# Törmäyskurssi kilpailulukuteoriaan – pienin välttämätön oppimäärä

Anne-Maria Ernvall-Hytönen

14. tammikuuta 2011

## Sisältö

**1 Jaollisuus, alkuluvut, ynnä muut perustavanlaatuiset asiat** **2**
1.1 Lukujen tekijöiden lukumäärät ja summat . . . . . 2
1.2 SYT ja PYJ . . . . . 3
1.3 Täydelliset luvut, Mersennen alkuluvut . . . . . 4

**2 Kongruenssit** **5**
2.1 Eulerin $\varphi$-funktio, Eulerin lause ja Fermat'n pieni lause . . . . . 6
2.2 Kiinalainen jäännöslause . . . . . 6

**3 Diofantoksen yhtälöt** **7**
3.1 Ensimmäinen aste . . . . . 7
3.2 Korkeammat asteet . . . . . 8
3.3 Kahden peräkkäisen kokonaisluvun välissä ei tosiaankaan ole kokonaislukua . . 9

**4 Primitiiviset juuret** **10**
4.1 Harjoitustehtäviä . . . . . 11
4.2 Wilsonin lause . . . . . 11

**5 Välttämätön tietämys kompleksiluvuista** **11**
5.1 Gaussin kokonaisluvut . . . . . 11

# Esipuhe

Tämän materiaalin ei ole tarkoitus toimia johdantona lukuteoriaan, vaan lukijan oletetaan perehtyneen aiheeseen esimerkiksi lukiokirjojen tai Väisälän Lukuteorian ja korkeamman algebran alkeet -kirjan alun lukemalla. En missään nimessä yritäkään esittää asioita perusteellisesti, vaan tarjoilla kilpailullista näkökulmaa, sekä lisämateriaalia innostuneille kansalaisille.

# 1 Jaollisuus, alkuluvut, ynnä muut perustavanlaatuiset asiat

Sanomme, että kokonaisluku $a$ jakaa kokonaisluvun $b$ ja kirjoitamme $a \mid b$, jos on olemassa kokonaisluku $c$, jolla $b = ac$. Siispä $3 \mid 6$, mutta luku 9 ei jaa lukua 35.

Alkuluvuiksi kutsutaan positiivisia kokonaislukuja, jotka ovat jaollisia vain itsellään ja luvulla yksi (sekä vastaavilla negatiivisilla luvuilla). Ensimmäiset alkuluvut ovat siis $2, 3, 5, 7, 11, 13, \ldots$.

Jokainen positiivinen kokonaisluku voidaan esittää alkulukujen tulona järjestystä vaille täsmälleen yhdellä tavalla, eli

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

missä $p_1, \ldots p_k$ ovat alkulukuja ja $\alpha_1, \ldots \alpha_k \geq 1$, paitsi luku 1, jolla alkulukuhajotelman tulo on tyhjä. Alkulukuhajotelman yksikäsitteisyys todistetaan myöhemmin.

## 1.1 Lukujen tekijöiden lukumäärät ja summat

Luvun tekijöiden (positiivisten sellaisten) lukumäärälle on varsin yksinkertainen kaava

$$\tau(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (\alpha_1 + 1) \cdots (\alpha_k + 1)\,.$$

Tämä on helppo todistaa miettimällä, miten luvulle voidaan muodostaa tekijöitä. Ensimmäisen alkutekijän eksponentilla on $\alpha_1 + 1$ vaihtoehtoa, koska se voi olla mikä tahansa kokonaisluku joukosta $\{0, 1, \ldots, \alpha_k\}$. Vastaavasti kaikille muillekin alkutekijöille, joten tekijöiden lukumäärä saada ottamalla tulo kaikkien yksittäisten eksponenttien vaihtoehtojen määristä.

Vastaavasti voidaan todistaa myös luvun tekijöiden summan kaava, joka on

$$\sigma\left(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

Nämä funktiot äännetään
$\tau$: tau
$\sigma$: sigma.

On huomattava, että nämä kirjainvalinnat eivät suinkaan ole tarkoitettu vain näille funktioille, eivätkä ne myöskään ole yksikäsitteiset. $\tau$:n tilalla saattaa seikkailla esimerkiksi $d$ ja $\tau$ viittaa usein niin sanottuun Ramanujanin $\tau$-funktioon.

### Harjoitustehtäviä

1. Pääteekö a) $6 \mid 39$ b) $6 \mid 30$ c) $14 \mid 42$?
2. Listaapa lukujen a) 35 b) 87 c) 56 kaikki positiiviset tekijät sekä alkutekijät.
3. Laske edellisen tehtävän luvuille sekä positiivisten tekijöiden lukumäärä että niiden summa.

## 1.2 SYT ja PYJ

Suurin yhteinen tekijä ja pienin yhteinen jaettava opetetaan koulussa jo ensimmäisten vuosien aikana — näiden osaaminen nimittäin tuottaa paljon iloa murtoluvuilla laskettaessa.

Lukujen $a$ ja $b$ suurin yhteinen tekijä on suurin positiivinen kokonaisluku, joka jakaa sekä luvun $a$ että luvun $b$. Esimerkiksi $\text{syt}(24, 18) = 6$. Voitaisiin myös määritellä, että suurin yhteinen tekijä on pienin positiivinen kokonaisluku $c$, jolla yhtälöllä

$$ax + by = c$$

on kokonaislukuratkaisu $(x, y)$. Tämä määritelmä on itse asiassa varsin hyödyllinen, sillä sen avulla voidaan todistaa alkutekijähajotelman yksikäsitteisyys. Aloitetaan apulauseella, eli lemmalla:

**Lemma 1.1.** *Jos $p$ on alkuluku, $p \mid ab$ ja $p$ ei jaa lukua $a$, niin $p \mid b$.*

*Todistus.* Koska luku $p$ ei jaa lukua $a$ ja $p$ on alkuluku, niin $\text{syt}(p, a) = 1$, eli on olemassa kokonaisluvut $x$ ja $y$, joilla $px + ay = 1$. Nyt $aby = b(1 - px)$. Koska $p \mid ab$, niin $p \mid aby$. Täten $p \mid (b - bpx)$, eli on olemassa kokonaisluku $c$, jolla $pc = b - bpx$. Tästä saadaankin $b = pc + pbx = p(c + bx)$, eli $p \mid b$. □

Tämä lemma on hengentärkeä alkulukulauseen todistuksen kannalta. Loppu meneekin itse asiassa varsin yksinkertaisella induktionkaltaisella toiminnalla: Olkoot

$$p_1^{\alpha_1} \cdots p_k^{\alpha_k} = n = q_1^{\beta_1} \cdots q_\ell^{\beta_\ell}.$$

Koska $p_1 \mid n$, ja $p_1 \mid q_j^{\beta_j}$, jos ja vain jos $p_1 = q_j$ (lemman nojalla), on lukujen $q_1, \ldots, q_\ell$ joukossa oltava $p_1$. Voidaan jakaa luvulla $p_1$ ja jatkaa näin $\alpha_1$ kertaa. Vastaavasti kaikilla muillakin alkuluvuilla $p_i$. Samanlainen päättely voitaisiin tehdä lähtien liikkeelle luvusta $q_1$. (Aktiivinen lukija voi täydentää yksityiskohdat.)

Lukujen $a$ ja $b$ pienin yhteinen jaettava on pienin positiivinen kokonaisluku, joka on jaollinen sekä luvulla $a$ että luvulla $b$. On varsin helppo tehtävä osoittaa seuraava identiteetti:

$$\text{syt}(a, b) = \frac{ab}{\text{pyj}(a, b)}.$$

Käytännön elämässä fiksuin tapa etsiä suurin yhteinen tekijä on käyttää Eukleideen algoritmia. Eukleideen algoritmi perustuu siihen, että $\text{syt}(n, m) = \text{syt}(n, n - m)$. Eukleideen algoritmillä tarkoitetaan seuraavaa menetelmää:

**Menetelmä 1.** *Laskettava syt(m,n):*

1. *Olkoon $m > n$. Kirjoitetaan ensin $m$ muodossa $m = kn + r$, missä $r < n$.*
2. *Jos $r = 0$, niin syt$(m, n)$=n. Muutoin palataan kohtaan 1, mutta lukujen $m$ ja $n$ tilalla käytetään lukuja $n$ ja $r$. Viimeinen nollasta poikkeava jakojäännös on haettu syt.*

Voi olla hyvä käydä läpi yksinkertainen esimerkki:

**Esimerkki 1.** *Í„ Lasketaan syt$(135, 20)$. Kirjoitetaan aluksi*

$$135 = 20 \cdot 6 + 15.$$

*Nyt*

$$20 = 15 \cdot 1 + 5.$$

*ja $15 = 5 \cdot 3 + 0$, joten syt$(135, 20) = 5$.*

Jos lukujen alkutekijähajotelmat on tiedossa, on helppo myös tuottaa suurin yhteinen tekijä vertailemalla eksponentteja.

**Harjoitustehtäviä**

1. Määritä lukujen a) 54 ja 49 b) 87 ja 28 c) 126 ja 23872 syt ja pyj.
2. Määritä lukujen a) 54 ja 50 b) 51 ja 85 c) 127 ja 23872 syt ja pyj.
3. Olkoon $p$ alkuluku. Jakaako $p$ koskaan lukua $dp-1$?
4. Millä alkuluvuilla $p$, luku $p$ jakaa luvun $dp-3$? Entä luvun $dp-6$?
5. Todista, että jos $\text{syt}(a,b)=1$, niin $\tau(ab)=\tau(a)\tau(b)$ ja $\sigma(ab)=\sigma(a)\sigma(b)$.

## 1.3 Täydelliset luvut, Mersennen alkuluvut

Sellaisia lukuja, joiden itseään pienempien tekijöiden summa on sama kuin luku itse kutsutaan täydellisiksi luvuiksi. Formaalisti siis

$$\sigma(n)=2n.$$

Harmillisen vähän näistä tiedetään - toistaiseksi yhtään paritonta täydellistä lukua ei ole löytynyt. Konjekturoitu on, että näitä ei edes ole olemassa. Sen sijaan parillisten suhteen tilanne on paljon simppelimpi, tai ainakin siltä vaikuttaa alkuun. Esimerkiksi luvut 6 ja 28 ovat täydellisiä lukuja.

**Lause 1.2.** *Parilliset täydelliset luvut ovat muotoa*

$$2^{p-1}\left(2^p-1\right),$$

*missä* $2^p-1$ *on alkuluku.*

Tässä on nyt ensin huomattava, että jos luku $2^n-1$ on alkuluku, niin $n$ on alkuluku. Todistus on varsin yksinkertainen kaavamanipulaatio käyttäen hyväksi MAOL:n taulukkokirjastakin löytyviä indentiteettejä. Kuitenkaan se, että $n$ on alkuluku, ei takaa, että $2^n-1$ on alkuluku. Jos tämä luku kuitenkin on alkuluku, kutsutaan sitä Mersennen alkuluvuksi. Esimerkiksi luvut $3=2^2-1$ ja $7=2^3-1$ ovat täydellisiä lukuja.

*Todistus.* Kirjoitetaan $n=2^{p-1}\left(2^p-1\right)$. Todistetaan ensin, että kaikki tätä muotoa olevat luvut ovat täydellisiä lukuja. Tämä on varsin yksinkertainen lasku:

$$\sum_{d|n} d=\sum_{i=0}^{p-1}2^i+\sum_{i=0}^{p-1}2^i\left(2^p-1\right)=2^p\left(2^p-1\right).$$

Toinen suunta (eli muita parillisia täydellisiä lukuja ei ole) on aavistuksen työläämpi. Koska $n$ on parillinen, voidaan kirjoittaa $n=2^ch$, missä $h$ on pariton luku. Koska $\sigma(n)=\sigma\left(2^c\right)\sigma(h)=\left(2^{c+1}-1\right)\sigma(h)$, on pädettävä $\left(2^{c+1}-1\right)\sigma(h)=2^{c+1}h$. Koska $\text{syt}(2^c,2^{c+1}-1)=1$, on oltava $\left(2^{c+1}-1\right)\mid h$. Kirjoitetaan $h=\left(2^{c+1}-1\right)k$. Nyt $\sigma(h)=\sigma\left(2c+1-1\right)\sigma\left(k\right)\geq 2^{c+1}k$. Yhtäsuuruus vallitsee vain, jos $2^{c+1}-1$ on alkuluku ja $\sigma(k)=k$, eli $k=1$. Täten on osoitettu, $n=2^c\left(2^{c+1}-1\right)$. □

On suhteellisen hauskaa laskea eräs raja parittoman täydellisen luvun tekijöille:

**Esimerkki 2** (Esimerkki, mutta ei erityisen tarpeellinen sellainen)**.** *Jos* $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ *on pariton täydellinen luku, niin*

$$2p_1^{\alpha_1} \cdots p_k^{\alpha_k} = \frac{p^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

*Täten*

$$2 = \frac{p^{\alpha_1+1} - 1}{p_1^{\alpha_1}(p_1 - 1)} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k^{\alpha_k}(p_k - 1)} < \frac{p_1}{p_1 - 1} \cdots \frac{p_k}{p_k - 1} < \frac{p_1 + k - 1}{p_1 - 1},$$

*eli* $k \geq p_1$.

**Harjoitustehtäviä**

1. Etsi viisi täydellistä lukua.
2. Osoita, ettei pariton neliö voi olla täydellinen luku.
3. Osoita, että jos parittomia täydellisiä lukuja on olemassa, niin ne ovat muotoa $pd^2$, missä $p$ on alkuluku.

## 2 Kongruenssit

Sanotaan, että $m$ on konguentti luvun $n$ kanssa modulo $k$ ja kirjoitetaan

$$m \equiv n \pmod{k},$$

jos $k \mid (m - n)$.

**Harjoitustehtäviä**

1. Olkoot $a \equiv b \pmod{n}$ ja $c \equiv d \pmod{n}$. Todista seuraavat kongruenssien perusominaisuudet:
   (a) $-a \equiv -b \pmod{n}$
   (b) $a \pm c \equiv b \pm d \pmod{n}$
   (c) $ac \equiv bd \pmod{n}$. Erityisesti siis $a^m \equiv b^m \pmod{n}$
2. Osoita, että jos aritmeettisen jonon kahden peräkkäisen jäsenen välinen erotus on 5, niin kuuden peräkkäisen luvun joukossa on tasan yksi kuudella jaollinen.
3. Joukko $A$ koostuu kaikista luvuista muotoa $p^2 - 1$, jossa $p > 3$ on alkuluku. Etsi suurin luku, jolla kaikki joukon $A$ alkiot ovat jaollisia.
4. Olkoon $n > 6$ sellainen luku, että $n - 1$ ja $n + 1$ ovat alkulukuja. Osoita, että $720 \mid n^2\left(n^2 + 16\right)$.

## 2.1 Eulerin $\varphi$-funktio, Eulerin lause ja Fermat'n pieni lause

Eulerin $\varphi$-funktio (lausutaan fii-funktio) kertoo niiden korkeintaan luvun suuruisten positiivisten kokonaislukujen määrän, joiden suurin yhteinen tekijä kyseisen luvun kanssa on 1. Formaalisti:

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

Erityisesti siis $\varphi(p) = p - 1$, kun $p$ on alkuluku. Yleisesti (todistus on yksinkertainen vaikkapa kaksinkertaisella induktiolla) pätee

$$\varphi\left(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1).$$

Eulerin lauseen mukaan, jos $\text{syt}(a, n) = 1$, niin

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

Tämä voidaan todistaa havaitsemalla, että jos $b_1, \ldots, b_{\varphi(n)}$ muodostavan luvun $n$ täydellisen redusoidun jäännössysteeminen, niin myös luvut $ab_1, \ldots, ab_{\varphi(n)}$ muodostavat luvun $n$ täydellisen redusoidun jäännössysteemin. Täten

$$\prod_{i=1}^{\varphi(n)} b_i \equiv \prod_{i=1}^{\varphi(n)} ab_i = a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} b_i \pmod{n}.$$

Koska $\text{syt}\left(b_1 \cdots b_{\varphi(n)}, n\right) = 1$, voidaan sieventää ja saadaan

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

Erityisesti

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

jos $p$ on alkuluku. Tätä kutsutaan Fermat'n pieneksi lauseeksi. (Fermat'n suuri lause on puolestaan se Diofantoksen yhtälöön liittyvä, jonka Andrew Wiles todisti 1990-luvulla.)

Seuraava Dirichlet'n tulos ei ole missään nimessä alkeellinen (paitsi muotoilultaan tai jos alkeellisen tulkitaan tarkoittavan, että todistaminen ei vaadi kompleksista integrointia), mutta se tuottaa usein paljon iloa, sillä sen avulla voi generoida vaikkapa alkulukuja, joille Eulerin $\phi$-funktion arvo on jaollinen annetulla alkuluvulla. Lisäksi sillä olisi esimerkiksi eräs jokusen vuoden takainen (Hampuri 2002) Baltian Tien tehtävä ratkennut.

**Lause 2.1.** *Olkoon syt$(a, b) = 1$. Nyt äärettömän monella luvun $k$ kokonaislukuarvolla on $ak + b$ alkuluku.*

### Harjoitustehtävä

1. Laske a) $\varphi(30)$ b) $\varphi(60)$ c) $\varphi(128)$.

## 2.2 Kiinalainen jäännöslause

Olkoot luvut $n_1, \ldots, n_k$ pareittain yhteistekijättömiä. Nyt konguenssisysteemillä

$$\begin{aligned} x &\equiv d_1 \pmod{n_1} \\ x &\equiv d_2 \pmod{n_2} \\ &\cdots \\ x &\equiv d_k \pmod{n_k} \end{aligned}$$

on yksikäsitteinen ratkaisu (mod $n_1 \cdots n_k$).

**Harjoitustehtäviä**

1. Tiedämme, että $x \equiv 3 \pmod 5$ ja $x \equiv 5 \pmod 3$. Määritä $x \pmod{15}$.
2. Jos taas $x \equiv 4 \pmod 6$ ja $x \equiv 5 \pmod 7$, niin mitä voidaan sanoa luvusta $x$?
3. Jos $y \equiv 3 \pmod 4$ ja $y \equiv 4 \pmod 6$, niin mitä voidaan sanoa luvusta $y$?
4. Jos $y \equiv 3 \pmod 4$, $y \equiv 4 \pmod 5$ ja $y \equiv 1 \pmod{63}$, niin mitä tiedetään luvusta $y$?
5. Etsi mahdollisimman pieni positiivinen sellainen $d$, että $9^d \equiv 1 \pmod{35}$.

# 3 Diofantoksen yhtälöt

Diofantoksen yhtälöksi kutsutaan kokonaislukukertoimista yhtälöä, jolle etsitään kokonaislukuratkaisuja.

## 3.1 Ensimmäinen aste

Ensimmäisen asteen Diofantoksen yhtälölle

$$ax + by = c$$

on selvä ratkaisuprotokolla. Ensin kirjoitetaan Eukleideen algoritmi yhteen suuntaan ja sitten takaisin päätyen lopulta alkuperäisiin lukuihin, joiden edessä on kertoimet. Luonnollisestikin, jos $\text{syt}(a, b)$ ei jaa lukua $c$, niin ratkaisuja ei ole. Toisaalta, jos $c = h\text{syt}(a, b)$, niin on varsin kannattavaa kertoa tässä kohtaa Eukleideen algoritmista saadun yhtälön molemmat puolet luvulla $h$. Tähän ynnätään vastaavan homogeenisen yhtälön ratkaisu ja on saatu yhtälön kaikki ratkaisut.

**Esimerkki 3.** *Ratkaistaanpa esimerkiksi Diofantoksen yhtälö* $9x+5y = 2$*: Aloitetaan Eukleideen algoritmilla:*

$$9 = 1 \cdot 5 + 4$$

*ja*

$$5 = 1 \cdot 4 + 1.$$

*Täten* $syt(9, 5) = 1$*. Nyt*

$$1 = 5 - 1 \cdot 4.$$

*Tähän sijoitetaan* 4 *edelliseltä riviltä, eli*

$$1 = 5 - (9 - 5) = 2 \cdot 5 - 9.$$

*Nyt*

$$2 = 4 \cdot 5 - 2 \cdot 9$$

*ja on saatu yksittäinen ratkaisu* $x_0 = -2$ *ja* $y_0 = 4$*. Nyt ratkaistaan homogeeninen yhtälö* $9x + 5y = 0$*, eli* $x = 5k$ *ja* $y = -9k$ *millä tahansa kokonaisluvulla* $k$*. Yleinen ratkaisu Diofantoksen yhtälölle on siis* $x = -2 + 5k$ *ja* $y = 4 - 9k$*.*

**Harjoitustehtäviä**

1. Ratkaise Diofantoksen yhtälöt a) $54x - 49y = 1$ b) $54x - 49y = 7$ c) $87x + 28y = 3$.

2. Ratkaise Diofantoksen yhtälöt a) $54x - 50y = 1$ b) $54x - 50y = 8$ c) $51x + 85y = 3$ d) $51x + 85y = 34$.

3. Torimyyjällä meni kirjanpito sekaisin. Tiedossa on, että hän on myynyt porkkanoita kahden kilon ja omenoita kolmen kilon säkeissä. Hän on lisäksi täysin vakuuttunut, että kaksi kiloa porkkanoita maksoi 2 euroa ja kolme kiloa omenoita 7 euroa. Yhteensä kassassa on 123 euroa. Omenasäkkejä oli hänen muistaakseen ainakin 13 kappaletta. Mitä hänen myynnistään voidaan sanoa?

## 3.2 Korkeammat asteet

Valitettavasti korkeamman asteen Diofantoksen yhtälölle ei ole mitään yleistä ratkaisutapaa. Toisinaan on järkevää käyttää kongruenssitarkasteluja, toisinaan taas vaikkapa äärettömän laskeutumisen periaatetta todistamaan, että ratkaisuja ei ole. Matematiikan tutkimuksessa käytetään paljon elliptisiin käyriin perustuvia menetelmiä yhtälöiden käsittelyssä. Tässä sivuutamme kuitenkin elliptiset käyrät täysin ja käymme läpi vain pari esimerkkiä, joiden on tarkoitus kertoa, miten kongruensseja tai ääretöntä laskeutumista voi hyödyntää.

**Esimerkki 4.** *Osoitetaan, että yhtälöllä* $x^2 + y^2 = 103$ *ei ole kokonaislukuratkaisuja. Huomataan, että* $103 \equiv 3 \pmod 4$. *Nyt* $x^2 \equiv 1$ *tai* $0 \pmod 4$ *riippuen siitä, onko* $x$ *parillinen vai pariton. Vastaavasti* $y^2$. *Täten* $x^2 + y^2$ *on* $0$ *tai* $1$ *tai* $2 \pmod 4$, *mutta ei* $3$.

**Esimerkki 5.** *Osoitetaan, että yhtälöllä* $x^2 + y^2 + z^2 = 2xyz$ *ei ole muita kokonaislukuratkaisuja kuin* $x = y = z = 0$. *Äärettömän laskeutumisen periaatteen idea on, että jos yhtälöllä olisi ratkaisu, niin sillä olisi oltava myös jossakin mielessä pienempi ratkaisu. Jos tätä voidaan soveltaa ikuisesti, käsissämme on ristiriita, joten ratkaisuja ei ole. Toinen vaihtoehtoinen logiikka on, että jotakin tekijää pitäisi löytyä äärettömän monta jostain ratkaisusta, eli esim. luvusta* $x$ *löytyy äärettömän monta kertaa tekijänä luku* $2$.

*Esimerkin yhtälön oikea puoli on parillinen. Täten myös vasemman puolen on oltava. Vähintään yhden luvuista* $x$, $y$ *ja* $z$ *on oltava parillinen. Koska tilanne on symmetrinen, voidaan kirjoittaa* $x = 2x_1$. *Nyt*

$$4x_1^2 + y^2 + z^2 = 4x_1yz.$$

*Oikea puoli on neljällä jaollinen, täten vasemmankin on oltava. Jos* $y \equiv z \equiv 1 \pmod 2$, *niin vasen puoli* $\equiv 2 \pmod 4$, *mikä ei ole mahdollista. Täten* $y \equiv z \equiv 0 \pmod 2$. *Kirjoitetaan* $y = 2y_1$ *ja* $z = 2z_1$. *Nyt*

$$4\left(x_1^2 + y_1^2 + z_1^2\right) = 16x_1y_1z_1.$$

*Lausekkeen* $x_1^2 + y_1^2 + z_1^2$ *on oltava jälleen parillinen ja peräti neljällä jaollinen. Kuten edellä, käy ilmi, että* $2 \mid x_1, y_1, z_1$. *Näin voidaan jatkaa. Ratkaisuja ei siis ole.*

**Harjoitustehtäviä**

1. Osoita, ettei yhtälöllä

$$\frac{x^{2000} - 1}{x - 1} = y^2$$

ole positiivisia kokonaislukuratkaisuja.

2. Osoita, ettei yhtälöllä

$$4\left(x_1^4 + \cdots + x_{14}^4\right) = 7\left(x_1^3 + \cdots x_{14}^3\right)$$

ole positiivisia kokonaislukuratkaisuja.

3. Olkoot $x$ ja $y$ positiivisia kokonaislukuja, joiden mikään alkutekijä ei ole suurempi kuin 5. Etsi kaikki $x$ ja $y$, jotka toteuttavat ehdon

$$x^2 - y^2 = 2^k$$

jollakin epänegatiivisella kokonaisluvulla $k$.

### 3.3 Kahden peräkkäisen kokonaisluvun välissä ei tosiaankaan ole kokonaislukua

Tarkastellaan nyt ajan kuluksi Diofantoksen yhtälöä

$$abc - 1 = k(a-1)(b-1)(c-1),$$

missä $1 < a < b < c$. Aloitetaan arvioimalla:

$$1 < \frac{abc}{(a-1)(b-1)(c-1)} < \frac{2 \cdot 3 \cdot 4}{1 \cdot 2 \cdot 3} = 4.$$

Täten $1 < k < 4$. Koska tälllä välillä ainoat kokonaisluvut ovat 2 ja 3, on oltava $k = 2$ tai $k = 3$. Käydään läpi nämä tapaukset.

1. $k = 2$. Nyt yhtälön oikea puoli on parilinen. Jotta yhtälön vasenkin puoli on parillinen, on oltava $a \equiv b \equiv c \equiv 1 \pmod 2$. Jos olisi $a \geq 5$, olisi myös

$$\frac{abc - 1}{(a-1)(b-1)(c-1)} < \frac{5 \cdot 6 \cdot 7}{4 \cdot 5 \cdot 6} < 2.$$

Tämä ei kuitenkaan ole mahdollista, koska lukujen 1 ja 2 välissä ei ole kokonaislukuja. On siis oltava $a = 3$. Nyt

$$3bc - 1 = 4(b-1)(c-1).$$

Jos olisi $b \geq 7$, olisi myös

$$\frac{3bc - 1}{2(b-1)(c-1)} < \frac{3 \cdot 7 \cdot 8}{2 \cdot 6 \cdot 7} = 2,$$

joten tämäkään ei ole mahdollista. On siis oltava $b = 5$. Voidaan lopulta ratkaista $c$:

$$15c - 1 = 16(c-1),$$

eli $c = 15$. Voidaan nyt siirtyä toiseen tapaukseen.

2. $k = 3$. Nyt

$$abc - 1 = 3(a-1)(b-1)(c-1)$$

ja täten kaikkien $a$, $b$ ja $c$ tulee olla samaa pariteettia. Jos olisi $a \geq 3$, olisi myös

$$\frac{abc-1}{(a-1)(b-1)(c-1)} < \frac{3 \cdot 5 \cdot 7}{2 \cdot 4 \cdot 6} = \frac{35}{26} < 3.$$

On siis oltava $a = 2$. Nyt on $b \geq 4$. Jos olisi $b \geq 6$, olisi myös

$$\frac{abc-1}{(a-1)(b-1)(c-1)} < \frac{2 \cdot 6 \cdot 8}{5 \cdot 7} = \frac{96}{35} < 3.$$

On siis oltava $b = 4$. Ratkaistaan nyt $c$:

$$8c - 1 = 9(c-1),$$

eli $c = 8$.

# 4 Primitiiviset juuret

Primitiiviseksi juureksi modulo $p$ kutsutaan sellaista lukua $g$, jonka potensseina saadaan koko redusoitu jäännössysteemi modulo $p$ (eli kaikki täydellisen jäännössysteemin luvut, jotka ovat yhteistekijättömiä $p$:n kanssa). Jokaisella parittomalla alkuluvulla on primitiivinen juuri. Myös parittomien alkulukujen potensseilla on primitiivinen juuri. Luvun 2 potenssien kohdalla saadaan parhaimmillaan yksittäisen luvun potenssien avulla puolet redusoidusta jäännössysteemistä.

**Esimerkki 6.** *Huomataan, että* $3^0 = 1,\ 3^1 = 3,\ 3^2 = 9$ *ja* $3^3 = 27 \equiv 11 \pmod{16}$*, eli näin on esitetty tasan puolet redusoidusta jäännössysteemista modulo* 16*. Koska* $3^4 = 81 \equiv 1 \pmod{16}$*, ei tää esitystapaa edes olisi voinut jatkaa.*

Osoitetaan, että kaikilla parittomilla alkuluvuilla on primitiivinen juuri ja jätetään muut asiat uskon (tai oman aktiivisuuden) varaan. Merkitään

$$\omega_p(n) = \min\{d > 0 : n^d \equiv 1 \pmod{p}\}.$$

Nyt $d \mid (p-1)$. Merkitään

$$\psi(d) = |\{n : \omega_p(n) = d\}|.$$

Koska $\omega_p(n) = \omega_p(n^j)$, jos ja vain jos $\text{syt}(j, p-1) = 1$, on oltava $\psi(d) = \varphi(d)$ tai $\psi(d) = 0$. On oltava

$$\sum_{d|(p-1)} \psi(d) = p - 1.$$

Toisaalta on helppo osoittaa vaikka induktiolla, että

$$\sum_{d|(p-1)} \varphi(d) = p - 1.$$

Koska

$$\sum_{d|(p-1)} \varphi(d) = \sum_{d|(p-1)} \psi(d)$$

ja $\psi(d) \leq \varphi(d)$, niin $\psi(d) = \varphi(d)$. Täten $\psi(d) = \varphi(d)$.

### 4.1 Harjoitustehtäviä

1. Etsi jokin primitiivinen juuri (mod 25).
2. Kuinka monta primitiivistä juurta on olemassa (mod 25)?
3. Olkoon $2^k + 1$ alkuluku, $k > 1$. Osoita, että 3 on primitiivinen juuri (mod $2^k + 1$).
4. Olkoon $g$ primitiinen juuri (mod 25). Etsi sellainen $d$, että $g^{3d} \equiv 1 \pmod{25}$.
5. Etsi primitiiviset juuret (mod 25).

### 4.2 Wilsonin lause

Wilsonin lauseen mukaan

$$(p-1)! \equiv -1 \ (\mathrm{mod} p),$$

jos ja vain jos $p$ on alkuluku. On varsin helppo todistaa, että muilla kuin alkuluvuilla tämä ei päde. Toinen suunta on aavistuksen hankalampi, mutta hoituu näppärästi primitiivisten juurten avulla: Kirjoitetaan luvut $1, \ldots p-1$ muodossa $g^j$, missä $g$ on primitiivinen juuri. Nyt $j$ saa kaikki arvot joukosta $\{0, \ldots, p-2\}$. Täten

$$(p-1)! \equiv \prod_{j=0}^{p-2} g^j = g^{0+1+\cdots+(p-2)} = g^{(p-1)(p-2)/2} \equiv -1 \ (\mathrm{mod} p)$$

## 5 Välttämätön tietämys kompleksiluvuista

Kompleksiluvuiksi kutsutaan pareja $(x, y)$, jotka voidaan myös kirjoittaa muodossa $x + iy$. Tässä $i$ toteuttaa ehdon $i^2 = -1$. Laskusäännöt:

$$(a + ib) + (c + id) = (a + c) + i\,(b + d)$$

ja

$$(a + ib) \cdot (c + id) = (ac - bd) + i\,(ad + cb)\,.$$

Kompleksiluvulle $a + bi$ määritellään itseisarvo seuraavalla kaavalla:

$$\sqrt{a^2 + b^2}.$$

Tässä kohtaa varsin hyvä kysymys on, mitä ihmettä kompleksiluvuilla on tekemistä lukuteorian kanssa (paitsi tietenkin analyyttinen lukuteoria käyttää innokkaasti kompleksisia integraaleja ja niiden residylausetta ja muuta vastaavaa). Seuraavan luvun on tarkoitus hieman valottaa kompleksilukujen lukuteoreettisia ominaisuuksia.

### 5.1 Gaussin kokonaisluvut

Jos $x$ ja $y$ ovat kokonaislukuja, niin $x + iy$ on Gaussin kokonaisluku. Gaussin kokonaisluvuille määritellään *normi* itseisarvon neliönä, eli luvun $x + iy$ normi Gaussin kokonaislukujen joukossa on $x^2 + y^2$. Merkitään tätä normia $N$:llä, eli

$$N(x + iy) = x^2 + y^2$$

Tämä ratkaisu on varsin järjellinen, sillä tällöin normi on kokonaisluku. (Muuten voisimme käyttää vapaasti aiemmin määriteltyä itseisarvoa tämän normin sijaan.)

Gaussin kokonaislukujen $\mathbb{Z}[i]$ joukossa määritellään jaollisuus seuraavasti:

$$z_1 \mid z_2,$$

jos on olomassa sellainen $z_3 \in \mathbb{Z}[i]$, että $z_1 z_3 = z_2$. Huomionarvoista on, että jos $z_1 \mid z_2$, niin $N(z_1) \mid N(z_2)$. Toisaalta, jos $s \mid N(z_1)$, niin on oltava kompleksiluku $z_1$, joka toteuttaa ehdot

1. $z_1 \mid z_2$
2. $N(z_1) = s$.

Alkulukujen käsite on mielekäs Gaussin kokonaislukujen joukossa. Voidaan osoittaa, että alkulukuja on täsmälleen kolmea eri ty yppiä:

1. Luku 2. Ainoa parillinen alkuluku. Kompleksitasossa $2 = (1 - i)(1 + i) = i(1 + i)^2$. Kannattaa huomata, että luku $i$ ei ole alkuluku vaan yksikkö, eli kuten luvut $-1$ ja $+1$ tavallisten kokonaislukujen joukossa.
2. Alkuluvut, jotka ovat $\equiv 3 \pmod 4$ kokonaislukujen joukossa, ovat alkulukuja myös Gaussin kokonaislukujen joukossa.
3. Alkuluvut, jotka ovat $\equiv 1 \pmod 4$ (tai 2) jakautuvat alkutekijöihin $a + bi$ ja $a - bi$. Nämä ovat alkulukuja Gaussin kokonaislukujen joukossa. Jos $p = (a + bi)(a - bi)$, niin $p = a^2 + b^2$.

Tästä eräs varsin lystikäs seuraus on, että alkuluvut $\equiv 1 \pmod 4$ voidaan esittää kahden neliön summana ja alkulukuja $\equiv 3 \pmod 4$ ei voida. Yleisesti, jos luvun alkutekijähajotelmassa alkuluvut $\equiv 3 \pmod 4$ ovat kaikki parilliseen potenssiin ja muut alkutekijät ihan mihin vain, niin luku voidaan esittää kahden neliön summana, mutta ei koskaan muulloin.