n = 83 \cdot 103 = 8549$. Nyt $\varphi(n) = (83-1)(103-1) = 82 \cdot 102 = 8364$. Valitaan $e = 13$. Tämä on täysin laillista, sillä $\text{syt}(13, 8364) = 1$. Ratkaistaan nyt $d$ yhtälöstä

$$de - +k\varphi(n) = 1,$$

eli

$$13d + k8364 = 1.$$

Ensinnäkin

$$8364 = 643 \cdot 13 + 5,$$

ja

$$13 = 2 \cdot 5 + 3,$$

josta

$$5 = 1 \cdot 3 + 2,$$

nyt

$$3 = 1 \cdot 2 + 1,$$

ja vihdoinkin jako menee tasan: $2 = 2 \cdot 1 + 0$. Siispä

$$1 = 3 - 1 \cdot 2,$$

johon sijoittaen saadaan

$$1 = 3-1(5-3) = 2{\cdot}3-5 = 2(13-2{\cdot}5)-5 = 2{\cdot}13-5{\cdot}5 = 2{\cdot}13-5(8364-643{\cdot}13) = 3217{\cdot}13-5{\cdot}8364.$$

Voidaan siis valita $d = 3217$. Salataan nyt luku 87. Tämä tapahtuu yksinkertaisesti seuraavasti: Lasketaan $87^{13} \pmod{8549}$. Nyt

$$87^{13} \equiv 7929 \pmod{8549}.$$

Purkaminen tulee olemaan selvästi työläämpi operaatio. On siis laskettava

$$7929^{3217} \pmod{8549}.$$

Tämä on todennäköisesti kivuttominta tehdä toistuvalla neliöinnillä, jota varten kirjoitetaan

$$3217_{10} = 110010010001_2$$

binääriesitys. (Binääriesityksestä näkee helposti, miten luku on laskettava.) Nyt

$$7929^{3217} = 7929^{2048} \cdot 7929^{1024} \cdot 7929^{128} \cdot 7929^{16} \cdot 7929.$$

Tämän laskutavan nerokkuus on nopeus: korotetaan neliöön, ja saadaan aina hoidettua monta laskutoimitusta kerralla. Siispä:

$$7929^{16} \equiv \left(7929^2\right)^8 \equiv 8244^8 \equiv 305^8 \equiv 7535^4 \equiv 2316^2 \equiv 3633 \pmod{8549}.$$

Koska $128 = 16 \cdot 8$, niin

$$7929^{128} \equiv 3633^8 \pmod{8549}.$$

Nyt voidaan laskea

$$3633^8 \equiv 7582^4 \equiv 3248^2 \equiv 38 \pmod{8549}.$$

Koska taas $1024 = 8 \cdot 128$, voidaan laskea

$$7929^{1024} \equiv 38^8 \pmod{8549},$$

joten lasketaan

$$38^8 = 1444^4 \equiv 7729^2 \equiv 5578 \pmod{8549}.$$

Lopulta vielä $2048 = 1024$, joten riittää laskea

$$7929^{2048} \equiv 5578^2 \equiv 4273 \pmod{8549}.$$

Ja nyt

$$7929^3217 \equiv 4273 \cdot 5578 \cdot 38 \cdot 3633 \cdot 7929 \equiv 87 \pmod{8549}.$$

### 7.1.1 Järjestelmän heikkouksia

Osoitetaan nyt, että $p - q$ ei saa olla liian pieni:

**Lause 42.** *Mikäli* $\left|\frac{p-q}{2}\right|^2 < 2\sqrt{n} + 1$, *niin luku* $n = pq$ *saadaan välittömästi jaettua tekijöihin (ts. RSA murtuu).*

*Todistus.* Jos $p = q$, on tekijöihinjako helppo tehdä. Olkoon siis $p > q$, ja kirjoitetaan $p = t + r$ ja $q = t - r$, missä $t$ ja $r$ ovat positiivisia kokonaislukuja. Nyt $p - q = 2r$, eli $r^2 < 2\sqrt{n} + 1$ ja

$$n = pq = (t + r)(t - r) = t^2 - r^2.$$

Toisaalta

$$(\lceil\sqrt{n}\rceil + 1)^2 = \lceil\sqrt{n}\rceil^2 + 2\lceil\sqrt{n}\rceil + 1 > n + 2\sqrt{n} + 1 > n + r^2.$$

Nyt $t^2 = n + r^2$, joten $t^2 > n$. Kuitenkin $t^2 < (\lceil\sqrt{n}\rceil + 1)^2$, joten $t = \lceil\sqrt{n}\rceil$. Tämän avulla puolestaan saadaan ratkaistua $r$:

$$r^2 = \lceil\sqrt{n}\rceil^2 - n,$$

ja nyt

$$p = \lceil\sqrt{n}\rceil + r$$

ja

$$q = \lceil\sqrt{n}\rceil - r.$$

□

- Wiener on osoittanut, että RSA murtuu, kun $d < \frac{1}{3}n^{1/4}$
- Boneh ja Durfee paransivat tulosta ja osoittivat, että RSA murtuu, kun $d < n^{0,292}$.
- Uskotaan yleisesti, että RSA murtuu, kun $d < \sqrt{n}$.

## 7.2 Diffie-Hellmannin avaimenvaihtoprotokolla

Diffie-Hellmannin avaimenvaihtoprotokolla sopii tilanteeseen, jossa on sovittava jokin satunnaisehko luku yhteisesti, mutta käytössä on vain julkinen kanava kommunikointiin. (Julkiseksi kanavaksi voi ajatella esimerkiksi Hesarin etusivun, puhelinpylvään, ilmoitustaulun tai muun vastaavaan esineen, jonka yksityisyyttä ei voi valvoa.)

1. Ensin tahot (olkoot Bonnie ja Clyde) sopivat alkuluvusta $p$ ja primitiivisestä juuresta $g$ modulo $p$. Nämä voidaan julkistaa, eli sopiminen voi käytännössä tarkoittaa sitä, että Bonnie postaa Hesariin ilmoituksen: "Valitaan alkuluvuksi $p$ ja primitiiviseksi juureksi $g$."

2. Seuraavaksi Bonnie ja Clyde valitsevat omat eksponenttinsa $b$ ja $c$, ja näitä he eivät kerro kellekään, edes toisilleen (koska turvallista kanavaa ei ole käytettävissä).

3. Nyt Bonnie laskee luvun $g^b$ ja redusoi sen modulossa $p$ ja Clyde puolestaan laskee luvun luvun $g^c$ ja redusoi sen modulossa $p$. Merkitään näitä uusia lukuja $b'$ ja $c'$. Nyt Bonnie postaa luvun $b'$ ja Clyde postaa luvun $c'$.

4. Nyt Bonnie laskee luvun $c'^b$ modulossa $p$ ja Clyde laskee luvun $b'^c$ modulossa $p$, ja molemmat ovatkin saaneet saman luvun, sillä

$$c'^b \equiv (g^c)^b = g^{cb} \equiv (g^b)^c \equiv b'^c \pmod{p}.$$

Kriittistä on reduktio modulossa $p$: Se ei muuta tuloksia mitenkään, mutta se toimii salauksena. Jos Bonnie ja Clyde vain laskisivat luvut $g^b$ ja $g^c$, eivätkä redusoisi, olisi lukujen $b$ ja $c$ selvittäminen ihan liian helppoa ($g$-kantainen logaritmi).