Lyhyt johdatus alkeelliseen lukuteoriaan

Esa V. Vesalainen

Sisällysluettelo

Luku 1

Aritmetiikan peruslause

Jakoyhtälö

Lukuteorian alku on seuraavassa intuitiivisesti selvässä tuloksessa, jota toisinaan *jakoyhtälöksi* kutsutaan. Jokainen, joka on ikinä jakanut äärellistä määrää erillisiä olioita yhtäsuuriin kasoihin, tuntee tuloksen jo.

Jakoyhtälö. *Olkoot $a \in \mathbb{Z}$ ja $b \in \mathbb{Z} \setminus \{0\}$. Tällöin on olemassa yksikäsitteiset luvut $q \in \mathbb{Z}$ ja $r \in \mathbb{Z}$, joille*

$$a = qb + r, \qquad ja \qquad 0 \leqslant r < |b| .$$

Käytännössä annetuille luvuille muodostetaan jakoyhtälö kätevimmin tietysti jakokulman avulla. Jakoyhtälön lukua q voi kutsua nimellä *(vaillinainen) osamäärä*, ja luvun r luontevin nimi on *jakojäännös*.

Jaollisuus

Se tilanne, jossa jakoyhtälön antama jakojäännös häviää, on erityinen ja antaa aiheen seuraavaan määritelmään: Olkoot a ja b kokonaislukuja. Sanomme, että *luku a jakaa luvun b*, jos löytyy kokonaisluku c, jolle $b = ac$. Merkitsemme tällöin $a \,|\, b$, ja käytämme myös ilmaisuita *luku b on jaollinen luvulla a*, sekä *luku a on luvun b tekijä*. Jos luku a ei satu jakamaan lukua b, niin merkitsemme $a \nmid b$. Huomautamme, että usein puhumme luvun *positiivisista tekijöistä* sanomalla pelkästään *tekijä*. Käytännössä tämä ei aiheuta sekaannusta.

Olkoot a, b, c ja d kokonaislukuja. On helppo nähdä, että yllä määrittelemällämme jaollisuusrelaatiolla on seuraavat mukavat ominaisuudet:

* Jos $a \mid b$ ja $a \mid c$, niin myös $a \mid (b + c)$ ja $a \mid (b - c)$.
* Jos $a \mid b$ ja $c \mid d$, niin myös $ac \mid bd$.
* Jos $a \mid b$ ja $b \mid c$, niin myös $a \mid c$.
* Jos $a \mid b$ ja $b \mid a$, niin $a = b$ tai $a = -b$.
* Aina pätee $1 \mid a$, $-1 \mid a$ ja $a \mid 0$.
* Aina pätee $a \mid a$ ja $a \mid -a$.

∗ Jos $b \neq 0$ ja $a \mid b$, niin $|a| \leqslant |b|$.

Näistä ensimmäisistä seuraa muun muassa, että

∗ Jos luku jakaa summan jokaisen termin, niin se jakaa myös koko summan.

∗ Jos luku jakaa summan jokaisen termin yhtä lukuun ottamatta, niin se ei voi jakaa koko summaa.

Esimerkkeinä kahdesta viimeisestä ominaisuudesta mainittakoon, että kolmella jaollisten lukujen summat ovat kolmella jaollisia, ja että kun seitsemällä jaolliseen lukuun lisää seitsemällä jaottoman luvun, vaikkapa luvun yksi, niin saadaan seitsemällä jaoton luku.

Alkuluvut

Olkoon $p \in \mathbb{Z}_+$. Lukua p sanotaan *alkuluvuksi*, jos $p > 1$ ja luvun p ainoat tekijät ovat sen triviaalit tekijät ± 1 sekä $\pm p$. Positiivista lukua $n \in \mathbb{Z}_+$ sanotaan *yhdistetyksi luvuksi*, jos se on suurempi kuin yksi mutta ei alkuluku. Luku yksi ei ole alkuluku eikä yhdistetty luku. Pienimmät alkuluvut ovat 2, 3, 5 ja 7.

Havainto. *Jokainen ykköstä suurempi luonnollinen luku on äärellisen monen alkuluvun tulo.*

Todistamme väitteen induktiolla luonnollisen luvun koon suhteen. Luku 2 on alkuluku ja siten varmasti alkulukujen tulo. Olkoon $n \in \mathbb{Z}_+$ lukua kaksi suurempi, ja oletetaan, että kaikki pienemmät ykköstä suuremmat luonnolliset luvut ovat alkulukujen tuloja. Nyt, jos n on alkuluku, asia on selvä. Jos n ei ole alkuluku, niin $n = ab$ joillakin $a, b \in \mathbb{Z}_+$, jotka ovat lukua yksi suurempia mutta lukua n pienempiä. Induktio-oletuksen nojalla siis a ja b, ja siis myös n, ovat alkulukujen tuloja, ja asia on jälleen selvä.

——— : ———

Nyt pääsemme todistamaan ensimmäisen mielenkiintoisen tuloksemme.

Lause. *Alkulukuja on äärettömän monta.*

Vanhin tunnettu todistus tälle, joka löytyy jo Eukleideen *Alkeista*, perustuu seuraavaan yksinkertaiseen havaintoon: Jos parilliseen lukuun lisää ykkösen, saa parittoman luvun. Jos kolmella jaolliseen lukuun lisää ykkösen, saa kolmella jaottoman luvun. Samoin jos viidellä jaolliseen lukuun lisää ykkösen, saa viidellä jaottoman luvun, ja niin edelleen.

Jos alkulukuja olisi vain äärellinen määrä, sanokaamme $n \in \mathbb{Z}_+$ kappaletta, niin ne kaikki voisi kertoa keskenään. Näin saisimme ison luvun P, joka olisi jaollinen kahdella, kolmella, viidellä, ja ylipäätänsä kaikilla alkuluvuilla. Mutta nyt luku $P + 1$ on varmasti suurempi kuin yksi ja siis alkulukujen tulo, mutta toisaalta luvun P määritelmän nojalla se ei voi olla jaollinen kahdella eikä kolmella eikä viidellä, eikä ylipäätänsä millään alkuluvulla, eikä $P + 1$ siis voi olla alkulukujen tulo. Siis se oletus, että alkulukuja olisi vain äärellinen määrä, johtaa ristiriitaan, eikä siten voi pitää paikkaansa.

Kirjoittajan mielestä tämä on koko matematiikan yksinkertaisin (siis helpoiten todistettava) aidosti mielenkiintoinen tulos.

Aritmetiikan peruslause

Tämän luvun päätulos on

Aritmetiikan peruslause. *Jokainen luku $n \in \mathbb{Z}_+$ on tekijöiden järjestystä vaille yksikäsitteisellä tavalla alkulukujen tulo.*

Tässä selkeyden vuoksi sovimme, että tyhjä tulo, jossa ei ole yhtään multiplikandia, on yhtä kuin yksi.

Alkuluvut ovat siis eräänlaisia atomeita, joista kaikki muut luonnolliset luvut on rakennettu kertolaskulla, ja jokaisen luonnollisen luvun saa vain oleellisesti ottaen yhdellä tavalla kertomalla alkulukuja keskenään. Esitämme tälle väitteelle Zermelon todistuksen:

Todistus. Todistamme väitteen induktiolla luvun n suhteen. Ensinnäkin väite on selvä tapauksessa $n = 1$. Samoin muut pienet tapaukset, kuten $n = 2$, $n = 3$, ja niin edelleen, ovat varsin selviä.

Oletetaan sitten, että $n > 1$ ja että väite on jo todistettu kaikille lukua n pienemmille positiivisille kokonaisluvuille. Meidän on siis todistettava kaksi asiaa: ensinnäkin meidän on osoitettava, että luku n on alkulukujen tulo, ja toiseksi meidän on osoitettava, että se on alkulukujen tulo vain yhdellä tavalla. Toisin sanoen, meidän on myös osoitettava, että jos luvun n kirjoittaa kahdella eri tavalla alkulukujen tulona, niin itse asiassa molemmissa tuloissa esiintyvät täsmälleen samat alkuluvut, tosin mahdollisesti eri järjestyksessä.

Jos luku n sattuu olemaan alkuluku, mitään todistettavaa ei ole. Muutoin on olemassa pienin epätriviaali luvun n tekijä p, siis pienin $p \in \mathbb{Z}_+$, jolle $p \mid n$ ja $1 < p < n$. Varmasti tämä luku p on alkuluku, sillä sen epätriviaali tekijä olisi lukua p pienempi luvun n epätriviaali tekijä.

Kirjoitetaan $n = pb$, missä $b \in \mathbb{Z}_+$ on varmasti pienempi kuin n. Nyt induktio-oletuksen nojalla luku b on alkulukujen tulo, ja siis luku n on myös alkulukujen tulo. Lisäksi, koska luku b on alkulukujen tulo yksikäsitteisellä tavalla, on luvulla n vain yksi alkutekijöihinjako, jossa esiintyy luku p.

Seuraavaksi on osoitettava, että luvulla n ei voi olla muita alkutekijöihinjakoja. Tehdään se vastaoletus, että luvulla n olisi jokin muukin alkutekijöihinjako. Olkoon sen pienin alkutekijä q. Nyt siis $p < q$ ja $n = qc$ jollakin $c \in \mathbb{Z}_+$, jolle $c < n$ ja $p \nmid c$.

Seuraavaksi tarkastellaan lukua

$$n_0 = n - pc = \begin{cases} pb - pc = p\,(b - c)\,, \\ qc - pc = (q - p)\,c. \end{cases}$$

Tämä luku on positiivinen kokonaisluku ja varmasti pienempi kuin n. Koska $p \mid n_0$, on induktio-oletuksen nojalla alkuluvun p esiinnyttävä tulon $(q - p)\,c$ alkutekijähajotelmassa, ja siis ainakin toisen luvuista $q - p$ ja c alkutekijähajotelmassa. Mutta olemme jo todenneet, että $p \nmid c$, ja jos olisi $p \mid (q - p)$, niin olisi myös $p \mid (q - p + p) = q$, ja koska p ja q ovat molemmat alkulukuja, olisi $p = q$, vastoin sitä seikkaa, että $p < q$. Olemme päätyneet ristiriitaan, ja siksi luvulla n on oltava vain yksi alkutekijöihinjako, ja olemme valmiit.

Yksikäsitteisen tekijöihinjaon epäonnistuminen

Tarkastelemme seuraavaksi sitä, miten yksikäsitteinen tekijöihinjako voi mennä pieleen. Luonnollisesti tavalliset luonnolliset luvut eivät tarjoa tähän mahdollisuutta juuri todistetun aritmetiikan peruslauseen nojalla, joten joudumme turvautumaan toisenlaisiin esimerkkeihin.

Hilbertin esimerkki

Tarkastellaan lukuja muotoa $4n+1$, missä $n = 0, 1, 2, \ldots$, siis lukuja

$$1,\ 5,\ 9,\ 13,\ 17,\ 21,\ 25,\ 29,\ 33,\ 37,\ 41,\ 45,\ 49,\ 53,\ 57,\ 61,\ \&c.$$

Tällaisten lukujen tulot ovat samaa muotoa, onhan kaikilla $m \in \mathbb{Z}$ ja $n \in \mathbb{Z}$

$$(4m+1)(4n+1) = 4\,(4mn + m + n) + 1.$$

Voimme siis määritellä näille luvuille jaollisuuden ja alkuluvun käsitteen. Tällöin "alkulukuja" tulevat olemaan

$$5,\ 9,\ 13,\ 17,\ 21,\ 29,\ 33,\ \&c.$$

Lisäksi meillä tulee olemaan tekijöihinjakoja, kuten vaikkapa

$$25 = 5 \cdot 5, \quad 45 = 5 \cdot 9, \quad 81 = 9 \cdot 9, \quad \text{ja niin edelleen.}$$

Mutta yksikäsittinen tekijöihinjako ei näille luvuille päde. Nimittäin, luku 441 voidaan esittää "alkulukujen" tulona sekä tavalla $21 \cdot 21$ että tavalla $9 \cdot 49$.

Vakavampia esimerkkejä

Lukuteoriassa tarkastellaan usein erilaisia kokonaislukukäsitteen laajennoksia. Esimerkiksi *Gaussin kokonaisluvuille*, joiden määritellään olevan kompleksilukuja muotoa $a + bi$ kokonaisluvuilla a ja b. Tällaisten lukujen summat, erotukset ja tulot ovat samaa muotoa, ja siksi voimme näillekin luvuille määritellä jaollisuuden ja alkuluvun käsitteet. Osoittautuu, että Gaussin kokonaisluvuille pätee yksikäsitteinen tekijöihinjako.

Toisaalta, jos tarkastelemme kompleksilukuja muotoa $a+bi\sqrt{5}$, missä lukujen a ja b on oltava kokonaislukuja, niin tätäkin muotoa olevien lukujen summat, erotukset ja tulot tulevat olemaan samaa muotoa; onhan kaikilla $a, b, c, d \in \mathbb{Z}$:

$$\left(a + bi\sqrt{5}\right) \pm \left(c + di\sqrt{5}\right) = (a \pm c) + (b \pm d)\, i\sqrt{5},$$

sekä

$$\left(a + bi\sqrt{5}\right)\left(c + di\sqrt{5}\right) = (ac - 5bd) + (ad + bc)\, i\sqrt{5}.$$

Siis näillekin luvuille voi määritellä jaollisuuden ja alkuluvut. Mutta nyt meillä ei olekaan yksikäsitteistä tekijöihinjakoa. Nimittäin,

$$21 = 3 \cdot 7 = \left(1 - 2i\sqrt{5}\right)\left(1 + 2i\sqrt{5}\right),$$

ja luvut 3, 7, $1-2i\sqrt{5}$ ja $1+2i\sqrt{5}$ ovat kaikki "alkulukuja" viimeksi määritellyssä mielessä.

Luvun tekijöiden lukumäärä ja summa

Olkoon $n \in \mathbb{Z}_+$ ja $n > 1$. Luvulla n tiedetään olevan yksikäsitteinen tekijöihinjako, sanokaamme $n = q_1 q_2 \cdots q_t$, missä q_1, q_2, …, q_t ovat alkulukuja, ja $t \in \mathbb{Z}_+$. Ryhmittelemällä yhtä suuret alkuluvut alkulukupotensseiksi voimme kirjoittaa

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\nu^{\alpha_\nu}$$

joillakin alkuluvuilla $p_1 < p_2 < \ldots < p_\nu$, ja joillakin $\alpha_1, \alpha_2, \ldots, \alpha_\nu \in \mathbb{Z}_+$, missä $\nu \in \mathbb{Z}_+$. Tätä on tapana kutsua nimellä luvun n *kanoninen alkutekijähajotelma*.

Sovellutuksena alkutekijöihinjaon yksikäsitteisyydestä esitämme kaavat luvun n positiivisten tekijöiden lukumäärälle ja summalle sen kanonisen alkutekijähajotelman avulla.

Luvun n tekijöiden lukumäärä

Luvun n tekijöiden lukumäärää merkitään $d(n)$, toisinaan myös $\tau(n)$.

Esimerkkejä. Varmasti $d(1) = 1$. Luvun 6 tekijät ovat 1, 2, 3 ja 6, joten $d(6) = 4$. Jos p on alkuluku, niin luvun p ainoat tekijät ovat sen triviaalit tekijät 1 ja p, ja siis $d(p) = 2$.

Jokainen luvun n tekijä on aritmetiikan peruslauseen nojalla muotoa

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_\nu^{\beta_\nu}$$

joillakin ei-negatiivisilla kokonaisluvuilla $\beta_1, \beta_2, \ldots \beta_\nu$. Eksponentin β_1 voi valita $\alpha_1 + 1$ eri tavalla, eksponentin β_2 voi valita $\alpha_2 + 1$ eri tavalla, ja niin edelleen, ja eksponentin β_ν voi valita $\alpha_\nu + 1$ eri tavalla. Näin voidaan varmasti valita mikä tahansa luvun n tekijä. Toisaalta, jokaisen tekijän voi muodostaa tällä tavalla vain yhdellä tavalla. Siispä luvun n tekijöitä on yhtä monta kuin eksponenttien β valintoja, eli

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_\nu + 1)\,.$$

Esimerkki. Helposti nähdään, että luvun 360 kanoninen alkutekijähajotelma on $2^3 \cdot 3^2 \cdot 5$, ja sijoittamalla tästä eksponentit yllä johdettuun kaavaan saadaan, että

$$d(360) = (3+1)(2+1)(1+1) = 4 \cdot 3 \cdot 2 = 24.$$

Toinen esimerkki. Eräs tärkeä seuraus yllä johdetusta kaavasta on tekijäfunktion $d(\cdot)$ *multiplikatiivisuus*: jos $m \in \mathbb{Z}_+$ ja $n \in \mathbb{Z}_+$ ovat yhteistekijättömiä, niin $d(mn) = d(m)\,d(n)$.

Luvun n tekijöiden summa

Luvun n tekijöiden summaa merkitään $\sigma(n)$.

Esimerkkejä. Varmasti $\sigma(1) = 1$. Luvun 6 tekijät ovat 1, 2, 3 ja 6, joten

$$\sigma(6) = 1 + 2 + 3 + 6 = 12.$$

Jos p on alkuluku, niin luvun p ainoat tekijät ovat sen triviaalit tekijä 1 ja p, eli

$$\sigma(p) = p + 1.$$

Koska luvun n tekijät ovat täsmälleen keskenään erisuuret luvut $p_1^{\beta_1} \cdots p_\nu^{\beta_\nu}$, niin on oltava

$$\begin{aligned}\sigma(n) = &\left(1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1}\right) \\ &\cdot \left(1 + p_2 + p_2^2 + \ldots + p_2^{\alpha_2}\right) \\ &\cdot \ldots \cdot \left(1 + p_\nu + p_\nu^2 + \ldots + p_\nu^{\alpha_\nu}\right) \\ =&\frac{p^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_\nu^{\alpha_\nu+1} - 1}{p_\nu - 1}.\end{aligned}$$

Esimerkki. Käyttämällä jälleen tekijöihinjakoa $360 = 2^3 \cdot 3^2 \cdot 5$ nähdään, että

$$\sigma(360) = \frac{2^{3+1} - 1}{2 - 1} \cdot \frac{3^{2+1} - 1}{3 - 1} \cdot \frac{5^{1+1} - 1}{5 - 1} = 15 \cdot \frac{26}{2} \cdot \frac{24}{4} = 15 \cdot 13 \cdot 6 = 1170.$$

Toinen esimerkki. Jälleen johdetusta kaavasta seuraa multiplikatiivisuus: jos $m \in \mathbb{Z}_+$ ja $n \in \mathbb{Z}_+$ ovat yhteistekijättömiä, niin $\sigma(mn) = \sigma(m)\,\sigma(n)$.

Täydelliset luvut

Luvun $n \in \mathbb{Z}_+$ sanotaan olevan *täydellinen*, jos

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

Tämä tarkoittaa siis sitä, että n on itseään pienempien tekijöidensä summa.

Esimerkki. Luvut 6 ja 28 ovat täydellisiä, sillä luvun 6 itseään pienemmät tekijät ovat 1, 2 ja 3, ja

$$1 + 2 + 3 = 6,$$

kun taas puolestaan luvun 28 itseään pienemmät tekijät ovat 1, 2, 4, 7 ja 14, ja näiden summa on

$$1 + 2 + 4 + 7 + 14 = 28.$$

Eukleideen–Eulerin lause. *Parillinen positiivinen kokonaisluku n on täydellinen jos ja vain jos n on muotoa $2^{p-1}\,(2^p - 1)$ jollakin luvulla p, jolle $2^p - 1$ on myös alkuluku.*

On varsin suoraviivaista todistaa, että muotoa $2^{p-1}\,(2^p-1)$ olevat luvut, missä p on alkuluku ja 2^p-1 oletetaan myös alkulukuvuksi, ovat täydellisiä. Nimittäin

$$\sigma\big(2^{p-1}(2^p-1)\big) = \sigma\big(2^{p-1}\big)\,\sigma\big(2^p-1\big) = \frac{2^p-1}{2-1}\cdot(1+2^p-1) = 2\cdot 2^{p-1}\,(2^p-1)\,.$$

Oletetaan seuraavaksi, että $n \in \mathbb{Z}_+$ on mielivaltainen täydellinen luku. Olkoon $n = 2^\alpha m$, missä $\alpha, m \in \mathbb{Z}_+$ ja m on pariton. Näillä merkinnöillä

$$2^{\alpha+1}m = 2n = \sigma(n) = \sigma(2^\alpha m) = \sigma(2^\alpha)\,\sigma(m) = \big(2^{\alpha+1}-1\big)\,\sigma(m)\,.$$

Tästä seuraa välittömästi, että $\big(2^{\alpha+1}-1\big)\,|\,m$, ja uudelleenryhmittelemällä nähdään, että

$$\sigma(m) = m + \frac{m}{2^{\alpha+1}-1}.$$

Mutta tämän nojalla luvulla m on vain kaksi tekijää. Luvun m on siis oltava alkuluku ja $m = 2^{\alpha+1}-1$, mikä oli todistettava.

Kotitehtäviä

1. Olkoot a, b, c ja d sellaisia kokonaislukuja että $a \neq c$ ja $(a-c)\,|\,(ab+cd)$. Osoita, että $(a-c)\,|\,(ad+bc)$.

2. **a)** Mitä voit sanoa luvusta $n \in \mathbb{Z}_+$, jos $d(n) = 2$?
b) Mitä voit sanoa luvusta $n \in \mathbb{Z}_+$, jos $d(n)$ on pariton alkuluku?
c) Mitä voit sanoa luvusta $n \in \mathbb{Z}_+$, jos $d(n)$ on pariton?

3. **a)** Mitä voit sanoa luvusta $n \in \mathbb{Z}_+$, jos $\sigma(n) = n+1$?
b) Mitä voit sanoa luvusta $n \in \mathbb{Z}_+$, jos $\sigma(n) = a+b$ joillakin luvun n kahdella eri tekijällä a ja b?
c) Totesimme aiemmin, että luvut 6 ja 28 ovat täydellisiä. Selvitä Eukleideen–Eulerin lauseeseen nojautuen kaksi seuraavaksi pienintä parillista täydellistä lukua.

4. **a)** Selvitä lukujen 1080, 667 ja 1573 kanoniset alkutekijähajotelmat.
b) Laske luvut $d(1080)$, $d(667)$, $d(1573)$, $\sigma(1080)$, $\sigma(667)$, sekä $\sigma(1573)$.

5. Mitä on luvun $n \in \mathbb{Z}_+$ tekijöiden tulo?

6. **a)** Osoita, että pariton täydellinen luku ei voi olla alkuluvun potenssi.
b) Osoita, että parittomalla täydellisellä luvulla on oltava ainakin kolme eri suurta alkulukutekijää.

7. **a)** Olkoon p alkuluku. Etsi positiiviset kokonaisluvut x ja y, joille

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{p}.$$

b) Etsi kokonaislukuparit $\langle x, y\rangle$, joille

$$(x+1)^2\,y + (y+1)^2\,x = 1.$$

8. Tämän tehtävän tavoitteena on soveltaa esitettyä aritmetiikan peruslauseen todistusta polynomeille.

Kutsumme ei-vakiota rationaalilukukertoimista polynomia $P(x)$ *jaottomaksi* jos se ei ole alempaa astetta olevien rationaalilukukertoimisten polynomien tulo. Kutsumme polynomia $P(x)$ *alkupolynomiksi* (tämä ei ole yleisesti käytetty termi), jos se on jaoton ja sen korkeimman asteen termin kerroin on yksi. Tämä vastaa rajoittumista positiivisiin alkulukuihin 2, 3, 5, 7, 11, ..., eli negatiivisten lukujen -2, -3, -5, ja niin edelleen, poissulkemista.

Osoita aiemmin esitettyä aritmetiikan peruslausetta mukaillen, että jokainen rationaalilukukertoiminen polynomi, jonka korkeimman asteen termin kerroin on yksi, on tekijöiden järjestystä vaille yksikäsitteisellä tavalla alkupolynomien tulo. [Vihje: suorita induktio polynomin asteen suhteen, ja erotuksen $n_0 = n - pc$ sijaan tarkastele erotusta $n_0 = n - hpc$, missä h on jokin polynomi, jolle $q - hp$ on alempaa astetta kuin q.]

Mitä todistukselle käy, jos sanan rationaaliluku korvaa sanalla reaaliluku tai sanalla kompleksiluku?

Luku 2

Eukleideen algoritmi ja kongruenssit

Suurin yhteinen tekijä ja Eukleideen algoritmi

Olkoot a ja b kokonaislukuja, jotka eivät molemmat ole nollia. Tällöin lukujen a ja b *suurin yhteinen tekijä* on suurin positiivinen kokonaisluku d, joka jakaa molemmat luvuista a ja b. Merkitsemme tätä lukua symbolilla (a, b). Pedanttinen lukija voi määritellä $(0, 0) = 0$, mutta tällä ei ole suurta merkitystä. Samoin määrittelemme useamman luvun a, b, $\ldots$, z suurimman yhteisen tekijän $(a, b, \ldots, z)$.

Suurimman yhteisen tekijän laskemiseen on olemassa *Eukleideen algoritmin* nimellä kulkeva menetelmä. Olkoot a ja b positiivisia kokonaislukuja, ja oletetaan, että vaikkapa $a > b$. Tällöin jakoyhtälön nojalla löytyy yksikäsitteiset kokonaisluvut q_1 ja r_1 joille

$$a = q_1 b + r_1, \quad \text{ja} \quad 0 \leqslant r_1 < b.$$

Jos $r_1 \neq 0$, niin edelleen löytyy yksikäsitteiset kokonaisluvut q_2 ja r_2, joille

$$b = q_2 r_1 + r_2, \quad \text{ja} \quad 0 \leqslant r_2 < r_1.$$

Ja jos $r_2 \neq 0$, niin löytyy yksikäsitteiset kokonaisluvut q_3 ja r_3, joille

$$r_1 = q_3 r_2 + r_3, \quad \text{ja} \quad 0 \leqslant r_3 < r_2.$$

Jatketaan tätä niin kauan kuin mahdollista. Koska jakojäännökset r_1, r_2, r_3, $\ldots$ muodostavat aidosti vähenevän ei-negatiivisten kokonaislukujen jonon, niin voimme toistaa operaatiota vain äärellisen monta kertaa. Lopulta jokin jakojäännös, sanokaamma r_N, missä $N \in \mathbb{Z}_+$, häviää.

Nyt olemme saaneet jonon yhtälöitä

$$\begin{cases} a = q_1 b + r_1, \\ b = q_2 r_1 + r_2, \\ r_1 = q_3 r_2 + r_3, \\ \quad \ldots\ldots\ldots\ldots \\ r_{N-4} = q_{N-2} r_{N-3} + r_{N-2}, \\ r_{N-3} = q_{N-1} r_{N-2} + r_{N-1}, \\ r_{N-2} = q_N r_{N-1}. \end{cases}$$

Koska (a, b) jakaa molemmat luvuista a ja b, niin se ensimmäisen yhtälön nojalla jakaa myös luvun r_1. Mutta nyt se jakaa molemmat luvuista b ja r_1, eli se toisen yhtälön nojalla jakaa myös luvun r_2. Jatkamalla samalla tavalla nähdään, että (a, b) jakaa jokaisen luvuista $r_1, r_2, \ldots, r_{N-1}$, erityisesti luvun r_{N-1}.

Toisaalta, viimeisen yhtälön nojalla $r_{N-1} \mid r_{N-2}$. Toiseksi viimeisen yhtälön nojalla $r_{N-1} \mid r_{N-3}$. Ja kolmanneksi viimeisen yhtälön nojalla myös $r_{N-1} \mid r_{N-4}$. Jatkamalla tätä päättelyketjua näemme lopulta, että $r_{N-1} \mid a$ ja $r_{N-1} \mid b$.

Nyt $0 < (a, b) \mid r_{N-1}$, eli $(a, b) \leqslant r_{N-1}$. Toisaalta, luku r_{N-1} on lukujen a ja b yhteinen tekijä. Varmasti nyt $r_{N-1} = (a, b)$.

Lineaariset Diofantosin yhtälöt

Olkoot annetut kokonaisluvut a ja b. Huomaamme, että Eukleideen algoritmissa laskettujen jakoyhtälöiden avulla voimme löytää kokonaisluvut x ja y, jotka ratkaisevat *lineaarisen Diofantoksen yhtälön*

$$ax + by = (a, b)\,.$$

Esimerkki. Etsitään kokonaisluvut s ja t, joille $123s + 152t = 1$. Käytetään Eukleideen algoritmia:

$$152 = 123 \cdot 1 + 29, \quad 123 = 29 \cdot 4 + 7, \quad 29 = 7 \cdot 4 + 1.$$

Tästä päättelemme, että

$$\begin{aligned} 1 &= 29 - 7 \cdot 4 = 152 - 123 - (123 - 29 \cdot 4) \cdot 4 \\ &= 152 - 123 - 123 \cdot 4 + (152 - 123) \cdot 16 \\ &= 152 - 123 \cdot 5 + 152 \cdot 16 - 123 \cdot 16 \\ &= 152 \cdot 17 - 123 \cdot 21. \end{aligned}$$

Yksikäsitteinen tekijöihinjako, jälleen kerran

Eukleideen lemma. *Olkoon p alkuluku, ja olkoot a ja b sellaisia kokonaislukuja, että $p \mid ab$. Tällöin $p \mid a$ tai $p \mid b$.*

Jos $p \mid a$, niin asia on selvä. Oletetaan siis, että $p \nmid a$. Tällöin luvut p ja a ovat yhteistekijättömiä ja on löydyttävä luvut $x, y \in \mathbb{Z}$, joille

$$ax + py = 1.$$

Mutta nyt myös

$$abx + pby = b,$$

ja koska luku p jakaa tässä vasemman puolen, on oltava $p \mid b$. q.e.d.

——:——

Yksikäsitteinen tekijöihinjako. *Jokainen lukua yksi suurempi positiivinen kokonaisluku on tekijöiden järjestystä vaille yksikäsitteisellä tavalla alkulukujen tulo.*

Olemme jo aiemmin todistaneet, että jokainen lukua yksi suurempi positiivinen kokonaisluku on alkulukujen tulo. Riittää siis todistaa yksikäsitteisyys. Tarkastellaan kahta yhtä suurta alkulukujen tuloa

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

missä $r, s \in \mathbb{Z}_+$ ja $p_1, p_2, \ldots, p_r$ sekä $q_1, q_2, \ldots, q_s$ ovat alkulukuja.

Oletetaan, että $r \geqslant s$. Alkuluku p_1 jakaa oikean puolen ja Eukleideen lemman nojalla siis myös jonkin luvun q_k, ... Mutta koska kyseiset luvut ovat alkulukuja, on oltava $p_1 = q_k$, ja voimme supistaa luvut p_1 ja q_k yhtälöstä pois. Voimme päätellä näin toistuvasti, kunnes vasemmalla puolella ei ole jäljellä kuin luku yksi. Nyt oikealla puolella ei myöskään voi olla jäljellä alkulukuja. Päädymme siis siihen johtopäätökseen, että $r = s$ ja alkuperäisen yhtäsuuruuden molemmilla puolilla olivat samat alkuluvut, mutta vain eri järjestyksessä.

Kongruenssin käsite ja perusominaisuuksia

Olemme jo tarkastelleet sitä tilannetta, jossa jakoyhtälön jakojäännös häviää. Seuraavaksi keskitymme tarkastelemaan niitä tilanteita jossa kahdella eri kokonaisluvulla a ja b on sama jakojäännös saman jakajan $m \in \mathbb{Z}_+$ suhteen. Tällaisessa tilanteessa $a = mq + r$ ja $b = m\widetilde{q} + \widetilde{r}$ joillakin yksikäsitteisillä $q, \widetilde{q} \in \mathbb{Z}$ sekä $r, \widetilde{r} \in \{0, 1, \ldots, m-1\}$. Huomaamme, että $a - b = m\,(q - \widetilde{q}\,)$, eli $m \,|\, (a - b)$. Tämä johtaa seuraavaan käsitteeseen sekä vastaavaan kätevään merkintään, jotka esitteli ensimmäisen kerran C. F. Gauss kuuluisassa teoksessaan *Disquisitiones Arithmeticae*.

Olkoot $a, b \in \mathbb{Z}$ ja $m \in \mathbb{Z}_+$. Jos $m \mid (a - b)$, niin sanomme, että *a ja b ovat keskenään kongruentteja modulo m*, ja merkitsemme $a \equiv b \pmod{m}$. Joskus myös merkitään $a \equiv b\,(m)$. Jos a ei ole kongruentti luvun b kanssa modulo m, merkitsemme vastaavasti $a \not\equiv b \pmod{m}$.

Vaikka tämä on uusi käsite, asian ydin tulee olemaan, että lukija jo osaa käsitellä kongruensseja. Kongruenssimerkintä kokonaisluvuille, kiinteällä m, käyttäytyy nimittäin peruslaskutoimitusten suhteen melkein samoin kuin yhtäsuuruusmerkintä rationaali- rai reaaliluvuillekin. Kun m on alkuluku, analogia tulee olemaan erityisen tarkka.

——— : ———

Olkoot $a, b, c, d \in \mathbb{Z}$ ja $m \in \mathbb{Z}_+$. Seuraavat havainnot ovat varsin selviä:

* Aina pätee $a \equiv a \pmod{m}$.
* Jos $a \equiv b \pmod{m}$, niin myös $b \equiv a \pmod{m}$.
* Jos $a \equiv b$ ja $b \equiv c \pmod{m}$, niin $a \equiv c \pmod{m}$.

Kongruensseja voi tutulla tavalla laskea yhteen, vähentaa ja kertoa puolittain: jos $a \equiv b$ ja $c \equiv d \pmod{m}$, niin

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

Jakaminen puolittain on mielenkiintoisempi operaatio. Tietysti, jos $ac \equiv bc \pmod{m}$, niin varmasti

$$a \equiv b \pmod{\frac{m}{(m, c)}}.$$

Erityisesti siis kongruensseista voi jakaa puolittain pois yhtäsuuria multiplikandeja jotka ovat yhteistekijättömiä moduluksen kanssa.

Mutta ilmenee, että kongruensseissa voi jakaa puolittain paljon yleisemmässäkin mielessä. Nimittäin, olkoot $a, b \in \mathbb{Z}$ ja $m \in \mathbb{Z}_+$ sellaisia, että a ja m ovat yhteistekijättömiä. Tarkastellaan seuraavaa kysymystä: milloin on olemassa ja miten löydetään $x \in \mathbb{Z}$ jolle

$$ax \equiv b \pmod{m}?$$

Tämä kongruenssi tietenkin tarkoittaa sitä, että $m \mid (ax - b)$, eli sitä, että $ax - b = my$ jollakin $y \in \mathbb{Z}$. Mutta nythän ongelma on palautettu lineaarisen Diofantoksen yhtälön

$$ax - my = b$$

ratkaisuun. Ja aiempien tässä luvussa tehtyjen havaintojen perusteella tällä on ratkaisu, ja osaamme jopa tuottaa sellaisen Eukleideen algoritmilla. Siis kongruenssien jakolasku on samaa kuin lineaaristen Diofantosin yhtälöiden ratkaisu!

Fermat'n pieni lause

Seuraavaksi todistamme keskeisen perustuloksen:

Fermat'n pieni lause. *Olkoon p alkuluku ja olkoon a sellainen kokonaisluku, että $p \nmid a$. Tällöin*

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

Luonnollisesti tämän tuloksen voi kirjoittaa myös toisessa muodossa:

Fermat'n pieni lause. *Olkoon p alkuluku ja olkoon a mielivaltainen kokonaisluku. Tällöin*

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

Ettei tuloksen tärkeys vain jäisi lukijalle epäselväksi, todistamme sen varmuuden vuoksi kolmella eri tavalla. Todistuksista ensimmäinen on tavoitteidemme kannalta selvästi tärkein. Muihin lukija voi suhtautua viihteenä.

Ensimmäinen todistus. Olkoon p alkuluku ja $a \in \mathbb{Z}$ luvulla p jaoton. Asian ydin on seuraava: mitkään kaksi luvuista

$$a, \quad 2a, \quad 3a, \quad \ldots, \quad (p-1)\,a$$

eivät ole keskenään kongruentteja modulo p. Nimittäin, jos $ka \equiv \ell a \pmod{p}$, missä $k, \ell \in \{1, 2, \ldots, p-1\}$, niin tietysti $k \equiv \ell \pmod{p}$.

Mutta koska mikään näistä luvuista ei ole jaollinen alkuluvulla p, jokainen näistä luvuista on kongruentti täsmälleen yhden luvuista 1, 2, ..., $p-1$ kanssa, ja päin vastoin.

Nyt siis varmasti

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a \cdot 2a \cdot \ldots \cdot \cdots \cdot (p-1)\,a \pmod{p},$$

eli $(p-1)! \equiv a^{p-1}\,(p-1)! \pmod{p}$. Lopuksi, koska varmasti $p \nmid (p-1)!$, on oltava $a^{p-1} \equiv 1 \pmod{p}$. Q.E.D.

Toinen todistus. Olkoon p alkuluku. Varmasti $0^p \equiv 0 \pmod{p}$. Oletetaan, että $a^p \equiv a \pmod{p}$ jollakin $a \in \mathbb{Z}$. Binomikertoimet $\binom{p}{1}$, $\binom{p}{2}$, $\ldots$, $\binom{p}{p-1}$ ovat kaikki jaollisia luvulla p, sillä jokainen niistä on muotoa $\frac{p(p-1)\cdots(p-\ell+1)}{1\cdot 2\cdot\ldots\cdot\ell}$ jollakin $\ell \in \{1, 2, \ldots, p-1\}$, ja tässä osamäärässä p jakaa osoittajan, mutta ei nimittäjää.

Mutta nyt binomikaavan nojalla

$$\begin{aligned}(a \pm 1)^p &\equiv \binom{p}{0}a^p \pm \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} \pm \ldots + \binom{p}{p-1}a \pm \binom{p}{p} \\ &\equiv a^p \pm 1 \equiv a \pm 1 \pmod{p},\end{aligned}$$

ja Fermat'n pienen lauseen toinen muotoilu seuraa induktiolla.

Kolmas todistus. Todistamme jälleen Fermat'n pienen lauseen toisen muotoilun, tällä kertaa kauniilla ja yksinkertaisella kombinatorisella argumentilla.

Itse asiassa paljon myöhemmin tätä lukeva lukiolainen tulee näkemään, että tässä argumentissa on loppujen lopuksi kysymys *transformaatioryhmistä*, jotka ovat matematiikan keskeisiä peruskäsitteitä.

Oletetaan, että meillä on a eri helmityyppiä, ja että käytettävissämme on kutakin tyyppiä rajattomasti. Ideana on tarkastella näistä helmistä valmistettavia p helmen kaulaketjuja. Tässä helminauha voi siis olla erilainen kuin peilikuvansa, ja sijainnilla on väliä; jokaisessa helminauhassa on yksikäsitteinen ensimmäinen helmi, toinen helmi, ja niin edelleen.

Helminauhamme, joita on yhteensä a^p eri kappaletta, jakautuvat kahteen eri kategoriaan. Ensimmäinen sisältää täsmälleen ne a eri helminauhaa, joista jokainen on rakennettu vain yhdentyyppisiä helmiä käyttäen. Loput $a^p - a$ helminauhaa ovat sellaisia, että niitä kiertämällä — siirtämällä ensimmäinen helmi toisen helmen paikalle, toinen helmi kolmannen paikalle, ja niin edelleen, ja p. helmi ensimmäisen paikalle — saadaan täsmälleen p eri helminauhaa.

Kyseiset $a^p - a$ helminauhaa jakautuvat siis p helmen ryhmiin, joista jokaisessa minkä tahansa nauhan saa toisesta sopivan monta kertaa kiertämällä. Mutta nyt täytyy olla $p \mid (a^p - a)$. Q.E.D.

Wilsonin lause

Koska meillä on vain äärellisen monta jäännösluokkaa modulo p, voimme kysyä vaikkapa mitä niiden tulo on modulo p? Modulo 2 asia on selvä: $1 \equiv 1 \equiv 1 \pmod{2}$, joten oletetaan, että p on pariton.

Havaitkaamme ensin seuraavaa: ainoat elementit, jotka ovat omia käänteiselementtejään modulo p, ovat ± 1. Tarkemmin, jos $x^2 \equiv 1 \pmod{p}$, niin $x \equiv \pm 1 \pmod{p}$. Nimittäin, $x^2 \equiv 1 \pmod{p}$ jos ja vain jos $(x+1)(x-1) \equiv 0 \pmod{p}$.

Mutta tämä tarkoittaa sitä, että jos $x \not\equiv 0$ ja $x \not\equiv \pm 1 \pmod{p}$, niin on olemassa yksikäsitteinen $y \not\equiv 0 \pmod{p}$, jolle $xy \equiv 1 \pmod{p}$, ja tälle y pätee $x \not\equiv y \pmod{p}$.

Jäännösluokat 2, 3, $\ldots$, $p-2$ jakautuvat siis siististi pareiksi joiden tulot ovat kaikki kongruentteja luvun yksi kanssa modulo p. Toisin sanoen, kaikkien nollasta poikkeavien jäännösluokkien tulossa kaikki multiplikandit paitsi ± 1 supistuvat pois, eli

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot \cdots (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

Yhdistämällä tämä siihen havaintoon, jonka jätämme lukijalle harjoitustehtäväksi, että $(m-1)! \equiv 0$ tai $2 \pmod{m}$ kaikilla yhdistetyillä $m \in \mathbb{Z}_+ \setminus \{1\}$, saamme seuraavan tuloksen

Wilsonin lause. *Olkoon $m > 1$ kokonaisluku. Tällöin m on alkuluku täsmälleen silloin kun*

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

Tämä teoreema antaa varsin epäkäytännöllisen tavan testata onko annettu luku alkuluku vai ei.

Kotitehtäviä

9. Ratkaise ensimmäisen asteen kongruenssit

a) $13x \equiv 31 \pmod{37}$;
b) $15x \equiv 9 \pmod{61}$.

10. Osoita, että murtoluku $\frac{21n+4}{14n+3}$ on aina supistetussa muodossa, oli luvun $n \in \mathbb{Z}$ arvo mikä tahansa.

11. Osoita Wilsonin lauseen toinen puoli: jos $n > 1$ on kokonaisluku mutta ei alkuluku, niin $(n-1)! \not\equiv -1 \pmod{n}$.

12. Olkoon p alkuluku ja $x_1, x_2, \ldots, x_p$ kokonaislukuja. Osoita, että jos

$$x_1^{p-1} + x_2^{p-1} + \ldots + x_p^{p-1} \equiv 0 \pmod{p},$$

niin löytyy indeksit $k, \ell \in \{1, 2, \ldots, p\}$ joille $k \neq \ell$ ja $x_k \equiv x_\ell \pmod{p}$.

13. Olkoon p pariton alkuluku ja olkoon n positiivinen kokonaisluku. Osoita, että luku

$$1^{p^n} + 2^{p^n} + 3^{p^n} + \ldots + (p-1)^{p^n}$$

on jaollinen luvulla p.

14. Osoita Wilsonin lauseen avulla, että jokaisella alkuluvulla p, jolle pätee $p \equiv 1 \pmod{4}$, löytyy kokonaisluku n siten, että $n^2 \equiv -1 \pmod{p}$.

15. Etsi kaikki ne positiiviset kokonaisluvut jotka ovat yhteistekijättömiä kaikkien jonon

$$a_n = 2^n + 3^n + 6^n - 1, \qquad (n \in \mathbb{Z}_+)$$

elementtien kanssa.

16. Olkoon n positiivinen kokonaisluku ja olkoot $a_1, a_2, \ldots, a_k$ $(k \geqslant 2)$ pareittain erisuuria kokonaislukuja joukosta $\{1, 2, \ldots, n\}$. Oletetaan, että $n \mid a_i\,(a_{i+1} - 1)$ jokaisella $i = 1, 2, \ldots, k-1$. Osoita, että $n \nmid a_k\,(a_1 - 1)$.

Luku 3

Lisää kongruensseista

Jaollisuussääntöjä

Tarkastellaan kokonaislukukertoimista polynomia

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

missä $n \in \mathbb{Z}_+$. Olkoon $m \in \mathbb{Z}_+$ ja olkoot $a, b \in \mathbb{Z}$ sellaisia, että $a \equiv b \pmod{m}$. Nyt varmasti

$$\left.\begin{array}{c} a_0 \equiv a_0 \\ a_1 a \equiv a_1 b \\ a_2 a^2 \equiv a_2 b^2 \\ \ldots\ldots\ldots \\ a_n a^n \equiv a_n b^n \end{array}\right\} \pmod{m},$$

ja laskemalla nämä kongruenssit puolittain yhteen nähdään, että

$$P(a) \equiv P(b) \pmod{m}.$$

——:——

Koska $10 \equiv 1 \pmod{3}$ ja $10 \equiv 1 \pmod{9}$, on kaikilla kokonaislukukertoimisilla polynomeilla pädettävä

$$P(10) \equiv P(1) \pmod{3} \quad \text{ja} \quad P(10) \equiv P(1) \pmod{9}.$$

Tästä tietenkin seuraa, että

> *jokainen positiivinen kokonaisluku on kongruentti numeroidensa summan kanssa modulo kolme ja modulo yhdeksän.*

Erityisesti siis luku on jaollinen kolmella (yhdeksällä) täsmälleen silloin kun sen numeroiden summa on jaollinen kolmella (yhdeksällä).

Kongruenssien hyödyntäminen Diofantoksen yhtälöissä

Kongruenssiaritmetiikkaa voidaan hyödyntää Diofantoksen yhtälöiden tarkastelussa. Seuraavat esimerkit näyttävät yksinkertaisimman sovellutuksen.

Esimerkki. Etsi Diofantoksen yhtälön

$$x^2 + y^2 = 10000003$$

kokonaislukuratkaisut.

Koska

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 0, \quad \text{ja} \quad 3^2 \equiv 1 \qquad (\text{mod } 4),$$

on jokainen neliöluku kongruentti toisen luvuista 0 ja 1 modulo 4. Siis kahden neliön summa on aina kongruentti 0, 1 tai 2 modulo 4. Mutta tarkasteltavan yhtälön oikea puoli on $\equiv 3 \pmod 4$. Kysyttyjä kokonaislukuratkaisuita ei siis ole.

Esimerkki. Etsi Diofantoksen yhtälön

$$x_1^4 + x_2^4 + \ldots + x_{14}^4 = 15999999999$$

kokonaislukuratkaisu.

Tällä kertaa osoittautuu, että kokonaisluvun neljäs potenssi on aina kongruentti luvun 0 tai 1 kanssa modulo 16. Siispä vasen puoli on aina kongruentti jonkin luvuista 0, 1, 2, ..., 14 kanssa modulo 16, kun taas oikea puoli on $\equiv 15 \pmod{16}$.

Eulerin φ-funktio

Olkoon $m \in \mathbb{Z}_+$. Merkitsemme $\varphi(m)$ niiden luvuista

$$1, \quad 2, \quad 3, \quad \ldots, \quad m,$$

jotka ovat yhteistekijättömiä luvun m kanssa, lukumäärää.

Esimerkkejä. Luvuista 1 jokaisen yhteinen tekijä luvun 1 kanssa on 1, ja siispä

$$\varphi(1) = 1.$$

Luvuista 1, ..., 6 luvun 6 kanssa yhteistekijättömiä ovat täsmälleen 1 ja 5, eli

$$\varphi(6) = 2.$$

Samassa hengessä luvuista 1, ..., 10 luvun 10 kanssa yhteistekijättömiä ovat täsmälleen 1, 3, 7 ja 9, eli on

$$\varphi(10) = 4.$$

Lisäesimerkkejä. Olkoon p alkuluku. Nyt luvuista 1, 2, ..., p yhteistekijättömiä luvun p kanssa ovat kaikki luvut 1, 2, ..., $p-1$, eli

$$\varphi(p) = p - 1.$$

Viimeisenä esimerkkinä, jos $\alpha \in \mathbb{Z}_+$, niin luvuista 1, 2, ..., p^α yhteistekijättömiä luvun p^α kanssa ovat täsmälleen ne luvut, jotka ovat yhteistekijättömiä alkuluvun p kanssa, eli alkuluvulla p jaottomat luvut. Täten

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \cdot \frac{p-1}{p}.$$

Eulerin φ-funktiolla on sama kätevä multiplikatiivisuusominaisuus kuin funktioilla $d(\cdot)$ ja $\sigma(\cdot)$:

Lause. *Olkoon m ja n keskenään yhteistekijättömiä positiivisia kokonaislukuja. Tällöin*

$$\varphi(mn) = \varphi(m)\,\varphi(n)\,.$$

Todistamme tämän kirjoittamalla luvut 1, 2, …, mn seuraavanlaisen taulukon muotoon:

$$\begin{array}{cccc} 1 & 2 & 3 & \cdots & n \\ n+1 & n+2 & n+3 & \cdots & 2n \\ 2n+1 & 2n+2 & 2n+3 & \cdots & 3n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (m-1)\,n+1 & (m-1)\,n+2 & (m-1)\,n+3 & \cdots & mn \end{array}$$

Tässä taulukossa on funktion $\varphi(\cdot)$ määritelmän nojalla täsmälleen $\varphi(mn)$ lukua, jotka ovat yhteistekijättömiä luvun mn kanssa. Toisaalta, koska luku on yhteistekijätön luvun mn kanssa jos ja vain jos se on yhteistekijätön molempien luvuista m ja n manssa erikseen, voimme laskea kyseiset $\varphi(mn)$ toisellakin tavalla.

Koska taulukossa yhdessä sarakkeessa olevat luvut ovat keskenään kongruentteja modulo n, taulukossa olevat luvun n kanssa yhteistekijättömät luvut muodostavat täsmälleen $\varphi(n)$ kokonaista saraketta. Edellä mainitut $\varphi(mn)$ sijaitsevat siis näissä sarakkeissa.

Tarkastellaan sitten yhtä näistä $\varphi(n)$ sarakkeesta. Koska $(m, n) = 1$, sen luvut ovat m keskenään epäkongruenttia lukua modulo m. Siis niistä täsmälleen $\varphi(m)$ ovat yhteistekijättömiä, paitsi luvun n kanssa, myös luvun m kanssa, ja olemme valmiit.

Kenties todistuksen luonnetta selvittää, jos näkee kyseisen taulukon rivit jossakin erikoistapauksessa. Valitaan $n = 12$ ja $m = 7$. Tällöin kyseinen taulukko näyttää seuraavalta:

1	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	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84

Näistä luvun 12 kanssa yhteistekijättömiä ovat seuraavat:

1	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	**41**	42	**43**	44	45	46	**47**	48
49	50	51	52	**53**	54	**55**	56	57	58	**59**	60
61	62	63	64	**65**	66	**67**	68	69	70	**71**	72
73	74	75	76	**77**	78	**79**	80	81	82	**83**	84

ja lukujen 12 ja 7 kanssa yhteistekijättömiä ovat:

1	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	**41**	42	**43**	44	45	46	**47**	48
49	50	51	52	**53**	54	**55**	56	57	58	**59**	60
61	62	63	64	**65**	66	**67**	68	69	70	**71**	72
73	74	75	76	77	78	**79**	80	81	82	**83**	84

Korollaari. *Olkoon luvun $n \in \mathbb{Z}_+ \setminus \{1\}$ kanoninen alkutekijähajotelma*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\nu^{\alpha_\nu}.$$

Tällöin

$$\varphi(n) = n \cdot \frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdot \ldots \cdot \ldots \cdot \frac{p_\nu - 1}{p_\nu}.$$

Esimerkki. Olemme jo aiemmin todenneet, että $360 = 2^3 \cdot 3^2 \cdot 5$. Käyttämällä yllä johdettua kaavaa näemme, että

$$\varphi(360) = 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 2^2 \cdot 3 \cdot 2 \cdot 4 = 96.$$

Eulerin lause

Eulerin φ-funktion esittelymme liittyy lähinnä siihen seikkaan, että ilmenee, että monet kertolaskuun modulo alkuluku liittyvät seikat yleistyvät siististi myös muille moduluksille kunhan rajoittuu kertomaan vain lukuja jotka ovat moduluksen suhteen yhteistekijättömiä. Esimerkkinä näytämme tästä Fermat'n pienen lauseen yleistyksen yhdistetyille moduluksille. Lukijan on hyvä verrata tätä ensimmäiseen Fermat'n pienen lauseen todistukseemme; todistus on oleellisesti ottaen sama.

Eulerin lause. *Olkoon $m \in \mathbb{Z}_+$ ja olkoon $a \in \mathbb{Z}$ yhteistekijätön luvun m kanssa. Tällöin*

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

Olkoot luvuista 1, 2, ..., m luvun m kanssa yhteistekijättömät

$$1 = r_1 < r_2 < r_3 < \ldots < r_{\varphi(m)} = m - 1.$$

Luvuista

$$r_1 a, \quad r_2 a, \quad r_3 a, \quad \ldots, \quad r_{\varphi(m)} a$$

mitkä tahansa kaksi ovat keskenään epäkongruentteja modulo m, sillä jos $r_k a \equiv r_\ell a \pmod{m}$ joillakin $k, l \in \{1, 2, \ldots, \varphi(m)\}$, niin varmasti $r_k \equiv r_\ell \pmod{m}$, ja koska luvut r_k ja r_ℓ ovat väliltä $[1, m]$ seuraa tästä, että $r_k = r_\ell$ ja $k = \ell$. Lisäksi kyseiset $\varphi(m)$ luvun a monikertaa ovat kaikki yhteistekijättömiä luvun m kanssa. Siispä jokainen niistä on kongruentti täsmälleen yhden luvuista 1, 2, ..., m kanssa modulo m, ja kääntäen.

Nyt varmasti

$$r_1 a \cdot r_2 a \cdot \ldots \cdot r_{\varphi(m)} a \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m},$$

eli

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m},$$

eli

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

mikä oli todistettava.

Kotitehtäviä

17. Olkoot a ja b kokonaislukuja. Osoita, että kaikilla alkuluvuilla p pätee $(a+b)^p \equiv a^p + b^p \pmod{p}$.

18. Osoita, että seuraava seitsemällä jaollisuussääntö toimii. Olkoon $n \in \mathbb{Z}_+$ vähintään kolminumeroinen. Jos luvun n viimeinen numero on d, niin lasketaan $m = \frac{n-d}{10} - 2d$. Tällöin $7 \mid n$ jos ja vain jos $7 \mid m$.

19. Osoita, ettei luku $385^{1980} + 18^{1980}$ ole neliöluku. [Vihje: 13.]

20. Osoita, että viiden peräkkäisen neliöluvun summa ei ole neliöluku.

21. Osoita, ettei Diofantoksen yhtälöllä

$$x^3 + y^4 = 7$$

ole kokonaislukuratkaisuita.

22. Osoita, ettei löydy lukua $n \in \mathbb{Z}_+$ jolle olisi $\varphi(n) = 14$.

23. Olkoon $n \in \mathbb{Z}_+$. Mikä on niiden positiivisten kokonaislukujen s summa, joille $(s, n) = 1$?

24. Osoita, että löytyy äärettömän monta positiivista kokonaislukua n siten, että $\varphi(n) = \frac{n}{3}$.

Luku 4

Primitiiviset juuret

Olkoon p jokin pariton alkuluku, sanokaamme luku seitsemän. Tunnemme jo monia hyviä ominaisuuksia kertolaskulle modulo p, mutta silti ei ole lainkaan selvää, miten monimutkaisia vaikkapa kertolaskutaulut ovat modulo p. Esimerkiksi kertolasku modulo 7 näyttää tältä:

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Ei näytä hirveän valaisevalta, eihän? Mutta jos järjestelemme luvut 1, 2, 3, 4, 5 ja 6 järjestykseen 1, 3, 2, 6, 4, 5, niin kertolaskutaulu näyttääkin tältä:

$\cdot$	1	3	2	6	4	5
1	1	3	2	6	4	5
3	3	2	6	4	5	1
2	2	6	4	5	1	3
6	6	4	5	1	3	2
4	4	5	1	3	2	6
5	5	1	3	2	6	4

Mutta verrattaessa tätä yhteenlaskutauluun modulo 6:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

huomataan, että ne ovat samat merkintöjä vaille! Kertolasku modulo 7 ei ole siis yhtään vaikeampaa tai monimutkaisempaa kuin yhteenlasku modulo 6, ja lisäksi kaikki nollasta poikkeavat jäännösluokat modulo 7 ovat kiinteän luvun, eli tässä luvun kolme, potensseja.

Tulemme tässä luvussa todistamaan, että jokaiselle alkuluvulle p löytyy *primitiivinen juuri*, luku jonka potensseina kaikki kääntyvät jäännösluokat voidaan esittää, ja siis myös että kertolasku modulo p on täsmälleen yhtä monimutkainen laskutoimitus kuin primitiivisten juurten eksponenttien yhteenlasku modulo $p-1$.

Lagrangen lause

Tulemme tarvitsemaan useampaan kertaan seuraavaa perustulosta, joka oikeastaan jatkaa kolmannella oppitunnilla esitettyä vastaavuutta kongruenssiaritmetiikan, varsinkin modulo alkuluku, ja rationaali- ja reaalilukujen kuntien välillä.

Lagrangen lause. *Olkoon p alkuluku ja olkoon $P(x)$ kokonaislukukertoiminen polynomi astetta $n \in \mathbb{Z}_+$, jonka korkeimman asteen termin kerroin ei ole jaollinen luvulla p. Tällöin kongruenssilla $P(x) \equiv 0 \pmod{p}$ on enintään n ratkaisua modulo p.*

Tässä siis keskenään kongruentit kokonaislukuratkaisut samaistetaan keskenään, tai vaihtoehtoisesti tarkastellaan vain jäännösluokkia.

Todistuksen ajatuksena on yksinkertaisesti käyttää induktiota asteen n suhteen. Tapaus $n = 1$ on selvä; ensimmäisen asteen kongruensseja ymmärrämme jo riittävän hyvin. Olettakaamme siis, että $n > 1$, ja että väite on jo todistettu polynomeille, jotka ovat enintään astetta $n-1$. Tämä tarkoittaa sitä, että jos $Q(x)$ on enintään astetta $n-1$ oleva kokonaislukukertoiminen polynomi, jolle kongruenssilla $Q(x) \equiv 0 \pmod{p}$ on enemmän kuin $\deg Q(x)$ ratkaisua modulo p, niin itse asiassa $p \mid Q(x)$ kaikilla $x \in \mathbb{Z}$.

Tarkastellaan astetta n olevaa kokonaislukukertoimista polynomia $P(x)$, jonka korkeimman asteen termin kerroin ei ole jaollinen luvulla p. Ilman yleisyyden menettämistä voimme olettaa, että se on yhtä kuin yksi. Jos kongruenssilla $P(x) \equiv 0 \pmod{p}$ on vähemmän kuin n pareittain epäkongruenttia ratkaisua, mitään todistettavaa ei ole. Oletetaan siis, että sillä on vähintään n ratkaisua. Olkoot jotkin n kappaletta niistä $x_1, x_2, \ldots, x_n$.

Nyt kongruenssilla

$$P(x) - (x - x_1)(x - x_2)\cdots(x - x_n) \equiv 0 \pmod{p}$$

on n keskenään epäkongruenttia ratkaisua modulo p, mutta sen vasemman puolen aste on aidosti pienempi kuin n. Siispä induktio-oletuksen nojalla

$$P(x) \equiv (x - x_1)(x - x_2)\cdots(x - x_n) \pmod{p}$$

jokaisella $x \in \mathbb{Z}$, ja selvästi kongruenssilla $P(x) \equiv 0 \pmod{p}$ on oltava täsmälleen n keskenään epäkongruenttia ratkaisua modulo p, ja olemme valmiit.

Pieni aputulos

Lemma. *Olkoon $n \in \mathbb{Z}_+$. Tällöin*

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

Jos $n = 1$, väite on varsin helppo tarkistaa. Oletetaan siis, että $n > 1$, ja kirjoitetaan luvun n kanoninen alkutekijähajotelma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots \alpha_\nu^{\alpha_\nu}.$$

Nyt voimme käyttää edellisessä luvussa todistamiamme φ-funktion ominaisuuksia ja päätellä seuraavasti:

$$\begin{aligned}
\sum_{d|n} \varphi(d) &= \sum_{p_1^{\beta_1}\cdots p_\nu^{\beta_\nu} | p_1^{\alpha_1}\cdots p_\nu^{\alpha_\nu}} \varphi\big(p_1^{\beta_1}\cdots p_\nu^{\beta_\nu}\big) = \sum_{p_1^{\beta_1}\cdots p_\nu^{\beta_\nu} | p_1^{\alpha_1}\cdots p_\nu^{\alpha_\nu}} \varphi\big(p_1^{\beta_1}\big)\cdots\varphi\big(p_\nu^{\beta_\nu}\big) \\
&= \big(\varphi(p_1^{\alpha_1}) + \varphi\big(p_1^{\alpha_1-1}\big) + \ldots + \varphi\big(p_1^2\big) + \varphi(p_1) + \varphi(1)\big) \\
&\quad \ldots\ldots\ldots\ldots\ldots\ldots \\
&\qquad \big(\varphi(p_\nu^{\alpha_\nu}) + \varphi\big(p_\nu^{\alpha_\nu-1}\big) + \ldots + \varphi\big(p_\nu^2\big) + \varphi(p_\nu) + \varphi(1)\big) \\
&= \big(p_1^{\alpha_1} - p_1^{\alpha_1-1} + p_1^{\alpha_1-1} - p_1^{\alpha_1-2} + \ldots + p_1^2 - p_1 + p_1 - 1 + 1\big) \\
&\quad \ldots\ldots\ldots\ldots\ldots\ldots \\
&\qquad \big(p_\nu^{\alpha_\nu} - p_\nu^{\alpha_\nu-1} + p_\nu^{\alpha_\nu-1} - p_\nu^{\alpha_\nu-2} + \ldots + p_\nu^2 - p_\nu + p_\nu - 1 + 1\big) \\
&= p_1^{\alpha_1}\cdots p_\nu^{\alpha_\nu} = n.
\end{aligned}$$

Eksponentit

Olkoon p pariton alkuluku ja olkoon a luvulla p jaoton kokonaisluku. Tällöin määrittelemme luvun

$$\operatorname{ord}_p a \stackrel{\text{def}}{=} \min\left\{ d \in \mathbb{Z}_+ \,\middle|\, a^d \equiv 1 \pmod p \right\}.$$

Fermat'n pienen lauseen nojalla $\operatorname{ord}_p a$ on hyvin määritelty ja vieläpä $\operatorname{ord}_p a \leqslant p-1$. Sanomme, että *$a$ kuuluu eksponenttiin* $\operatorname{ord}_p a$ modulo p.

Vaikka tämä käsite onkin sinänsä mielenkiintoinen ja selventävä (kuten tulemme näkemään), oppitunnin tavoitteen muistaen lukijan on hyvä pitää mielessä, että a on primitiivinen juuri modulo p jos ja vain jos se kuuluu eksponenttiin $p-1$ modulo p.

Ensimmäinen havainto. *Jos* $a^d \equiv 1 \pmod p$, *niin* $\operatorname{ord}_p a \,|\, d$. *Erityisesti* $\operatorname{ord}_p a \,|\, (p-1)$.

Nimittäin, jos olisi $\operatorname{ord}_p a \nmid d$, niin löytyisi luvut $q \in \mathbb{Z}$ ja $r \in \mathbb{Z}$, joille $d = q \operatorname{ord}_p a + r$ ja $0 < r < \operatorname{ord}_p a$, ja tällöin tietenkin olisi

$$a^r \equiv a^{q \operatorname{ord}_p a + r} \equiv a^d \equiv 1 \pmod p,$$

vastoin luvun $\operatorname{ord}_p a$ määritelmää.

Toinen havainto. *Olkoot* $d, e \in \mathbb{Z}_+$. *Tällöin* $a^d \equiv a^e \pmod p$ *jos ja vain jos* $d \equiv e \pmod{\operatorname{ord}_p a}$.

Nimittäin, jos vaikkapa $d \equiv e \pmod{\operatorname{ord}_p a}$ ja $d > e$, niin $d = e + q \operatorname{ord}_p a$ jollakin $q \in \mathbb{Z}_+$, jolloinka tietysti

$$a^d \equiv a^{d + q \operatorname{ord}_p a} \equiv a^e \pmod p,$$

ja toisaalta, jos $a^d \equiv a^e \pmod p$, ja vaikkapa $d > e$, niin $a^{d-e} \equiv 1 \pmod p$, jolloinka tietysti $\operatorname{ord}_p a \,|\, (d-e)$.

Kolmas havainto. *Olkoon $d \in \mathbb{Z}_+$. Tällöin a^d kuuluu eksponenttiin $\frac{\operatorname{ord}_p a}{(d,\operatorname{ord}_p a)}$ modulo p.*

Nimittäin varmasti

$$\left(a^d\right)^{\frac{\operatorname{ord}_p a}{(d,\operatorname{ord}_p a)}} \equiv \left(a^{\operatorname{ord}_p a}\right)^{\frac{d}{(d,\operatorname{ord}_p a)}} \equiv 1 \pmod{p},$$

ja toisaalta $\operatorname{ord}_p a \mid d \operatorname{ord}_p a^d$, eli

$$\frac{\operatorname{ord}_p a}{(d,\operatorname{ord}_p a)} \mid \operatorname{ord}_p a, \quad \text{eli} \quad \operatorname{ord}_p a^d \geqslant \frac{\operatorname{ord}_p a}{(d,\operatorname{ord}_p a)}.$$

Neljäs havainto. *Olkoon $d \mid (p-1)$. Tällöin eksponenttiin d kuuluu joko nolla tai $\varphi(d)$ jäännösluokkaa modulo p.*

Jos eksponenttiin d kuuluvia lukuja ei ole, niin myöskään mitään todistettavaa ei ole. Oletetaan siis, että jokin $a \in \mathbb{Z}$, jolle $p \nmid a$, kuuluu eksponenttiin d modulo p. Tällöin luvut

$$1, \quad a, \quad a^2, \quad \ldots, \quad a^{d-1}$$

ovat d keskenään epäkongruenttia kongruenssin $x^d \equiv 1 \pmod{p}$ ratkaisua, Lagrangen lauseen nojalla muita ratkaisuita ei ole, ja kolmannen havainnon nojalla näistä ratkaisuista eksponenttiin d kuuluvat täsmälleen ne potenssit a^e, $e \in \{1, 2, \ldots, d\}$, joille $(d, e) = 1$. Viimeksi mainittuja on tasan $\varphi(d)$ kappaletta.

——— : ———

Näiden havaintojen jälkeen pääsemme vihdoin asian ytimeen:

Lause. *Olkoon p pariton alkuluku ja olkoon $d \mid (p-1)$. Tällöin eksponenttiin d kuuluu täsmälleen $\varphi(d)$ jäännösluokkaa modulo p.*

Kuulukoot eksponenttiin d täsmälleen $\psi(d)$ jäännösluokkaa modulo p. Tällöin

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

ja tässä voi päteä yhtäsuuruus vain jos $\psi(d) = \varphi(d)$ kaikilla $d \mid (p-1)$. Q.E.D.

Korollari. *Jos p on pariton alkuluku, niin on olemassa täsmälleen $\varphi(p-1)$ primitiivistä juurta modulo p.*

Kotitehtäviä

25. Mitkä ovat primitiiviset juuret **a)** modulo viisi; **b)** modulo 11; **c)** modulo 43?

26. Mitkä luvut kuuluvat **a)** eksponenttiin 6 modulo 43; **b)** eksponenttiin 21 modulo 43?

27. Osoita, että $n \mid \varphi(2^n - 1)$ kaikilla $n \in \mathbb{Z}_+$.

28. Olkoon p pariton alkuluku ja r primitiivinen juuri modulo p. Osoita, että löytyy primitiivinen juuri r' modulo p siten, että $rr' \equiv 1 \pmod{p}$.

29. Olkoon p pariton alkuluku. Johda kongruenssi $(p-1)! \equiv -1 \pmod{p}$ suoraan siitä tiedosta lähtien, että löytyy primitiivisiä juuria modulo p.

30. Olkoon p pariton alkuluku, jolle $p \equiv 1 \pmod{4}$. Osoita kongruenssin $x^2 \equiv -1 \pmod{p}$ ratkeavuus suoraan siitä tiedosta, että löytyy primitiivisiä juuria modulo p.

31. Olkoon p pariton alkuluku ja $n \in \mathbb{Z}_+$. Mitä on summa

$$1^n + 2^n + 3^n + \ldots + (p-1)^n$$

modulo p?

32. Olkoon p pariton alkuluku. Olkoon r_1, r_2, $\ldots$, $r_{\varphi(p-1)}$ keskenään epäkongruentteja primitiivisiä juuria modulo p. Mitä on tulo $r_1 r_2 \cdots r_{p-1}$ modulo p?

Luku 5

Neliönjäännökset

Tässä luvussa esitämme neliönjäännösten kauniin teorian perusteet. Olkoon p pariton alkuluku. Kokonaisluku a on *neliönjäännös modulo* p, jos $p \nmid a$ ja $x^2 \equiv a \pmod{p}$ jollakin $x \in \mathbb{Z}$. Jos $p \nmid a$ ja a ei ole neliönjäännös modulo p, sanomme, että a on *neliönepäjäännös modulo* p. Luvulla p jaolliset luvut eivät ole neliönjäännöksiä eivätkä neliönjäännöksiä modulo p.

Esimerkkejä. Koska $1^2 \equiv 2^2 \equiv 1 \pmod{3}$, on luku yksi ainoa neliönjäännös, ja luku kaksi ainoa neliönepäjäännös modulo kolme.

Koska $1^2 \equiv 4^2 \equiv 1$ ja $2^2 \equiv 3^2 \equiv 4 \pmod{5}$, ovat 1 ja 4 neliönjäännökset modulo 5, ja 2 ja 3 vastaavasti neliönepäjäännökset.

Samassa hengessä neliönjäännökset modulo 7 ovat $1^1 \equiv 1$, $2^2 \equiv 4$ sekä $3^2 \equiv 2$, ja neliönepäjäännökset 3, 5 ja 6.

Aloitamme seuraavalla yksinkertaisella havainnolla:

Havainto. *Neliönjäännöksiä on yhtä monta kuin neliönepäjäännöksiä modulo p, nimittäin $\frac{p-1}{2}$ kappaletta.*

Tämä seuraa siitä, että lukujen $1^2, 2^2, \ldots, (p-1)^2$ joukossa on enintään $\frac{p-1}{2}$ keskenään epäkongruenttia neliötä, koska $x^2 \equiv (-x)^2 \pmod{p}$ kaikilla $x \in \mathbb{Z}$. Toisaalta, kongruenssilla $x^2 \equiv a \pmod{p}$ on enintään kaksi ratkaisua (ja siis tietysti täsmälleen kaksi ratkaisua) modulo p jokaisella neliönjäännöksellä a.

Neliönjäännösten teorian päätulokset on helpointa esittää niin sanotun *Legendren symbolin* avulla. Se määritellään seuraavasti: Kaikilla parittomilla alkuluvuilla p ja kokonaisluvuilla a asetamme

$$\left(\frac{a}{p}\right)_{\mathscr{L}} = \begin{cases} 1, & \text{jos } a \text{ on neliönjäännös modulo } p, \\ -1, & \text{jos } a \text{ on neliönepäjäännös modulo } p, \\ 0 & \text{muutoin.} \end{cases}$$

Esimerkkejä. Edellisessä esimerkissä tehtyjen laskujen nojalla

$$\left(\frac{1}{3}\right)_{\mathscr{L}} = 1, \quad \left(\frac{3}{5}\right)_{\mathscr{L}} = -1, \quad \text{ja} \quad \left(\frac{2}{7}\right)_{\mathscr{L}} = 1.$$

Jos kokonaisluvuilla a ja b pätee $a \equiv b \pmod{p}$, niin tietysti

$$\left(\frac{a}{p}\right)_{\mathscr{L}} = \left(\frac{b}{p}\right)_{\mathscr{L}}.$$

Eulerin kriteeri ja neliönjäännösten resiprookkilain ensimmäinen täydennyslause

Legendren symbolin $\left(\frac{a}{p}\right)_{\mathscr{L}}$ voi kätevästi esittää luvun a potenssina modulo p:

Eulerin kriteeri. *Olkoon p pariton alkuluku ja olkoon $a \in \mathbb{Z}$. Tällöin*

$$\left(\frac{a}{p}\right)_{\mathscr{L}} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Jos $p \mid a$, niin asia on selvä. Oletetaan siis, että $p \nmid a$. Tällöin Fermat'n pienen lauseen nojalla $a^{p-1} \equiv 1 \pmod{p}$, eli $a^{\frac{p-1}{2}} \equiv 1$ tai $-1 \pmod{p}$. Jokainen neliönjäännös, joita on siis $\frac{p-1}{2}$ kappaletta, on kongruenssin $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, ratkaisu, sillä jos a on neliönjäännös modulo p, niin $a \equiv y^2 \pmod{p}$ jollakin $y \in \mathbb{Z}$,

$$a^{\frac{p-1}{2}} \equiv \left(y^2\right)^{\frac{p-1}{2}} \equiv y^{p-1} \equiv 1 \pmod{p}.$$

Toisaalta, Lagrangen lauseen nojalla kongruenssilla $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ei voi olla enempää kuin $\frac{p-1}{2}$ ratkaisua, ja siten neliönepäjäännökselle a modulo p on pädettävä $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Eulerin kriteeristä saamme välittömästi seuraavat hyödylliset tulokset:

Korollaari. *Olkoot a ja b kokonaislukuja, ja olkoon p pariton alkuluku. Tällöin*

$$\left(\frac{a}{p}\right)_{\mathscr{L}} \left(\frac{b}{p}\right)_{\mathscr{L}} = \left(\frac{ab}{p}\right)_{\mathscr{L}}.$$

Neliönjäännösten resiprookkilain ensimmäinen täydennyslause. *Olkoon p pariton alkuluku. Tällöin*

$$\left(\frac{-1}{p}\right)_{\mathscr{L}} = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{jos } p \equiv 1 \pmod{4}, \text{ ja} \\ -1, & \text{jos } p \equiv -1 \pmod{4}. \end{cases}$$

Gaussin lemma ja neliönjäännösten resiprookkilain toinen täydennyslause

Gaussin lemma. *Olkoon p pariton alkuluku ja olkoon a luvulla p jaoton kokonaisluku. Olkoon lisäksi lukujen*

$$a, \quad 2a, \quad 3a, \quad \ldots, \quad \frac{p-1}{2}a$$

itseisesti pienimpien jäännösten joukossa $s \in \mathbb{Z}_+$ negatiivista. Tällöin

$$a^{\frac{p-1}{2}} \equiv (-1)^s \pmod{p}.$$

Todistuksen idea on sama kuin ensimmäisessä Fermat'n pienen lauseen todistuksessamme. Ilmenee, että lukujen a, $2a$, $\ldots$, $\frac{p-1}{2}a$ itseisesti pienimpien jäännösten itseisarvoista jokainen on kongruentti täsmälleen yhden luvuista 1, 2, $\ldots$, $\frac{p-1}{2}$ kanssa, ja kääntäen.

Nimittäin, jos $ak \equiv a\ell \pmod{p}$ joillakin $k, \ell \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, niin varmasti $k \equiv \ell \pmod{p}$ ja siis $k = \ell$. Jos taas olisi $ak \equiv a\ell \pmod{p}$, niin olisi $p \mid (k + \ell)$, mikä on mahdotonta, sillä $0 < k + \ell < p$.

On siis oltava

$$a \cdot 2a \cdot \ldots \cdot \frac{p-1}{2}a \equiv (-1)^s \cdot 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \pmod{p},$$

eli

$$a^{\frac{p-1}{2}} \cdot \frac{p-1}{2}! \equiv (-1)^s \cdot \frac{p-1}{2}! \pmod{p},$$

ja on oltava $a^{\frac{p-1}{2}} \equiv (-1)^s \pmod{p}$. q.e.d.

Neliönjäännösten resiprookkilauseen toinen täydennyslause. *Olkoon p pariton alkuluku. Tällöin*

$$\left(\frac{2}{p}\right)_{\mathscr{L}} = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \Longleftarrow p \equiv \pm 1 \pmod{8}, \\ -1 \Longleftarrow p \equiv \pm 3 \pmod{8}. \end{cases}$$

Eulerin kriteerin ja Gaussin lemman nojalla

$$\left(\frac{2}{p}\right)_{\mathscr{L}} \equiv 2^{\frac{p-1}{2}} \equiv (-1)^s \pmod{p}, \quad \text{eli} \quad \left(\frac{2}{p}\right)_{\mathscr{L}} = (-1)^s,$$

missä s on lukujen $2, 4, \ldots, p-1$ itseisesti pienimmistä jäännöksistä negatiivisten lukumäärä.

Meitä kiinnostaa vain luvun s parillisuus. Olkoon $t = \frac{p-1}{2} - s$ lukujen 2, 4, $\ldots$, $p - 1$ itseisesti positiivisten jäännösten määrä. Itseisesti positiivisia jäännöksiä kyseessä olevista luvuista on vain niillä, jotka ovat pienempiä kuin $\frac{p}{2}$.

Jos $p \equiv 1 \pmod{4}$, eli $p \equiv 1$ tai $5 \pmod{8}$, niin luku $\frac{p-1}{2}$ on parillinen ja

$$\left(\frac{2}{p}\right)_{\mathscr{L}} = (-1)^t.$$

Nyt lukua $\frac{p}{2}$ pienempiä luvun 2 monikertoja ovat

$$2, \quad 4, \quad 6, \quad \ldots, \quad \frac{p-1}{2},$$

eli $t = \frac{p-1}{4}$. Tapauksessa $p \equiv 1 \pmod{4}$ on siis

$$\left(\frac{2}{p}\right)_{\mathscr{L}} = \begin{cases} 1, & \text{jos } p \equiv 1 \pmod{8}, \text{ ja} \\ -1, & \text{jos } p \equiv 5 \pmod{8}. \end{cases}$$

Olkoon sitten $p \equiv 3 \pmod{4}$, eli $p \equiv 3$ tai $7 \pmod{8}$. Tässä tapauksessa luku $\frac{p-1}{2}$ on pariton, $\left(\frac{2}{p}\right)_{\mathscr{L}} = -(-1)^t$, ja lukua $\frac{p}{2}$ pienemmät luvun 2 monikerrat ovat

$$2, \quad 4, \quad 6, \quad \ldots, \quad \frac{p-3}{2}.$$

Täten $t = \frac{p-3}{4}$, ja tapauksessa $p \equiv 3 \pmod 4$ on oltava

$$\left(\frac{2}{p}\right)_{\mathscr{L}} = \begin{cases} -1, & \text{jos } p \equiv 3 \pmod 8, \text{ ja} \\ 1, & \text{jos } p \equiv 7 \pmod 8, \end{cases}$$

ja olemme valmiit.

Neliönjäännösten resiprookkilaki

Neliönjäännösten resiprookkilaki. *Olkoot p ja q kaksi eri paritonta alkulukua. Tällöin*

$$\left(\frac{p}{q}\right)_{\mathscr{L}} \left(\frac{q}{p}\right)_{\mathscr{L}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Toisin sanoen,

$$\left(\frac{p}{q}\right)_{\mathscr{L}} = \begin{cases} -\left(\frac{q}{p}\right)_{\mathscr{L}}, & \text{jos } p \equiv q \equiv 3 \pmod 4, \text{ ja} \\ \left(\frac{q}{p}\right)_{\mathscr{L}} & \text{muutoin.} \end{cases}$$

Todistus. Gaussin lemman nojalla

$$\left(\frac{p}{q}\right)_{\mathscr{L}} = (-1)^s \quad \text{ja} \quad \left(\frac{q}{p}\right)_{\mathscr{L}} = (-1)^t,$$

missä s on lukujen p, $2p$, …, $\frac{q-1}{2}p$ itseisesti pienimmistä jäännöksistä modulo q negatiivisten lukumäärä, ja t on lukujen q, $2q$, …, $\frac{p-1}{2}q$ itseisesti pienimmistä jäännöksistä modulo p negatiivisten lukumäärä. On siis osoitettava, että

$$s + t \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2.$$

Tätä tarkoitusta varten tarkastelemme niitä $\frac{p-1}{2} \cdot \frac{q-1}{2}$ lauseketta, jotka ovat muotoa $ap - bq$ joillakin $a \in \left\{1, 2, \ldots, \frac{q-1}{2}\right\}$ ja $b \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. Näistä välille $\left]-\frac{q}{2}, 0\right[$ kuuluu täsmälleen s kappaletta, ja välille $\left]0, \frac{p}{2}\right[$ kuuluu täsmälleen t kappaletta. Riittää siis osoittaa, että väleille $\left]-\infty, -\frac{q}{2}\right[$ ja $\left]\frac{p}{2}, \infty\right[$ kuuluu yhteensä täsmälleen parillinen määrä arvoja.

Viimeksi mainittu tavoite saavutetaan yksinkertaisesti osoittamalla, että välille $\left]-\infty, -\frac{q}{2}\right[$ kuuluu yhtä monta arvoa kuin välille $\left]\frac{p}{2}, \infty\right[$. Tämä on helppo nähdä. Nimittäin, jos $ap - bq < -\frac{q}{2}$, niin

$$\begin{aligned}\left(\frac{q+1}{2} - a\right)p - \left(\frac{p+1}{2} - b\right)q &= \frac{q+1}{2} \cdot p - \frac{p+1}{2} \cdot q - (ap - bq) \\ &> \frac{pq + p - pq - q}{2} + \frac{q}{2} = \frac{p}{2},\end{aligned}$$

ja toisaalta, jos $ap - bq > \frac{p}{2}$, niin

$$\begin{aligned}\left(\frac{q+1}{2} - a\right)p - \left(\frac{p+1}{2} - b\right)q &= \frac{q+1}{2} \cdot p - \frac{p+1}{2} \cdot q - (ap - bq) \\ &< \frac{pq + p - pq - q}{2} - \frac{p}{2} = -\frac{q}{2},\end{aligned}$$

ja neliönjäännösten resiprookkilaki on todistettu.

Kotitehtäviä

33. Laske Legendren symbolit $\left(\frac{-1}{5}\right)_{\mathscr{L}}$, $\left(\frac{2}{13}\right)_{\mathscr{L}}$, $\left(\frac{73}{83}\right)_{\mathscr{L}}$, $\left(\frac{371}{1367}\right)_{\mathscr{L}}$, ja $\left(\frac{682}{911}\right)_{\mathscr{L}}$.

34. Ratkaise toisen asteen kongruenssit
a) $4x^2 + 6x - 3 \equiv 0 \pmod{43}$.
b) $7x^2 - 8x + 5 \equiv 0 \pmod{19}$.
c) $x^2 + 12x + 5 \equiv 0 \pmod{73}$.

35. Olkoon p sellainen alkuluku, että $p \equiv 1 \pmod 4$. Todista, että peräkkäisten lukujen $1, 2, \ldots, \frac{p-1}{2}$ joukossa on yhtä monta neliönjäännostä kuin lukujen $\frac{p+1}{2}$, $\frac{p+3}{2}, \ldots, p-1$ joukossa. Toisin sanoen: osoita, että itseisesti positiivisia neliönjäännöksiä modulo p on yhtä monta kuin itseisesti negatiivisia neliönjäännöksiä modulo p.

36. Olkoon p pariton alkuluku. Laske Legendren symboli $\left(\frac{5}{p}\right)_{\mathscr{L}}$.

37. Osoita, että on äärettömän monta alkulukua p, joille
a) $p \equiv 3 \pmod 4$;
b) $p \equiv 1 \pmod 4$.

38. Olkoon p pariton alkuluku ja r primitiivinen juuri modulo p. **a)** Osoita, että r on neliönepäjäännös modulo p. **b)** Osoita, että neliönjäännös modulo p on muotoa r^{2k} modulo p jollakin $k \in \mathbb{Z}_+$.

39. Osoita, ettei 30 peräkkäistä kokonaislukua voi jakaa kahteen joukkoon siten, että joukkojen sisältämien lukujen tulot olisivat yhtä suuret.

40. Ratkaise Diofantoksen yhtälö

$$y^2 = x^3 + 23$$

kokonaislukujen joukossa.

Luku 6

Kiinalainen jäännöslause, neliöiden summat

Eksponentit muiden kuin alkulukumodulusten suhteen

Olkoon $m \in \mathbb{Z}_+$, oletetaan, että $m > 1$, ja olkoon a luvun m kanssa yhteistekijätön kokonaisluku. Tällöin määrittelemme luvun

$$\operatorname{ord}_m a \stackrel{\text{def}}{=} \min\left\{d \in \mathbb{Z}_+ \middle| a^d \equiv 1 \pmod{m}\right\}.$$

Eulerin lauseen nojalla $\operatorname{ord}_m a$ on hyvin määritelty ja vieläpä $\operatorname{ord}_m a \leqslant \varphi(m)$. Sanomme, että *$a$ kuuluu eksponenttiin* $\operatorname{ord}_m a$ modulo m.

Aiempaa terminologiaamme mukaillen sanommet, että a on *primitiivinen juuri modulo m* jos se kuuluu eksponenttiin $\varphi(m)$ modulo m.

Seuraavat todistukset olemme jo nähneet aiemmin, mutta silloin ne kirjoitettiin vain alkulukumoduksille.

Ensimmäinen havainto. *Jos* $a^d \equiv 1 \pmod{m}$, *missä* $d \in \mathbb{Z}_+$, *niin* $\operatorname{ord}_m a \mid d$. *Erityisesti* $\operatorname{ord}_m a \mid \varphi(p-1)$.

Nimittäin, jos olisi $\operatorname{ord}_m a \nmid d$, niin löytyisi luvut $q \in \mathbb{Z}$ ja $r \in \mathbb{Z}$, joille $d = q \operatorname{ord}_m a + r$ ja $0 < r < \operatorname{ord}_p a$, ja tällöin tietenkin olisi

$$a^r \equiv a^{q \operatorname{ord}_p a + r} \equiv a^d \equiv 1 \pmod{m},$$

vastoin luvun $\operatorname{ord}_m a$ määritelmää.

Toinen havainto. *Olkood* $d, e \in \mathbb{Z}_+$. *Tällöin* $a^d \equiv a^e \pmod{m}$ *jos ja vain jos* $d \equiv e \pmod{\operatorname{ord}_m a}$.

Nimittäin, jos vaikkapa $d \equiv e \pmod{\operatorname{ord}_m a}$ ja $d > e$, niin $d = e + q \operatorname{ord}_m a$ jollakin $q \in \mathbb{Z}_+$, jolloinka tietysti

$$a^d \equiv a^{d + q \operatorname{ord}_m a} \equiv a^e \pmod{m},$$

ja toisaalta, jos $a^d \equiv a^e \pmod{m}$, ja vaikkapa $d > e$, niin $a^{d-e} \equiv 1 \pmod{m}$, jolloinka tietysti $\operatorname{ord}_m a \mid (d-e)$.

Kolmas havainto. *Olkoon $d \in \mathbb{Z}_+$. Tällöin a^d kuuluu eksponenttiin $\frac{\operatorname{ord}_m a}{(d, \operatorname{ord}_m a)}$ modulo m.*

Nimittäin varmasti

$$\left(a^d\right)^{\frac{\operatorname{ord}_m a}{(d, \operatorname{ord}_m a)}} \equiv \left(a^{\operatorname{ord}_m a}\right)^{\frac{d}{(d, \operatorname{ord}_m a)}} \equiv 1 \pmod{m},$$

ja toisaalta $\operatorname{ord}_m a \mid d \operatorname{ord}_m a^d$, eli

$$\frac{\operatorname{ord}_m a}{(d, \operatorname{ord}_m a)} \mid \operatorname{ord}_m a, \quad \text{eli} \quad \operatorname{ord}_m a^d \geqslant \frac{\operatorname{ord}_m a}{(d, \operatorname{ord}_m a)}.$$

Primitiiviset juuret parittomille alkulukumoduleille

Lemma. *Olkoon p pariton alkuluku, ja olkoon $\alpha \in \mathbb{Z}_+$. Jos g on primitiivinen juuri modulo p^α, niin*

$$\operatorname{ord}_{p^{\alpha+1}} g \in \left\{p^{\alpha-1}(p-1), p^\alpha (p-1)\right\}.$$

Nimittäin, koska

$$g^{\operatorname{ord}_{p^{\alpha+1}} g} \equiv 1 \pmod{p^{\alpha+1}},$$

on

$$g^{\operatorname{ord}_{p^{\alpha+1}} g} \equiv 1 \pmod{p^\alpha},$$

ja siis

$$p^{\alpha-1}(p-1) \mid \operatorname{ord}_{p^{\alpha+1}} g.$$

Toisaalta, varmasti

$$\operatorname{ord}_{p^{\alpha+1}} g \mid p^\alpha (p-1).$$

Lemma. *Olkoon p pariton alkuluku, ja olkoon $g \in \mathbb{Z}$ primitiivinen juuri modulo p. Tällöin ainakin toinen luvuista g ja $g+p$ on primitiivinen juuri, paitsi modulo p, myös modulo p^2.*

Jos g on primitiivinen juuri modulo p^2, niin asia on selvä. Oletetaan siis, että g ei ole primitiivinen juuri modulo p^2. Tällöin edellisen lemman nojalla

$$\operatorname{ord}_{p^2} g = p-1, \quad \text{ja} \quad \operatorname{ord}_{p^2} (g+p) \in \{p-1, p(p-1)\}.$$

Mutta

$$(g+p)^{p-1} \equiv g^{p-1} + p(p-1) g^{p-2} \equiv 1 + p(p-1) g^{p-2} \not\equiv 1 \pmod{p^2},$$

eli on oltava $\operatorname{ord}_{p^2} (g+p) = p(p-1)$, ja asia on jälleen selvä.

Lause. *Olkoon p pariton alkuluku, ja olkoon $\alpha \in \mathbb{Z}_+$. Tällöin on olemassa primitiivinen juuri modulo p^α.*

Todistus suoritetaan induktiolla eksponentin α suhteen. Tiedämme jo, että on olemassa luku $g \in \mathbb{Z}$, joka on primitiivinen juuri sekä modulo p, että modulo p^2. Oletetaan, että jokin luku $g \in \mathbb{Z}$ on primitiivinen juuri modulo p^α ja modulo $p^{\alpha+1}$. Tavoitteemme on osoittaa, että se on myös primitiivinen juuri modulo $p^{\alpha+2}$.

Tämän pykälän ensimmäisen lemman nojalla

$$\operatorname{ord}_{p^{\alpha+2}} g = p^\alpha (p-1) \quad \text{tai} \quad p^{\alpha+1}(p-1).$$

Riittää sulkea pois edellinen tapaus.

Tehtyjen oletusten nojalla

$$g^{p^{\alpha-1}(p-1)} = 1 + p^\alpha \ell$$

jollakin alkuluvulla p jaottomalla kokonaisluvulla ℓ. Nyt

$$g^{p^\alpha (p-1)} = (1 + p^\alpha \ell)^p \equiv 1 + p^{\alpha+1}\ell \not\equiv 1 \pmod{p^{\alpha+2}},$$

ja olemme valmiit.

Kiinalainen jäännöslause

Kiinalainen jäännöslause. *Olkoot $m_1, m_2, \ldots, m_n$ pareittain yhteistekijättömiä positiivisia kokonaislukuja, ja olkoot $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, missä tietenkin $n \in \mathbb{Z}_+$. Tällöin on olemassa kokonaisluku $d \in \mathbb{Z}_+$ siten, että luku $x \in \mathbb{Z}$ ratkaisee kongruenssit*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_n \pmod{m_n}$$

jos ja vain jos $x \equiv d \pmod{m_1 m_2 \cdots m_n}$.

Merkitään yksinkertaisuuden vuoksi $M = m_1 m_2 \cdots m_n$. Olkoot ensin $x, x' \in \mathbb{Z}$. Jos x on ratkaisu ja $x' \equiv x \pmod{M}$, niin varmasti x' on myös ratkaisu. Jos x ja x' ovat molemmat ratkaisuita, niin $x - x' \equiv 0 \pmod{m_1}$, $x - x' \equiv 0 \pmod{m_2}$, ja niin edelleen, ja siis $M \mid (x - x')$. Riittää siis todistaa, että on olemassa ainakin yksi ratkaisu $d \in \mathbb{Z}$. Tätä varten menettelemme kuten Lagrangen interpolaatiopolynomin konstruoinnissa.

Olkoon e_1, e_2, …, e_n sellaisia kokonaislukuja, että

$$e_1 \cdot \frac{M}{m_1} \equiv 1 \pmod{m_1}, \quad e_2 \cdot \frac{M}{m_2} \equiv 1 \pmod{m_2}, \quad \text{ja} \quad e_n \cdot \frac{M}{m_n} \equiv 1 \pmod{m_n}.$$

Valitaan

$$d = a_1 e_1 \cdot \frac{M}{m_1} + a_2 e_2 \cdot \frac{M}{m_2} + \ldots + a_n e_n \cdot \frac{M}{m_n}.$$

Tällöin

$$\begin{cases} d \equiv a_1 e_1 \frac{M}{m_1} + 0 + 0 + \ldots + 0 \equiv a_1 \pmod{m_1}, \\ d \equiv 0 + a_2 e_2 \frac{M}{m_2} + 0 + \ldots + 0 \equiv a_2 \pmod{m_2}, \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots \\ d \equiv 0 + 0 + \ldots + 0 + a_n e_n \frac{M}{m_n} \equiv a_n \pmod{m_n}, \end{cases}$$

ja olemme valmiit.

Fermat'n–Girardin lause

Fermat'n–Girardin lause. *Olkoon p sellainen alkuluku, että $p \equiv 1 \pmod 4$. Tällöin $p = x^2 + y^2$ joillakin kokonaisluvuilla x ja y.*

Ensin toteamme, että löytyy "pieni" luvun p monikerta, joka on kahden neliön summa. Nimittäin, koska $p \equiv 1 \pmod 4$, on kongruenssilla $x^2 \equiv -1 \pmod p$ ratkaisu $x \in \mathbb{Z}$. Valitkaamme itseisesti pienin ratkaisu, jolle siis pätee $|x| < \frac{p}{2}$. Tällöin siis $p \mid \left(x^2 + 1\right)$ ja

$$0 < x^2 + 1 < \frac{p^2}{4} + 1 = \frac{p^2 + 4}{4} < p^2.$$

Voimme siis valita *pienimmän* luvun $m_0 \in \mathbb{Z}_+$, jolle $m_0 p = a^2 + b^2$ joillakin $a, b \in \mathbb{Z}$. Varmasti pätee $m_0 < p$. Jos $m_0 = 1$, mitään todistettavaa ei ole. Oletamme siis, että $m_0 > 1$ tavoitteenamme johtaa ristiriita.

Seuraavaksi toteamme, että m_0 on välttämättä pariton. Nimittäin, jos m_0 olisi parillinen, niin olisi

$$\frac{m_0 p}{2} = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2,$$

vastoin luvun m_0 määritelmää.

Tarkastelkaamme sitten lukujen a ja b itseisesti pienimpiä jäännöksiä α ja β modulo m_0. Näille siis pätee $\alpha, \beta \in \mathbb{Z}$,

$$\alpha \equiv a \quad \text{ja} \quad \beta \equiv b \pmod{m)_0},$$

$|\alpha| < \frac{m_0}{2}$, ja $|\beta| < \frac{m_0}{2}$. Lisäksi α ja β eivät voi molemmat olla nollia, koska tällöin luku $m_0 p = a^2 + b^2$ olisi jaollinen luvulla m_0^2, eli p olisi jaollinen luvulla m_0, mikä on mahdotonta. Täten

$$\alpha^2 + \beta^2 \equiv a^2 + b^2 \pmod{m)_0}$$

ja

$$0 < \alpha^2 + \beta^2 < 2 \cdot \frac{m_0^2}{4} < m_0^2,$$

eli $\alpha^2 + \beta^2 = m_1 m_0$ jollakin $m_1 \in \mathbb{Z}_+$, jolle $m_1 < m_0$.

Lopuksi,

$$m_0^2 m_1 p = m_0 p \cdot m_1 m_0 = \left(a^2 + b^2\right)\left(\alpha^2 + \beta^2\right)$$
$$(a\alpha + b\beta)^2 + (a\beta - b\alpha)^2,$$

ja

$$a\alpha + b\beta \equiv a^2 + b^2 \equiv 0 \quad \text{ja} \quad a\beta - b\alpha \equiv 0 \pmod{m)_0},$$

eli

$$m_1 p = \left(\frac{a\alpha + b\beta}{m_0}\right)^2 + \left(\frac{a\beta - b\alpha}{m_0}\right)^2,$$

vastoin luvun m_0 määritelmää.

Lagrangen neljän neliön lause

Päätämme tämän luvun esittämällä todistuksen kuuluisalle teoreemalle, jonka ensimmäisen kokonaisen todistuksen esitti J. L. Lagrange vuonna 1770.

Lagrangen neljän neliön lause. *Jokainen $n \in \mathbb{Z}_+$ on esitettävissä enintään neljän neliöluvun summana.*

Todistuksessa seuraamme klassikkoteosta [**?**]. Koska $1 = 1^2$ ja $2 = 1^2 + 1^2$, riittää aritmetiikan peruslauseen ja seuraavan Eulerin identiteetin perusteella todistaa Lagrangen lause vain parittomille alkuluvuille.

Eulerin identiteetti. *Kaikilla $a, b, c, d, \alpha, \beta, \gamma, \delta \in \mathbb{Z}$ pätee*

$$(a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2) = (a\alpha+b\beta+c\gamma+d\delta)^2$$
$$+ (a\beta-b\alpha+c\delta-d\gamma)^2 + (a\gamma-c\alpha+d\beta-b\delta)^2 + (a\delta-d\alpha+b\gamma-c\beta)^2$$

Todistus. Suora lasku.

Lause. *Jokainen pariton alkuluku on esitettävissä neljän neliön summana.*

Todistus. Olkoon p pariton alkuluku. Osoitetaan ensin, että löytyy luonnollinen luku $m \in \{1, 2, \ldots, p-1\}$ siten, että $mp = x^2 + y^2 + 1^2 + 0^2$, joillakin $x, y \in \mathbb{Z}$. $\frac{p+1}{2}$ lukua $0^2, 1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ ovat keskenään epäkongruentteja modulo p. Niin myös $\frac{p+1}{2}$ lukua $-1-0^2, -1-1^2, -1-2^2, \ldots, -1-(\frac{p-1}{2})^2$. Siispä kyyhkyslakkaperiaatteen nojalla välttämättä $x^2 \equiv -1 - y^2 \pmod{p}$ joillakin $x, y \in \{0, 1, 2, \ldots, \frac{p-1}{2}\}$, eli $x^2 + y^2 + 1 = mp$ jollakin $m \in \mathbb{Z}$. Selvästi tässä $m > 0$. Toisaalta $mp = x^2 + y^2 + 1 \leqslant (\frac{p-1}{2})^2 + (\frac{p-1}{2})^2 + 1 < p^2$, joten $m < p$. Siis $1 \leqslant m \leqslant p-1$.

Voidaan siis valita **pienin** $m_0 \in \mathbb{Z}_+$, jolle $m_0 p$ on neljän neliön summa – sanokaamme $m_0 p = a^2 + b^2 + c^2 + d^2$, missä $a, b, c, d \in \mathbb{Z}$. Edellä sanotun nojalla varmasti $m_0 < p$. Jos nyt $m_0 = 1$, niin $p = m_0 p = a^2 + b^2 + c^2 + d^2$ ja asia on selvä. Tarkastellaan siis tilannetta, missä $m_0 > 1$.

Jos m_0 on parillinen, niin välttämättä parillinen määrä luvuista a, b, c, d on parillisia. Jos täsmälleen kaksi niistä ovat parillisia niin voidaan olettaa, että nimenomaan a ja b ovat parillisia ja c ja d parittomia. Nyt joka tapauksessa luvut $a+b, a-b, c+d, c-d$ ovat kaikki varmasti parillisia ja saadaan

$$\frac{m_0}{2} p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2,$$

vastoin luvun m_0 määritelmää. Siis m_0 on välttämättä pariton, ja erityisesti $m_0 \geqslant 3$.

Seuraavaksi todetaan, että kaikki luvut a, b, c, d eivät voi olla jaollisia luvulla m_0, sillä tällöin olisi $m_0 \mid p$, mikä on mahdotonta. Kun nyt valitaan $\alpha, \beta, \gamma, \delta$ lukujen a, b, c, d (vastaavasti) itseisesti pienimmiksi jäännöksiksi modulo m_0, on

$$\alpha \equiv a, \beta \equiv b, \gamma \equiv c, \text{ja } \delta \equiv d \pmod{m_0},$$

lisäehdoin $\alpha, \beta, \gamma, \delta \in \mathbb{Z} \cap \left]-\frac{m_0}{2}, \frac{m_0}{2}\right[$ sekä $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 > 0$. Toisaalta myös

$$0 < \alpha^2 + \beta^2 + \gamma^2 + \delta^2 < 4\left(\frac{m_0}{2}\right)^2 = m_0^2,$$

ja

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m_0},$$

eli $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = m_0 m_1$ jollakin $m_1 \in \{1, 2, \ldots, m_0 - 1\}$.

Eulerin identiteettiä käyttämällä: $m_0^2 m_1 p = m_0 p \cdot m_0 m_1 = (a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = A^2 + B^2 + C^2 + D^2$, missä

$$\begin{cases} A = a\alpha + b\beta + c\gamma + d\delta \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m_0}, \\ B = a\beta - b\alpha + c\delta - d\gamma \equiv ab - ba + cd - dc \equiv 0 \pmod{m_0}, \\ C = a\gamma - c\alpha + d\beta - b\delta \equiv ac - ca + db - bd \equiv 0 \pmod{m_0}, \\ D = a\delta - d\alpha + b\gamma - c\beta \equiv ad - da + bc - cb \equiv 0 \pmod{m_0}. \end{cases}$$

Siis $m_1 p = \left(\frac{A}{m_0}\right)^2 + \left(\frac{B}{m_0}\right)^2 + \left(\frac{C}{m_0}\right)^2 + \left(\frac{D}{m_0}\right)^2$, vastoin luvun m_0 määritelmää. Täten $m_0 = 1$ ja $p = m_0 p = a^2 + b^2 + c^2 + d^2$ on neljän neliön summa. Q.E.D.

Kotitehtäviä

41. Etsi pienin positiivinen kokonaisluku x, jolle

$$x \equiv 1 \pmod 3, \quad x \equiv 2 \pmod 5, \quad \text{ja} \quad x \equiv 3 \pmod 7.$$

42. Olkoon $k, \alpha \in \mathbb{Z}_+ \cup \{0\}$. Osoita, ettei luku $4^\alpha (8k + 7)$ voi olla kolmen neliön summa. [Syvällinen *Legendren lause* sanoo, että nämä ovat itse asiassa ainoat luonnolliset luvut, jotka eivät ole kolmen neliön summia.]

43. Olkoon p pariton alkuluku ja olkoon $\alpha \in \mathbb{Z}_+$. Osoita, että on olemassa primitiivinen juuri modulo $2p^\alpha$.

44. Osoita, että on olemassa 10^{100} peräkkäistä kokonaislukua, joista jokainen on jaollinen kahdella eri alkuluvulla.

45. Osoita, että on olemassa kokonaislukukertoiminen polynomi $P(x)$ jolla ei ole kokonaislukunollakohtaa, mutta jolle jokaisella $n \in \mathbb{Z}_+$ löytyy $a \in \mathbb{Z}$, jolle $n \mid P(a)$.

46. Olkoon $m \in \mathbb{Z}_+$ sellainen, että $m \neq 1$, $m \neq 2$, $m \neq 4$, ja että m ei ole muotoa p^α eikä $2p^\alpha$ millään parittomalla alkuluvulla p eikä millään $\alpha \in \mathbb{Z}_+$. Osoita, ettei ole olemassa primitiivistä juurta modulo m. [Vihje: Riittää osoittaa, että $a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod m$ aina kun $a \in \mathbb{Z}$ on luvun m kanssa yhteistekijätön.]

47. *Neliölukuja* ovat luvut 0^2, 1^2, 2^2, 3^2, 4^2, j.n.e. Tässä tehtävässä tarkastellaan kokonaislukujen esittämistä kahden neliöluvun summina.

a) Osoita, että jos kokonaisluku x on kahden neliöluvun summa, niin myös luku $2x$ on.

b) Osoita, että jos kokonaisluvut x ja y ovat kahden neliöluvun summia, niin myös luku xy on.

c) Olkoon q sellainen alkuluku, että $q \equiv 3 \pmod 4$ ja olkoot a ja b kokonaislukuja. Osoita, että jos $q \mid (a^2 + b^2)$, niin $q \mid a$ ja $q \mid b$.

d) *Fermat'n ja Girardin lause* sanoo, että jos p on alkuluku jolle pätee $p \equiv 1 \pmod 4$, niin p on kahden neliöluvun summa. Selvitä yllä tehtyjen havaintojen a), b) ja c), sekä Fermat'n ja Girardin lauseen avulla, mitkä kokonaisluvut ovat esitettävissä kahden neliöluvun summina.

48. Olkoon $\alpha \in \mathbb{Z}_+$ ja oletetaan, että $\alpha \geqslant 3$. Tällöin jokaiselle parittomalle $n \in \mathbb{Z}_+$ löytyy yksikäsitteinen luku $\beta \in \mathbb{Z}_+$, jolle

$$n \equiv (-1)^{\frac{n-1}{2}} 5^{\beta} \pmod{2^{\alpha}} \quad \text{ja} \quad 1 \leqslant \beta \leqslant \frac{\varphi(2^{\alpha})}{2}.$$

Luku 7

Gaussin kokonaisluvut

Kutsumme *Gaussin kokonaisluvuksi* kompleksilukua $x+yi$, jonka reaali- ja imaginaariosat ovat kokonaislukuja. Merkitsemme Gaussin kokonaislukujen joukkoa $\mathbb{Z}[i]$. Tyypillisesti merkitsemme Gaussin kokonaislukuja pienillä kreikkalaisilla kirjaimilla α, β, γ, ...

Tietenkin Gaussin kokonaislukujen summat, erotukset ja tulot ovat edelleen Gaussin kokonaislukuja. Voimme siis määritellä jaollisuusrelaation kuten tavallisestikin: Olkoot $\alpha, \beta \in \mathbb{Z}[i]$. Tällöin merkitsemme $\beta \mid \alpha$, jos on olemassa $\gamma \in \mathbb{Z}[i]$, jolle $\alpha = \beta\gamma$. Muutoin merkitsemme $\beta \nmid \alpha$. Kun $\beta \mid \alpha$, käytämme samaa terminologiaa kuin aiemminkin. Sanomme esimerkiksi, että β *jakaa luvun* α, *luku* α *on jaollinen luvulla* β, ja niin edelleen.

Määrittelemme myös joitakin muitakin uusia käsitteitä. Koska emme voi käyttää reaalilukujen järjestysrelaatiota, tarvitsemme jonkin muun tavan vertailla lukujen kokoja. Tätä varten määrittelemme Gaussin kokonaisluvun $\alpha = x + yi$ *normin*

$$N\alpha = |\alpha|^2 = \alpha\overline{\alpha} = x^2 + y^2.$$

On helppo nähdä, että tällä normilla on seuraavat ominaisuudet:

* $N\alpha \in \{0\} \cup \mathbb{Z}_+$.
* $N\alpha = 0$ jos ja vain jos $\alpha = 0$.
* $N\alpha = 1$ jos ja vain jos $\alpha \in \{\pm 1, \pm i\}$.
* $N\alpha \geqslant 2$ jos ja vain jos $\alpha \notin \{0, \pm 1, \pm i\}$.

Tämän käsitteen etu pelkkään kompleksiseen itseisarvoon nähden on se, että, toisin kuin $|\alpha|$, normi $N\alpha$ on aina kokonaisluku, ja normin kautta voimme kytkeä Gaussin kokonaislukujen jaollisuuden tavallisten kokonaislukujen jaollisuuteen.

Havainto. *Olkoot* $\alpha, \beta \in \mathbb{Z}[i]$. *Tällöin* $N(\alpha\beta) = N\alpha \cdot N\beta$. *Lisäksi, jos* $\beta \mid \alpha$, *niin* $N\beta \mid N\alpha$.

Todistukset näille seikoille ovat helppoja. Nimittäin,

$$N(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\overline{\alpha} \cdot \beta\overline{\beta} = N\alpha \cdot N\beta,$$

ja jos $\beta \mid \alpha$, niin $\alpha = \beta\gamma$ jollakin $\gamma \in \mathbb{Z}[i]$, jolloin

$$N\alpha = N\beta \cdot N\gamma.$$

——— : ———

Tavallisten kokonaislukujen ± 1 yleistys Gaussin kokonaisluvuille tulevat olemaan niin sanotut *yksiköt*, jotka määritellään luvuiksi $\varepsilon \in \mathbb{Z}[i]$, joille $\varepsilon \,|\, 1$. Koska varmasti $N\varepsilon \,|\, N1 = 1$, on oltava $N\varepsilon = 1$, eli $\varepsilon \in \{\pm 1, \pm i\}$. Tästä seuraa helposti, että Gaussin kokonaislukujen yksiköt ovat täsmälleen ± 1 ja $\pm i$, eli täsmälleen ne luvut ε, joille $N\varepsilon = 1$.

Sanomme, että Gaussin kokonaisluvut α ja β ovat *keskenään yhteistekijättömät*, jos niiden ainoat yhteiset tekijät ovat yksiköitä.

Kutsumme Gaussin kokonaislukua π *Gaussin alkuluvuksi*, jos jokaisessa tulossa $\pi = \alpha\beta$, missä $\alpha, \beta \in \mathbb{Z}[i]$, jokin tekijä on aina yksikkö. [Oikeastaan tämä on *jaottoman* Gaussin kokonaisluvun määritelmä; alkuluvut määritellään yleensä luvuiksi, joille pätee Eukleideen lemman kanssa analoginen yleistys. Mutta koska tulee osoittautumaan, että Gaussin kokonaisluvuille pätee yksikäsitteinen tekijöihinjako, nämä käsitteet tulevat lopulta olemaan samoja.]

Esimerkki. Luku 3 on Gaussin alkuluku. Nimittäin, $N3 = 9$, ja jos π olisi luvun 3 epätriviaali tekijä, olisi luvun $N\pi$ oltava luvun $N3 = 9$ epätriviaali tekijä, eli olisi oltava $N\pi = 3$, mikä on mahdotonta, koska $N\pi$ on kahden neliön summa kun taas luku 3 ei ole.

Havainto. *Olkoon $\pi \in \mathbb{Z}[i]$ sellainen, että $N\pi$ on alkuluku. Tällöin π on Gaussin alkuluku.*

Nimittäin, jos $\pi = \alpha\beta$ joillekin $\alpha, \beta \in \mathbb{Z}[i]$, niin $N\pi = N\alpha \cdot N\beta$, eli $N\alpha = 1$ tai $N\beta = 1$, eli toinen luvuista α ja β on varmasti yksikkö.

Esimerkki. Nyt pystymme helposti tuottamaan konkreettisia esimerkkejä Gaussin alkuluvuista. Koska $N(1+i) = 2$, on $1+i$ Gaussin alkuluku. Luvulla 2 on siis Gaussin kokonaislukujen joukossa tekijöihinjako $-i\,(1+i)^2$.

Koska $N(1+2i) = 5$ ja $N(2+3i) = 13$, ovat luvut $1 \pm 2i$ sekä $2 \pm 3i$ Gaussin alkulukuja.

——— : ———

Koska Gaussin kokonaislukujen kanssa emme voi kanonisesti valita vain yhtä luvuista α, $-\alpha$, $i\alpha$ ja $-i\alpha$, tulee esimerkiksi jokaisesta Gaussin alkuluvusta olemaan aina läsnä neljä eri versiota. Selkiyttääksemme tilannetta otamme käyttöön *liitännäisyyden käsitteen*: Sanomme kahden Gaussin kokonaisluvun α ja β olevan keskenään *liitännäisiä*, jos $\alpha = \varepsilon\beta$ jollakin yksiköllä ε, ja merkitsemme tätä asiaintilaa $\alpha \sim \beta$. Muutoin merkitsemme $\alpha \not\sim \beta$. Luvun α kanssa liitännäiset luvut ovat siis täsmälleen $\pm\alpha$ ja $\pm i\alpha$.

Luvut $\pm 1 \pm i$ ovat kaikki keskenään liitännäisiä. Jos $x, y \in \mathbb{Z}$ ja $x \neq y$, niin luvun $x + yi$ liitännäiset ovat

$$x + yi, \quad -y + xi, \quad -x - yi, \quad \text{ja} \quad y - xi,$$

kun taas luvun $x - yi$ ovat vastaavasti

$$x - yi, \quad y + xi, \quad -x + yi, \quad \text{ja} \quad -y - xi.$$

Erityisesti luvut $x \pm yi$ eivät ole keskenään liitännäisiä kun $x \neq y$.

Aritmetiikan peruslause Gaussin kokonaisluvuille

Jakoyhtälö. *Olkoot $\alpha, \beta \in \mathbb{Z}[i]$, ja oletetaan, että $\beta \neq 0$. Tällöin löytyy luvut $\xi, \rho \in \mathbb{Z}[i]$, joille*

$$\alpha = \xi\beta + \rho, \quad \text{ja} \quad N\rho < N\beta.$$

Toisin sanoen, on olemassa luku $\xi \in \mathbb{Z}[i]$, jolle

$$\left|\frac{\alpha}{\beta} - \xi\right| < 1.$$

Mutta tämä on selvää, sillä kompleksitasosta löytyy varmasti kokonaislukukoordinaattinen kompleksiluku enintään etäisyydeltä $\frac{1}{\sqrt{2}}$ pisteestä $\frac{\alpha}{\beta}$.

On hyvä huomata, että tässä ξ ja ρ eivät suinkaan ole yksikäsitteisiä.

Lause. *Olkoot α ja β keskenään yhteistekijättömiä Gaussin kokonaislukuja. Tällöin löytyy luvut $\xi, \eta \in \mathbb{Z}[i]$, joille*

$$\alpha\xi + \beta\eta = 1.$$

Vaihtelun vuoksi todistamme tämän eri tavalla kuin todistimme sen tavallisille kokonaisluvuille. Tarkastellaan kaikkia nollasta poikkeavia Gaussin kokonaislukuja, jotka ovat muotoa $\alpha\xi + \beta\eta$ joillakin $\xi, \eta \in \mathbb{Z}[i]$. Näiden normit ovat positiivisia kokonaislukuja, ja siksi jollakin niistä, sanokaamme luvulla γ, on pienin mahdollinen normi. Siis $\gamma = \alpha\xi + \beta\eta$ joillakin $\xi, \eta \in \mathbb{Z}[i]$.

Kirjoitetaan sitten jakoyhtälöt

$$\alpha = \kappa\gamma + \rho \quad \text{ja} \quad \beta = \kappa'\gamma + \rho',$$

missä $\kappa, \kappa', \rho, \rho' \in \mathbb{Z}[i]$, ja $N\rho < N\gamma$ ja $N\rho' < N\gamma$. Nyt

$$\rho = \alpha\left(1 - \kappa\xi\right) - \beta\eta \quad \text{ja} \quad \rho' = -\alpha\xi + \beta\left(1 - \kappa'\eta\right),$$

ja luvun γ määritelmän nojalla on oltava $\rho = \rho' = 0$, eli γ on lukujen α ja β yhteinen tekijä. Siis γ on yksikkö, mistä seuraa, että

$$\alpha \cdot \frac{\xi}{\gamma} + \beta \cdot \frac{\eta}{\gamma} = 1.$$

Eukleideen lemma. *Olkoon π Gaussin alkuluku, ja olkoot $\alpha, \beta \in \mathbb{Z}[i]$. Jos $\pi \mid \alpha\beta$, niin $\pi \mid \alpha$ tai $\pi \mid \beta$.*

Jos $\pi \mid \alpha$, mitään todistettavaa ei ole. Oletetaan siis, että $\pi \nmid \alpha$. Tällöin luvut π ja α ovat yhteistekijättömiä, koska niiden epätriviaali yhteinen tekijä olisi Gaussin alkuluvun π epätriviaali tekijä. Nyt edellisen lauseen nojalla löytyy luvut $\xi, \eta \in \mathbb{Z}[i]$, joille

$$\alpha\xi + \pi\eta = 1, \quad \text{ja edelleen} \quad \alpha\beta\xi + \pi\beta\eta = \beta.$$

Koska π jakaa viimeisen yhtälön vasemman puolen molemmat termit, on sen jaettava myös luku β, ja olemme valmiit.

Gaussin kokonaislukujen yksikäsitteinen tekijöihinjako. *Jokainen nollasta poikkeava Gaussin kokonaisluku on tekijöiden järjestystä ja yksiköillä kertomista vaille yksikäsitteisellä tavalla Gaussin alkulukujen tulo.*

Osoitetaan ensin alkutekijähajotelman olemassaolo. Olkoon annettu jokin $\alpha \in \mathbb{Z}[i] \setminus \{0, \pm 1, \pm i\}$. Jos α on Gaussin alkuluku, asia on selvä. Muutoin $\alpha = \beta\gamma$, joillakin $\beta, \gamma \in \mathbb{Z}[i]$, joilla molemmilla on aidosti pienempi normi kuin luvulla α. Jos β ja γ ovat Gaussin alkulukuja, asia on selvä. Muutoin ainakin toinen niistä voidaan pilkkoa vielä pienempien Gaussin kokonaislukujen tuloksi. Jatketaan näin niin kauan kuin mahdollista. Koska $N\alpha$ ei voi olla mielivaltaisen monen ykköstä suuremman kokonaisluvun tulo, tämän prosessin on joskus loputtava, jolloin α on kirjoitettu Gaussin alkulukujen tuloksi.

Tekijähajotelman yksikäsitteisyys seuraa nyt kuten tavallisillekin kokonaisluvuille. Olkoot $\pi_1, \pi_2, \ldots, \pi_m$ ja $\pi'_1, \pi'_2, \ldots, \pi'_n$, missä $m, n \in \mathbb{Z}_+$, Gaussin alkulukuja, ja oletetaan, että

$$\pi_1\pi_2 \cdots \pi_m = \pi'_1\pi'_2 \cdots \pi'_n.$$

Ilman yleisyyden menettämistä voidaan olettaa, että $m \leqslant n$. Nyt luvun π_1 täytyy jakaa jokin oikean puolen alkuluvuista, sanokaamme luku π'_1, jolloin $\pi'_1 = \varepsilon\pi_1$ jollakin yksiköllä ε. Nyt

$$\pi_2\pi_3 \cdots \pi_m = \varepsilon\pi'_2\pi'_3 \cdots \pi'_n.$$

Samalla tavalla kaikki vasemman puolen tekijät voi supistaa pois, kunnes lopulta jäljelle jää vain

$$1 = \varepsilon'\pi'_{m+1}\pi'_{m+2} \cdots \pi'_n,$$

missä ε' on yksikkö, kunhan oikean puolen tekijöiden järjestystä vain muutetaan sopivasti. Mutta tästä yhtälöstä seuraa välittömästi, että $n = m$, ja olemme valmiit.

Gaussin alkulukujen luokittelu

Lemma. *Jokainen Gaussin alkuluku π jakaa täsmälleen yhden tavallisen alkuluvun p.*

Gaussin alkuluku π varmasti jakaa ainakin yhden positiivisen kokonaisluvun, nimittäin oman norminsa $N\pi$. Jaetaan $N\pi$ alkutekijöihin tavallisten kokonaislukujen joukossa, jolloin Eukleideen lemman nojalla π jakaa jonkin niistä.

Yksikäsitteisyys seuraa siitä, että jos π jakaisi kaksi eri tavallista alkulukua p ja q, niin olisi $px + qy = 1$, joillakin $x, y \in \mathbb{Z}$, jolloinka $\pi \mid (px + qy) = 1$.

Gaussin alkulukujen luokittelu. *Gaussin alkuluvut jakautuvat seuraaviin kolmeen luokkaan:*

- *Luvun $1 + i$ liitännäisluvut, eli luvut $\pm 1 \pm i$.*
- *Tavalliset alkuluvut p, joille $p \equiv 3 \pmod 4$.*
- *Ne luvut $x + yi \in \mathbb{Z}[i]$, joille $x^2 + y^2$ on alkuluku, joka on $\equiv 1 \pmod 4$. Luvut $x + yi$ ja $x - yi$ eivät ole keskenään liitännäisiä.*

Olkoon $\pi = x + yi$ annettu Gaussin alkuluku, ja olkoon p se yksikäsitteinen tavallinen alkuluku, jonka π jakaa. Todistus jakautuu kolmeen eri tapaukseen sen mukaan, onko $p \equiv 1$, $p \equiv 2$ vai $p \equiv 3 \pmod 4$.

Olkoon ensin $p \equiv 2 \pmod 4$. Tällöin tietenkin $p = 2 = (1+i)(1-i)$, eli $\pi \mid (1 \pm i)$. Toisaalta, luvut $\pm 1 \pm i$ ovat Gaussin alkulukuja, sillä niiden normi on tavallinen alkuluku. Eli tässä tapauksessa $\pi \sim 1 + i$, eli $\pi = \pm 1 \pm i$.

Oletetaan sitten, että $p \equiv \pm 1 \pmod 4$. Todistuksen loppuosa perustuu siihen, että nyt on oltava $N\pi = p$ tai $N\pi = p^2$. Onhan $N\pi \mid Np = p^2$ ja $N\pi \neq 1$.

Olkoon ensin $p \equiv 3 \pmod 4$. Nyt ei voi olla $N\pi = p$, sillä tällöin olisi $p = x^2 + y^2$, eikä p voi olla kahden neliön summa. On siis $N\pi = p^2 = Np$. Koska $p = \pi\alpha$ jollakin $\alpha \in \mathbb{Z}[i]$, ja $Np = N\pi \cdot N\alpha$, on $N\alpha = 1$, eli α on yksikkö, ja $\pi \sim p$.

Olkoon lopuksi $p \equiv 1 \pmod 4$. Tiedämme, että löytyy $n \in \mathbb{Z}$, jolle $p \mid \big(n^2 + 1\big)$. Viimeksi mainittu luku jakautuu tietenkin tekijöiden $n \pm i$ tuloksi, ja p ei tietenkään voi jakaa kumpaakaan näistä. Erityisesti p ei voi olla Gaussin alkuluku. Tapaus $N\pi = p^2$ johtaisi siihen, että p olisi Gaussin alkuluku, kuten edellisessä tapauksessa. Täten on oltava $N\pi = p$, ja olemme valmiit.

Erityisesti tämä todistus antaa sivutuotteena myös seuraavan Fermat'n–Girardin lauseen tarkennuksen:

Fermat'n–Girardin lause. *Olkoon p alkuluku, jolle $p \equiv 1 \pmod 4$. Tällöin löytyy täsmälleen kahdeksan kokonaislukuparia $\langle x, y \rangle$, joille*

$$x^2 + y^2 = p.$$

Toisin sanoen, paitsi että p on kahden neliön summa, se on sitä vain oleellisesti ottaen yhdellä tavalla.

Pythagoraan kolmikot Gaussin kokonaisluvuilla

Päätämme tämän luvun esimerkkiin siitä, miten hyödyntää Gaussin kokonaislukujen tarjoamia ylimääräisiä tekijöihinjakoja Diofantoksen yhtälöitä ratkaistaessa. Tavoitteemme on ymmärtää yhtälön

$$x^2 + y^2 = z^2$$

kokonaislukuratkaisuita.

Koska lukujen x ja y yhteinen tekijä on myös luvun z tekijä, voimme ilman yleisyyden menettämistä rajoittua vain sellaisten ratkaisuiden tarkasteluun, joille $(x, y) = 1$. Tällöin erityisesti $2 \nmid z$, sillä jos olisi $2 \mid z$, olisi $x \equiv y \pmod 2$. Mutta x ja y eivät voi molemmat olla parillisia, sillä ne ovat keskenään yhteistekijättömiä, ja jos ne olisivat molemmat parittomia, olisi

$$0 \equiv z^2 \equiv x^2 + y^2 \equiv 1 + 1 \pmod 4,$$

mikä on mahdotonta. Täten $2 \nmid z$.

Gaussin kokonaislukujen joukossa tarkasteltavan yhtälön vasen puoli jakautuu tekijöihin seuraavasti:

$$(x + yi)(x - yi) = z^2.$$

Vasemman puolen kaksi tekijää $x \pm yi$ ovat keskenään yhteistekijättömät. Nimittäin, jos $\delta \in \mathbb{Z}[i]$ on niiden yhteinen tekijä, niin $\delta \,|\, 2x$ ja $\delta \,|\, 2y$. Nyt, jos luvulla δ olisi, Gaussin kokonaislukujen joukossa, yhteinen tekijä luvun $2 = -i\,(1+i)^2$ kanssa, eli jos $(1+i) \mid \delta$, niin olisi $(1+i)^2 \mid (x+yi)(x-yi) = z^2$, eli olisi $2 \mid z^2$, eli $2 \mid z$, mikä on jo aiemmin osoitettu mahdottomaksi. Siispä $\delta \,|\, x$ ja $\delta \,|\, y$. Koska x ja y ovat yhteistekijättömiä, on $ax + by = 1$ joillakin $a, b \in \mathbb{Z}$, ja siis $\delta \mid 1$, ja luvut $x \pm yi$ ovat osoittautuneet yhteistekijättömiksi.

Nyt Gaussin kokonaislukujen yksikäsitteisen tekijöihinjaon nojalla

$$(x+yi) = \varepsilon\,(a+b)^2 = \varepsilon\left(a^2 - b^2 + 2abi\right),$$

missä $a, b \in \mathbb{Z}$ ja ε on yksikkö. On siis tarkasteltava neljää eri tapausta sen mukaan, onko ε yhtä kuin 1, i, -1 vai $-i$:

$$\begin{cases} 1 & \Longrightarrow & x = a^2 - b^2, & y = 2ab, \\ i & \Longrightarrow & x = -2ab, & y = a^2 - b^2, \\ -1 & \Longrightarrow & x = b^2 - a^2, & y = -2ab, \\ -i & \Longrightarrow & x = 2ab, & y = b^2 - a^2. \end{cases}$$

On helppo tarkistaa, että kaikissa näissä tapauksissa $x^2 + y^2 = \left(a^2 + b^2\right)^2$. Siis jokainen alkuperäisen Diofantoksen yhtälön kokonaislukuratkaisu, jolle $(x, y) = 1$, on oleellisesti ottaen muotoa

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2,$$

joillakin keskenään yhteistekijättömillä luvuilla $a, b \in \mathbb{Z}$. Toisaalta, selvästi tätä muotoa olevat kolmikot ovat aina alkuperäisen yhtälön ratkaisuita. Kaikki muuta yhtälön ratkaisut saadaan kertomalla kaikki tuntemattomat samalla vakiolla.

Kotitehtäviä

49. Jaa Gaussin alkulukujen tuloiksi Gaussin kokonaisluvut **a)** 4; **b)** $103+103i$; **c)** 2011; ja **d)** $11 + 23i$. Ryhmittele keskenään liitännäiset Gaussin alkuluvut potensseiksi.

50. Etsi kaikki Gaussin kokonaislukujen parit $\langle \kappa, \rho \rangle$, joille

$$11 + 23i = \kappa\,(7 + 2i) + \rho \quad \text{ja} \quad N\rho < N(7 + 2i)\,.$$

51. Etsi jotkin Gaussin kokonaisluvut ξ ja η, joille

$$(11 + 23i)\,\xi + (7 + 2i)\,\eta = 1.$$

52. Olkoon $x + yi \in \mathbb{Z}[i]$. Milloin $(1+i) \mid (x+yi)$?

53. Olkoon $\pi \not\sim (1+i)$ ei-reaalinen Gaussin alkuluku. Oletetaan, että $\alpha \in \mathbb{Z}[i]$ on sellainen, että $\pi \mid \alpha$ ja $\pi \mid \overline{\alpha}$. Osoita, että $N\pi \mid \alpha$.

54. Olkoon π Gaussin alkuluku, ja $\alpha \in \mathbb{Z}[i]$ yhteistekijätön luvun π kanssa. Osoita, että

$$\alpha^{N\pi - 1} \equiv 1 \pmod{\pi},$$

eli että $\pi \mid \left(a^{N\pi-1} - 1\right)$. [Vihje: Hyödynnä Gaussin alkulukujen luokittelua. Tapauksessa, jossa π jakaa parittoman alkuluvun p, tarkastele lukuja α^p ja α^{p^2} modulo p.]

55. Etsi yhtälön

$$x^2 + 4 = y^3$$

sellaiset kokonaislukuratkaisut, joille x on pariton. [Vihje: käytä helppoa tekijöihinjakoa, osoita luvut $2 \pm xi$ keskenään yhteistekijättömiksi, totea että luku $2+ix$ voidaan kirjoittaa muodossa $(a + bi)^3$, ja tarkastele lopuksi imaginaariosia. Tämän pitäisi tuottaa kaksi ratkaisua.]

56. Tarkasteltaessa edellisen tehtävän niitä ratkaisuita, joille x on parillinen, päädytään helposti tarkastelemaan yhtälöä

$$x^2 + 1 = 2y^3.$$

Ratkaise tämä kokonaislukujen joukossa. [Vihje: Käytä jälleen sopivaa tekijöihinjakoa, tarkastele lukujen $x \pm i$ yhteisiä tekijöitä, päättele että voit kirjoittaa $(x \pm i) = (1 + i)(a + bi)^3$, ja tarkastele imaginaariosia. Tämän pitäisi johtaa kahteen yhtälöryhmään luvuille a ja b:

$$\begin{cases} a - b = \pm 1, \\ a^2 + 4ab + b^2 = \pm 1, \end{cases}$$

joista ensimmäisen pitäisi antaa kaksi ratkaisua, jälkimmäisen ei yhtäkään.]

Kotitehtävien ratkaisuita ja ratkaisuhahmotelmia

1. $(a-c) \mid \big((a-c)(d-b)+ab+cd\big) = (ad+bc)$.

2. a) Jokaisella lukua yksi suuremmalla kokonaisluvulla on ainakin kaksi positiivista tekijää, nimittäin luku yksi ja luku itse. Jos luvulla on vain kaksi positiivista tekijää, niin sen täytyy tietenkin olla alkuluku.

b) Jos $d(n)$ on pariton alkuluku, niin kanonisen alkutekijähajotelman mukainen kaava luvulle $d(n)$ voi sisältää vain yhden tulontekijän. Siis luvun n on oltava alkuluvun potenssi, missä eksponentin on oltava muotoa $q-1$ jollakin alkuluvulla q, onhan $q = d(n)$.

c) Jos $d(n)$ on pariton, niin kanoniseen alkutekijähajotelmaan perustuva kaavamme luvun n tekijöiden lukumäärälle voi sisältää vain parittomia tulontekijöitä. Siispä luvun n kanonisessa alkutekijähajotelmassa kaikkien eksponenttien on oltava parillisia. Tämä puolestaan tarkoittaa sitä, että luku n on neliöluku.

3. a) Jokaisella lukua yksi suuremmalla kokonaisluvulla on ainakin kaksi posiitivista tekijää, nimittäin luku yksi ja luku itse. Jos näiden summa on kaikkien tekijöiden summa, niin luvulla on tietenkin vain nämä kaksi tekijää, eli se on alkuluku.

b) Jälleen annetusta ehdosta seuraa, että luvulla n on vain kaksi tekijää ja sen on oltava alkuluku.

c) Parilliset täydelliset luvut ovat muotoa $2^{n-1}\,(2^n-1)$, missä multiplikandin 2^n-1 on oltava alkuluku ja $n \in \mathbb{Z}_+$. Tämä lauseke on aidosti kasvava muuttujan n suhteen ja $28 = 2^{3-1}\big(2^3-1\big)$. Riittää siis tarkastella kyseisen lausekkeen arvoja kun $n = 4, 5, \ldots$, kunnes on löydetty kaksi alkulukua muotoa 2^n-1.

Tämä suunnitelma on suoraviivainen toteuttaa: luku $2^4-1 = 15$ ei ole alkuluku, luku $2^5-1 = 31$ on alkuluku, luku $2^6-1 = 63$ ei ole alkuluku ja luku $2^7-1 = 127$ on alkuluku. Näin löydetyt alkuluvut 2^5-1 ja 2^7-1 vastaavat parillisia täydellisiä lukuja

$$16 \cdot 31 = 496 \quad \text{ja} \quad 64 \cdot 127 = 8128.$$

4. a) Helposti saadaan alkutekijähajotelmat $1080 = 2^3 \cdot 3^3 \cdot 5$, $667 = 23 \cdot 29$, ja $1573 = 11^2 \cdot 13$.

b) Lukujen alkutekijähajotelmien avulla on helppo laskea

$$\begin{cases} d(1080) = d\big(2^3 \cdot 3^3 \cdot 5\big) = (3+1)(3+1)(1+1) = 4 \cdot 4 \cdot 2 = 32, \\ d(667) = d(23 \cdot 29) = (1+1)(1+1) = 4, \\ d(1573) = d\big(11^2 \cdot 13\big) = (2+1)(1+1) = 6, \\ \sigma(1080) = \sigma\big(2^3 \cdot 3^3 \cdot 5\big) = \frac{2^4-1}{2-1} \cdot \frac{3^4-1}{3-1} \cdot \frac{5^2-1}{5-1} = 15 \cdot 40 \cdot 6 = 3600, \\ \sigma(667) = \sigma(23 \cdot 29) = \frac{23^2-1}{23-1} \cdot \frac{29^2-1}{29-1} = (23+1)(29+1) = 24 \cdot 30 = 720, \\ \sigma(1573) = \sigma\big(11^2 \cdot 13\big) = \frac{11^3-1}{11-1} \cdot \frac{13^2-1}{13-1} = 133 \cdot \frac{168}{12} = 133 \cdot 14 = 1862. \end{cases}$$

5. Merkitään tavanmukaisesti tuloa luvun n tekijöiden yli symbolilla $\prod_{d|n}$. Koska $\frac{n}{d}$ käy läpi luvun n tekijä kun d käy läpi luvun n tekijät, voimme päätellä seuraavasti:

$$\prod_{d|n} d = \sqrt{\prod_{d|n} d \cdot \prod_{d|n} d} = \sqrt{\prod_{d|n} d \cdot \prod_{d|n} \frac{n}{d}} = \sqrt{\prod_{d|n} d \cdot \frac{n}{d}} = \sqrt{\prod_{d|n} n} = n^{\frac{d(n)}{2}}.$$

6. Olkoon $n \in \mathbb{Z}_+$ pariton täydellinen luku. Luku 1 ei ole täydellinen koska $\sigma(1) = 1 \neq 2$. Siis luvulla n on ainakin yksi alkutekijä p.

Oletetaan, että $n = p^\alpha$, missä $\alpha \in \mathbb{Z}_+$ ja p on pariton alkuluku. Koska

$$\frac{p^{\alpha+1}-1}{p-1} = \sigma(n) = 2n = 2p^\alpha,$$

on oltava

$$p^{\alpha+1} - 2p^\alpha + 1 = 0,$$

mikä on mahdotonta. Siispä luvulla n on ainakin kaksi eri alkutekijää.

Oletetaan seuraavaksi, että $n = p^\alpha q^\beta$, missä p ja q ovat erisuuria parittomia alkulukuja ja $\alpha, \beta \in \mathbb{Z}_+$. Tällöin

$$\frac{p^{\alpha+1}-1}{p-1} \cdot \frac{q^{\beta+1}-1}{q-1} = \sigma(n) = 2n = 2p^\alpha q^\beta.$$

Sieventämällä saadaan, että

$$p^\alpha q^\beta \left(pq - 2p - 2q + 2\right) + 1 = 0. \qquad (\beta)$$

Koska p ja q ovat parittomia ja keskenään erisuuria alkulukuja, voidaan ilman yleisyyden menettämistä olettaa, että $p \geqslant 3$ ja $q \geqslant 5$, jolloin

$$pq - 2p - 2q + 2 = (p-2)\,q - 2\,(p-2) - 2 = (p-2)(q-2) - 2 > 1 \cdot 3 - 2 = 1.$$

Mutta nyt yhtälö (β) ei voi pitää paikkaansa, mikä on ristiriita. Täten luvulla n on vähintään kolme erisuurta alkutekijää.

7. a) Annettu Diofantoksen yhtälö voidaan kirjoittaa muodossa

$$(x-p)(y-p) = p^2.$$

Siispä $x-p$ on jokin luvuista p^2, p, 1, -1, $-p$ ja $-p^2$.

Tapauksista $x-p = p^2$, $x-p = p$ ja $x-p = 1$ saadaan ratkaisut $\langle x, y\rangle = \big\langle p^2+p, p+1\big\rangle$, $\langle x, y\rangle = \langle 2p, 2p\rangle$, ja $\langle x, y\rangle = \big\langle p+1, p^2+p\big\rangle$, vastaavasti.

Tapauksessa $x-p=-1$ olisi oltava $y=p-p^2<0$, tapauksessa $x-p=-p$ olisi oltava $x=0$ ja tapauksessa $x-p=-p^2$ olisi oltava $x=p-p^2<0$. Siispä yhtälöllä on vain yllä saadut kolme ratkaisua.

b) Annetun yhtälön voi kirjoittaa muodossa

$$(x+y+4)(xy+1)=5.$$

Nyt ensimmäisen tekijän on oltava jokin luvuista 5, 1, -1 ja -5, jolloin toisen tekijän on vastaavasti oltava jokin luvuista 1, 5, -5 ja -1. Siispä ratkaisut saadaan yhtälöryhmistä

$$\begin{cases} x+y=1, \\ xy=0, \end{cases} \quad \begin{cases} x+y=-3, \\ xy=4, \end{cases} \quad \begin{cases} x+y=-5, \\ xy=-6, \end{cases} \quad \text{sekä} \quad \begin{cases} x+y=-9, \\ xy=-2. \end{cases}$$

Näistä toisella ja viimeisellä ei ole kokonaislukuratkaisuita, ensimmäisella on kokonaislukuratkaisut $\langle x,y\rangle=\langle 1,0\rangle$ ja $\langle x,y\rangle=\langle 0,1\rangle$, ja kolmannella on kokonaislukuratkaisut $\langle x,y\rangle=\langle -6,1\rangle$ ja $\langle x,y\rangle=\langle 1,-6\rangle$.

8. Olkoon $n(x)\not\equiv 0$ $\mathbb{Z}$-kertoiminen pääpolynomi. Tehtävämme on siis osoittaa (Zermelon todistusta mukaillen), että $n(x)$ on tekijöiden järjestystä vaille yksikäsitteisellä tavalla jaottomien pääpolynomien tulo. Sovellamme tässä aiemmin esittelemäämme konventiota, jonka mukaan tyhjä tulo on $=1$.

Todistamme väitteen induktiolla asteen $\deg n(x)$ suhteen. Ensinnäkin väite on selvä tapauksessa $\deg n(x)=0$, jossa $n(x)\equiv 1$. Samoin esimerkiksi tapaus $\deg n(x)=1$ on varsin selvä.

Oletetaan sitten, että $\deg n(x)>0$, ja että väite on jo todistettu kaikille alempiasteisille ei-identtisesti häviäville pääpolynomeille. Jos $n(x)$ on jaoton, mitään todistettavaa ei ole. Oletetaan siis, että $n(x)$ ei ole jaoton. Tällöin löytyy alinta mahdollista positiivista astetta oleva pääpolynomi $p(x)$ joka jakaa polynomin $n(x)$. Tämä polynomi ei välttämättä ole yksikäsitteinen.

Voimme siis kirjoittaa $n(x)=p(x)\,b(x)$, missä $b(x)$ on $\mathbb{Z}$-kertoiminen pääpolynomi, jolle $0<\deg b(x)<\deg n(x)$. Polynomi $p(x)$ on jaoton, sillä sen alempiasteinen positiivisasteinen tekijä olisi myös polynomin $n(x)$ tekijä vastoin polynomin $p(x)$ määritelmää.

Koska $b(x)$ on alempaa astetta kuin $n(x)$, on se induktio-oletuksen nojalla jaottomien pääpolynomien tulo oleellisesti ottaen yksikäsitteisellä tavalla, ja siten $n(x)$ on jaottomien pääpolynomien tulo, ja sillä on vain oleellisesti ottaen yksi tällainen tekijähajotelma jossa esiintyy polynomi $p(x)$.

Seuraavaksi osoitamme, ettei polynomilla $n(x)$ ole muita tekijähajotelmia. Tehdään se vastaoletus, että löytyy jokin oleellisesti ottaen erilainen tekijähajotelma. Olkoon $q(x)$ eräs siinä esiintyvistä alimman asteen jaottomista tekijöistä. Nyt $p(x)\neq q(x)$, $\deg p(x)\leqslant q(x)$, ja $n(x)=q(x)\,c(x)$ jollakin $\mathbb{Z}$-kertoimisella pääpolynomilla $c(x)$, jolle $0<\deg c(x)<\deg n(x)$.

Olkoon nyt $h(x)$ jokin $\mathbb{Z}$-kertoiminen pääpolynomi, jolle $q(x)-h(x)\,p(x)$ on alempaa astetta kuin $q(x)$. Tällaisen saa tietysti vaikkapa polynomien jakokulmasta, tai vain yksinkertaisesti valitsemalla $h(x)=x^{\deg q(x)-\deg p(x)}$. Tietenkin $q(x)\neq h(x)\,p(x)$, koska $p(x)\nmid q(x)$.

Tarkastellaan nyt polynomia

$$n_0(x)=n(x)-h(x)\,p(x)\,c(x)=\begin{cases} p(x)\,\big(b(x)-h(x)\,c(x)\big) \\ \big(q(x)-h(x)\,p(x)\big)\,c(x)\,. \end{cases}$$

Varmasti $\deg n_0(x) < \deg n(x)$, ja siten induktio-oletus pätee polynomille $n_0(x)$ (ainakin jos sen jakaa korkeimman asteen termin kertoimellaan), eli polynomin $p(x)$ on esiinnyttävä ainakin toisen polynomeista $q(x) - h(x)\,p(x)$ ja $c(x)$ tekijähajotelmassa. Jälkimmäinen tapaus on suljettu pois jo aiemmin, ja edellisestä seuraisi, että $p(x) \mid q(x)$ johtaen ristiriitaan $p(x) = q(x)$. Olemme valmiit.

9. a) Käytetään Eukleideen algoritmia: Suorilla jakolaskuilla saamme

$$37 = 2 \cdot 13 + 11, \quad 13 = 1 \cdot 11 + 2, \quad 11 = 5 \cdot 2 + 1,$$

mistä seuraa, että

$$1 = 11 - 5 \cdot 2 = 37 - 2 \cdot 13 - 5\,(13 - 11) = 37 - 7 \cdot 13 + 5\,(37 - 2 \cdot 13) = 6 \cdot 37 - 17 \cdot 13.$$

Erityisesti siis $-13 \cdot 17 \equiv 1 \pmod{37}$, mistä saamme ensimmäisen kongruenssin ratkaisuksi $x \equiv -17 \cdot 31 \equiv -9 \pmod{37}$.

b) Koska $4 \cdot 15 \equiv 60 \equiv -1 \pmod{61}$, on kysytty ratkaisu $x \equiv -4 \cdot 9 \equiv 25 \pmod{61}$.

10. Väite seuraa suoraan siitä, että lukujen $21n + 4$ ja $14n + 3$ suurimman yhteisen tekijän on jaettava myös luku

$$3\,(14n + 3) - 2\,(21n + 4) = 42n + 9 - 42n - 8 = 1.$$

11. Väite seuraa siitä luvuilla $(n-1)!$ ja n on oltava epätriviaali yhteinen tekijä.

12. Jos mitkään kaksi luvuista $x_1, x_2, \ldots, x_p$ eivät olisi kongruentteja keskenään modulo p, niin silloin olisi täsmälleen yksi niistä kongruentti nollan kanssa, täsmälleen yksi niistä kongruentti yhden kanssa, täsmälleen yksi niistä kongruentti kahden kanssa, j.n.e., modulo p. Fermat'n pienen lauseen nojalla olisi tällöin

$$\begin{aligned} x_1^{p-1} + x_2^{p-1} + \ldots + x_p^{p-1} &\equiv 0^{p-1} + 1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \\ &\equiv 0 + 1 + 1 + \ldots + 1 \equiv p - 1 \pmod{p}. \end{aligned}$$

13. Suoraan Fermat'n pienen lauseen nojalla

$$1^{p^n} + 2^{p^n} + \ldots + (p-1)^{p^n} \equiv 1 + 2 + \ldots + (p-1) \equiv \frac{p\,(p-1)}{2} \equiv 0 \pmod{p}.$$

14. Koska $p \equiv 1 \pmod 4$, on lukuja $1, 2, \ldots, \frac{p-1}{2}$ parillinen määrä. Wilsonin lauseen nojalla

$$\begin{aligned} \left(\left(\tfrac{p-1}{2}\right)!\right)^2 \equiv \left(\tfrac{p-1}{2}\right)!\left(\tfrac{p-1}{2}\right)! &\equiv \left(\tfrac{p-1}{2}\right)! \cdot \tfrac{p+1}{2} \cdot \tfrac{p+3}{2} \cdot \ldots \cdot (p-1) \\ &\equiv (p-1)! \equiv -1 \pmod{p}. \end{aligned}$$

15. Olkoon $p \geqslant 5$ alkuluku. Tällöin

$$6a_{p-2} \equiv 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \equiv 3 + 2 + 1 - 6 \equiv 0 \pmod{p},$$

eli $p \mid a_{p-2}$. Lisäksi $2 \mid 10 = a_1$ ja $3 \mid 48 = a_2$. Täten ainoa luku joka on yhteistekijätön kaikkien jonon $a_1, a_2, \ldots$ elementtien kanssa, on yksi.

16. Tiedämme, että

$$a_2a_1 \equiv a_1, \quad a_3a_2 \equiv a_2, \quad \ldots, \quad \text{ja} \quad a_ka_{k-1} \equiv a_{k-1} \pmod{n}.$$

Jos olisi $n \mid a_k\,(a_1 - 1)$, olisi $a_1a_k \equiv a_k \pmod{n}$, ja sen seurauksena

$$a_1 \equiv a_2a_1 \equiv a_3a_2a_1 \equiv \ldots \equiv a_ka_{k-1}\ldots a_2a_1 \pmod{n},$$

ja

$$a_2 \equiv a_3a_2 \equiv a_4a_3a_2 \equiv \ldots \equiv a_ka_{k-1}\ldots a_2 \equiv a_1a_ka_{k-1}\ldots a_2 \pmod{n}.$$

Erityisesti olisi siis $a_1 \equiv a_2 \pmod{n}$, mistä seuraisi, että $a_1 = a_2$. Tämä on ristiriita ja täten $n \nmid a_k\,(a_1 - 1)$.

25. Koska $2^2 \equiv 4$ ja $2^3 \equiv 3 \pmod{5}$, on luku 2 eräs primitiivinen juuri modulo 5. Luvuista 1, 2, 3 ja 4 luvun $\varphi(5) = 4$ kanssa yhteistekijättömiä ovat vain 1 ja 3. Siis primitiivisiä juuria modulo 5 ovat täsmälleen ne luvut r joille $r \equiv 2$ tai $r \equiv 2^3 \equiv 3 \pmod{5}$.

b) Luvun $\varphi(11) = 10$ tekijät ovat 1, 2, 5 ja 10. Koska $2^2 \equiv 4$ ja $2^5 \equiv 10 \pmod{11}$, on luku 2 eräs primitiivinen juuri modulo 11. Koska luvuista 1, 2, ..., 10 on luvun $\varphi(11) = 10$ kanssa yhteistekijättömiä täsmälleen luvut 1, 3, 7 ja 9, ovat primitiivisiä juuria modulo 11 täsmälleen ne kokonaisluvut r, joille $r \equiv 2$, $r \equiv 2^3 \equiv 8$, $r \equiv 2^7 \equiv 7$, tai $r \equiv 2^9 \equiv 6$ modulo 11.

c) Luku kolme on eräs primitiivinen juuri modulo 43. Tämän näkemiseksi riittää osoittaa, että $3^d \not\equiv 1 \pmod{43}$ kaikilla luvun $\varphi(43) = 42 = 2 \cdot 3 \cdot 7$ epätriviaaleilla tekijöillä. Kyseiset epätriviaalit tekijät ovat 2, 3, 6, 7, 14 ja 21, ja vastaavat luvun kolme potenssit ovat seuraavaa modulo 43:

$$\begin{cases} 3^2 \equiv 9, \\ 3^3 \equiv 27, \\ 3^6 \equiv 729 \equiv -2, \\ 3^7 \equiv 3 \cdot (-2) \equiv -6, \\ 3^{14} \equiv (-6)^2 \equiv 36, \quad \text{ja} \\ 3^{21} \equiv (-6)^3 \equiv -216 \equiv -1. \end{cases}$$

Nyt primitiivisten juurten modulo 43 edustajisto saadaan potensseista 3^d, missä d on kokonaisluku jolle $1 \leqslant d \leqslant \varphi(42)$, ja $\big(d, \varphi(42)\big) = 1$. Nämä eksponentit d ovat 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37 ja 41. Näistä saadaan primitiivisiksi juuriksi modulo 43

$$\begin{cases} 3^1 \equiv 3, \\ 3^5 \equiv 243 \equiv 28, \\ 3^{11} \equiv 28^2 \cdot 3 \equiv 28 \cdot 84 \equiv 2352 \equiv 30, \\ 3^{13} \equiv 30 \cdot 9 \equiv 270 \equiv 12, \\ 3^{17} \equiv 3 \cdot 28 \cdot 30 \equiv 84 \cdot 30 \equiv 2520 \equiv 26, \\ 3^{19} \equiv 26 \cdot 9 \equiv 19, \\ 3^{23} \equiv 19 \cdot 81 \equiv 34, \\ 3^{25} \equiv 34 \cdot 9 \equiv 5, \\ 3^{29} \equiv 5 \cdot 81 \equiv 405 \equiv 18, \\ 3^{31} \equiv 18 \cdot 9 \equiv 33, \\ 3^{37} \equiv 33 \cdot 81 \cdot 9 \equiv 2673 \cdot 9 \equiv 7 \cdot 9 \equiv 63 \equiv 20, \quad \text{sekä} \\ 3^{41} \equiv 20 \cdot 81 \equiv 1620 \equiv 29. \end{cases}$$

Siis eräs primitiivisten juurten modulo 43 edustajisto koostuu luvuista 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33 ja 34.

26. a) Koska edellisen tehtävän c)-kohdan nojalla luku kolme kuuluu eksponenttiin 42 modulo 43, saadaan eksponenttiin 6 kuuluvien lukujen edustajistoksi potenssit 3^d, missä d on kokonaisluku jolle $1 \leqslant d \leqslant 42$ ja $(d, 42) = \frac{42}{6} = 7$. Tällaisia eksponentteja d ovat vain 7 ja 35. Näitä vastaavat potenssit modulo 43 ovat

$$3^7 \equiv 2187 \equiv 37, \quad \text{ja} \quad 3^{35} \equiv 243^7 \equiv 28^7 \equiv \left(28^2\right)^3 \cdot 28 \equiv 10^3 \cdot 28 \equiv 28000 \equiv 7.$$

b) Edellisen tehtävän c)-kohdassa saatiin primitiivisten juurten modulo 43 edustajistoksi joukko $\{3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34\}$. Eksponenttiin 21 kuuluvat täsmälleen näiden lukujen neliöt, eli eksponenttiin 21 kuuluvien lukujen edustajistoksi saadaan modulo 43

$$\begin{cases} 3^2 \equiv 9, & 26^2 \equiv 676 \equiv 31, \\ 5^2 \equiv 25, & 28^2 \equiv 784 \equiv 10, \\ 12^2 \equiv 144 \equiv 15, & 29^2 \equiv 841 \equiv 24, \\ 18^2 \equiv 324 \equiv 23, & 30^2 \equiv 900 \equiv 40, \\ 19^2 \equiv 361 \equiv 17, & 33^2 \equiv 1089 \equiv 14, \quad \text{sekä} \\ 20^2 \equiv 400 \equiv 13, & 34^2 \equiv 1156 \equiv 38. \end{cases}$$

Edustajistoksi saadaan siis $\{9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40\}$.

27. Selvästi luku 2 kuuluu eksponenttiin n modulo $2^n - 1$.

28. Koska $(p-2, p-1) = 1$, on luku $r' = r^{p-2}$ myös primitiivinen juuri modulo p ja toisaalta

$$rr' \equiv r \cdot r^{p-2} \equiv r^{p-1} \equiv 1 \pmod{p}.$$

29. Olkoon r primitiivinen juuri modulo p. Tällöin

$$\begin{aligned} (p-1)! &\equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot r \cdot r^2 \cdot r^3 \cdot \ldots \cdot r^{p-2} \equiv r^{1+2+3+\ldots+(p-2)} \\ &\equiv r^{\frac{(p-1)(p-2)}{2}} \equiv \left(r^{\frac{p-1}{2}}\right)^{p-2} \equiv (-1)^{p-2} \equiv -1 \pmod{p}. \end{aligned}$$

30. Olkoon r primitiivinen juuri modulo p. Koska luku $r^{\frac{p-1}{2}}$ ratkaisee yhtälön $x^2 \equiv 1 \pmod{p}$, ja $r^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, on oltava $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Erityisesti siis

$$\left(r^{\frac{p-1}{4}}\right)^2 \equiv r^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

31. Jos $(p-1) \mid n$, niin Fermat'n pienen lauseen nojalla on

$$1^n + 2^n + 3^n + \ldots + (p-1)^n \equiv 1 + 1 + 1 + \ldots + 1 \equiv p - 1 \equiv -1 \pmod{p}.$$

Olkoon r primitiivinen juuri modulo p. Jos $(p-1) \nmid n$, niin löytyy sellainen kokonaisluku s, että $s\,(r^n - 1) \equiv 1 \pmod{p}$. Tavanomaisesta geometrisen sarjan summakaavasta sekä Fermat'n pienestä lauseesta seuraa, että

$$\begin{aligned} 1^n + 2^n + 3^n + \ldots + (p-1)^n &\equiv 1^n + r^n + r^{2n} + r^{3n} + \ldots + r^{(p-2)n} \\ &\equiv s\left((r^n)^{p-1} - 1\right) \equiv s\,(1-1) \equiv 0 \pmod{p}. \end{aligned}$$

32. Jos $p = 3$, niin (kongruenssia modulo p vaille) ainoa primitiivinen juuri modulo p on -1. Siispä tapauksessa $p = 3$ on $r_1 \equiv -1 \pmod 3$. Oletetaan sitten, että $p > 3$. Koska -1 kuuluu eksponenttiin $2 < p-1$ modulo p, ei -1 ole primitiivinen juuri modulo p. Tehtävän 4 nojalla luvut r_1, r_2, …, $r_{\varphi(p-1)}$ voidaan jakaa pareiksi $\langle r, r' \rangle$, joille $rr' \equiv 1 \pmod p$. Siis tulossa $r_1 r_2 \cdots r_{\varphi(p-1)}$ kaikki supistuu kun sitä tarkastellaan modulo p, ja siis

$$r_1 r_2 \cdots r_{\varphi(p-1)} \equiv 1 \pmod p.$$

33. a) Neliönjäännösten resiprookkilauseen toisen täydennyslauseen nojalla

$$\left(\frac{-1}{5}\right)_{\mathscr{L}} = (-1)^{\frac{5-1}{2}} = 1.$$

b) Neliönjäännösten resiprookkilauseen toisen täydennyslauseen mukaan

$$\left(\frac{2}{13}\right)_{\mathscr{L}} = (-1)^{\frac{13^2-1}{8}} = -1.$$

c) Luvut 73 ja 83 ovat molemmat alkulukuja. Neliönjäännösten resiprookkilauseen nojalla

$$\begin{aligned}\left(\frac{73}{83}\right)_{\mathscr{L}} &= (-1)^{\frac{73-1}{2}\cdot\frac{83-1}{2}} \cdot \left(\frac{83}{73}\right)_{\mathscr{L}} = \left(\frac{10}{73}\right)_{\mathscr{L}} = (-1)^{\frac{73^2-1}{8}} \cdot \left(\frac{5}{73}\right)_{\mathscr{L}} \\ &= 1 \cdot (-1)^{\frac{5-1}{2}\cdot\frac{73-1}{2}} \cdot \left(\frac{73}{5}\right)_{\mathscr{L}} = \left(\frac{3}{5}\right)_{\mathscr{L}} = -1.\end{aligned}$$

d) Osoittautuu, että 1367 on alkuluku, ja helposti saadaan tekijöihinjako $371 = 7 \cdot 53$. Neliönjäännösten resiprookkilauseella siis

$$\begin{aligned}\left(\frac{371}{1367}\right)_{\mathscr{L}} &= \left(\frac{7}{1367}\right)_{\mathscr{L}} \cdot \left(\frac{53}{1367}\right)_{\mathscr{L}} \\ &= (-1)^{\frac{7-1}{2}\cdot\frac{1367-1}{2}} \cdot \left(\frac{1367}{7}\right)_{\mathscr{L}} \cdot (-1)^{\frac{53-1}{2}\cdot\frac{1367-1}{2}} \cdot \left(\frac{1367}{53}\right)_{\mathscr{L}} \\ &= -\left(\frac{2}{7}\right)_{\mathscr{L}} \cdot \left(\frac{42}{53}\right)_{\mathscr{L}} = -(-1)^{\frac{7^2-1}{8}} \cdot \left(\frac{2}{53}\right)_{\mathscr{L}} \cdot \left(\frac{3}{53}\right)_{\mathscr{L}} \cdot \left(\frac{7}{53}\right)_{\mathscr{L}} \\ &= -(-1)^{\frac{53^2-1}{8}} \cdot (-1)^{\frac{3-1}{2}\cdot\frac{53-1}{2}} \cdot \left(\frac{53}{3}\right)_{\mathscr{L}} \cdot (-1)^{\frac{7-1}{2}\cdot\frac{53-1}{2}} \cdot \left(\frac{53}{7}\right)_{\mathscr{L}} \\ &= -(-1) \cdot (+1) \cdot \left(\frac{2}{3}\right)_{\mathscr{L}} \cdot (+1) \cdot \left(\frac{4}{7}\right)_{\mathscr{L}} = (-1) \cdot (+1) = -1.\end{aligned}$$

e) Luvun 682 tekijöihinjako on $2 \cdot 11 \cdot 31$. Neliönjäännösten resiprookkilauseen nojalla siis samassa hengessä hengessä kuin aiemminkin on

$$\begin{aligned}\left(\frac{682}{911}\right)_{\mathscr{L}} &= \left(\frac{2}{911}\right)_{\mathscr{L}} \cdot \left(\frac{11}{911}\right)_{\mathscr{L}} \cdot \left(\frac{31}{911}\right)_{\mathscr{L}} \\ &= (-1)^{\frac{911^2-1}{8}} \cdot (-1) \cdot \left(\frac{911}{11}\right)_{\mathscr{L}} \cdot (-1) \cdot \left(\frac{911}{31}\right)_{\mathscr{L}} \\ &= \left(\frac{9}{11}\right)_{\mathscr{L}} \cdot \left(\frac{12}{31}\right)_{\mathscr{L}} = \left(\frac{3}{31}\right)_{\mathscr{L}} = -\left(\frac{31}{3}\right)_{\mathscr{L}} = -1.\end{aligned}$$

34. a) Vasemman puolen polynomin diskriminantti $6^2 + 4 \cdot 3 \cdot 4 = 84$ on neliönjäännös modulo 43, sillä

$$\left(\frac{84}{43}\right)_{\mathscr{L}} = \left(\frac{-2}{43}\right)_{\mathscr{L}} = \left(\frac{-1}{43}\right)_{\mathscr{L}} \cdot \left(\frac{2}{43}\right)_{\mathscr{L}} = (-1)^{\frac{43-1}{2}} \cdot (-1)^{\frac{43^2-1}{8}} = (-1) \cdot (-1) = 1.$$

Siispä tarkasteltavalla kongruenssilla on kaksi keskenään epäkongruenttia ratkaisua modulo 43. Koska $84 \equiv 256 \equiv 16^2 \pmod{43}$, saadaan ne kongruensseista

$$8x \equiv -6 \pm 16 \pmod{43}.$$

Koska $27 \cdot 8 \equiv 216 \equiv 1 \pmod{43}$, ratkaisuiksi saadaan $x \equiv 27 \cdot 10 \equiv 270 \equiv 12$ ja $x \equiv 27 \cdot (-22) \equiv -594 \equiv 8 \pmod{43}$.

b) Tässä tapauksessa diskrimantti on $8^2 - 4 \cdot 5 \cdot 7 = -76$. Koska tämä on jaollinen luvulla 19, on tarkasteltavalla kongruenssilla yksikäsitteinen ratkaisu, joka saadaan kongruenssista $14x = 8 \pmod{19}$. Kyseinen ratkaisu on $x \equiv 6 \pmod{19}$.

c) Diskriminantti $12^2 - 4 \cdot 5 = 124$ on neliönepäjäännös modulo 73, sillä

$$\begin{aligned}
\left(\frac{124}{73}\right)_{\mathscr{L}} &= \left(\frac{-22}{73}\right)_{\mathscr{L}} = \left(\frac{-1}{73}\right)_{\mathscr{L}} \cdot \left(\frac{2}{73}\right)_{\mathscr{L}} \cdot \left(\frac{11}{73}\right)_{\mathscr{L}} \\
&= (-1)^{\frac{73-1}{2}} \cdot (-1)^{\frac{73^2-1}{8}} \cdot (-1)^{\frac{11-1}{2} \cdot \frac{73-1}{2}} \left(\frac{73}{11}\right)_{\mathscr{L}} \\
&= (+1) \cdot (+1) \cdot (+1) \cdot \left(\frac{7}{11}\right)_{\mathscr{L}} = (-1)^{\frac{7-1}{2} \cdot 11 - 12} \cdot \left(\frac{11}{7}\right)_{\mathscr{L}} \\
&= (-1) \cdot \left(\frac{4}{7}\right)_{\mathscr{L}} = (-1) \cdot (+1) = -1.
\end{aligned}$$

ja siksi ratkaisuita ei ole.

35. Koska $p \equiv 1 \pmod{4}$, on -1 neliönjäännös modulo p ja siis $\left(\frac{a}{p}\right)_{\mathscr{L}} = \left(\frac{-a}{p}\right)_{\mathscr{L}}$ kaikilla $a \in \mathbb{Z}$. Jos siis a on itseisesti positiivinen neliönjäännös modulo p niin $-a$ on itseisesti negatiivinen neliönjäännös modulo p ja päin vastoin.

36. Jos $p = 5$, on kyseinen Legendren symboli yhtä kuin nolla. Oletetaan siis, että $p \neq 5$. Tällöin Eulerin kriteerion nojalla

$$\left(\frac{p}{5}\right)_{\mathscr{L}} \equiv p^2 \pmod{5}.$$

Täten p on neliönjäännös tai neliönepäjäännös sen mukaan, onko p muotoa $10n \pm 1$ vai muotoa $10n \pm 3$ jollakin $n \in \mathbb{Z}$.

37. a) Oletetaan, että alkulukuja, jotka ovat $\equiv 3 \pmod{4}$, olisi vain äärellinen määrä, ja merkitään niiden tuloa kirjaimella P. Tällöin luku $4P - 1$ on $\equiv 3 \pmod{4}$ ja sillä on alkutekijä. Mutta tehtyjen oletusten mukaan jokainen sen alkutekijä on $\equiv 1 \pmod{4}$. Mutta tällöin $4P - 1 \equiv 1 \cdot 1 \cdot \ldots \cdot \ldots \cdot 1 \equiv 1 \pmod{4}$, mikä on mahdotonta.

b) Oletetaan, että olisi vain äärellisen monta alkulukua, jotka ovat $\equiv 1 \pmod{4}$, ja merkiään niiden tuloa kirjaimella P. Tällöin luvulla $4P^2 + 1$ on oltava pariton alkutekijä, mutta neliönjäännösten resiprookkilain ensimmäisen täydennyslauseen nojalla jokaisen sellaisen alkutekijän on oltava $\equiv 1 \pmod{4}$, ristiriita.

38. a) Jos olisi $r \equiv x^2 \pmod{p}$ jollakin $x \in \mathbb{Z}$, kuuluisi luku r pienempään eksponenttiin kuin luku x^2, joka taas vuorostaan varmasti kuuluu eksponenttiin, joka on pienempi kuin $\frac{p-1}{2}$. Tämä on ristiriidassa primitiivisen juuren määritelmän kanssa.

b) Olkoon a neliönjäännös modulo p. Tällöin $a \equiv x^2 \pmod{p}$ jollakin $x \in \mathbb{Z}$, jolla $p \nmid x$. Mutta tällöin myös $x \equiv r^k \pmod{p}$ jollakin $k \in \mathbb{Z}_+$, ja siis $a \equiv x^2 \equiv r^{2k} \pmod{p}$.

39. Tarkastellaan joitakin 30 peräkkäistä kokonaislukua. Enintään yksi niistä on jaollinen alkuluvulla 31. Jos yksi niistä on jaollinen alkuluvulla 31, niin ositettaessa ne kahteen joukkoon toisen elementtien tulo on ja toisen elementtien tulo ei ole jaollinen luvulla 31. Voidaan siis olettaa ettei mikään tarkasteltavista 30 peräkkäisestä luvusta ole jaollinen alkuluvulla 31.

Koska tarkasteltavat luvut muodostavat redusoidun jäännössysteemin modulo 31, on Wilsonin lauseen nojalla tarkasteltavien lukujen tulo kongruentti luvun -1 modulo 31. Jos tarkasteltavat luvut voisi jakaa kahteen joukkoon joiden tulot olisivat yhtäsuuret, olisi -1 neliönjäännös modulo 31, mikä on ristiriita, sillä onhan $31 \equiv -1 \pmod{4}$.

40. Voimme kirjoittaa yhtälön muodossa

$$y^2 + 4 = (x+3)\left(x^2 - 3x + 9\right).$$

Neliönjäännösten resiprookkilain ensimmäisen täydennyslauseen nojalla tämän yhtälön vasemmalla puolella ei voi olla alkulukutekijöitä, jotka olisivat $\equiv 3 \pmod{4}$. Jos $x \not\equiv 0 \pmod{4}$, niin oikean puolen jälkimmäinen tekijä on $\equiv 3 \pmod{4}$, ja koska se on varmasti positiivinen, olisi sillä tässä tapauksessa oltava alkutekijä joka olisi $\equiv 3 \pmod{4}$. Siispä ratkaisuille on pädettävä $4 \mid x$, mutta tällöin oikean puolen ensimmäinen tekijä olisi välttämättä positiivinen ja $\equiv 3 \pmod{4}$, eli sillä olisi oltava alkutekijä, joka olisi $\equiv 3 \pmod{4}$. Täten annetulla Diofantoksen yhtälöllä ei voi olla ratkaisuita.

41. Kiinalaisen jäännöslauseen todistusta seuraten ratkaisemme kongruenssit

$$e_1 \cdot 5 \cdot 7 \equiv 1 \pmod{3}, \quad 3 \cdot e_2 \cdot 7 \equiv 1 \pmod{5}, \quad \text{ja} \quad 3 \cdot 5 \cdot e_3 \equiv 1 \pmod{7}.$$

Näiden ratkaisut ovat

$$e_1 \equiv -1 \pmod{3}, \quad e_2 \equiv 1 \pmod{5}, \quad \text{ja} \quad e_3 \equiv 1 \pmod{7}.$$

Alkuperäisen kongruenssin ratkaisuiksi saadaan siis

$$x \equiv 1 \cdot (-1) \cdot 5 \cdot 7 + 2 \cdot 3 \cdot 1 \cdot 7 + 3 \cdot 3 \cdot 5 \cdot 1 \equiv -35 + 42 + 45 \equiv 52 \pmod{105}.$$

42. Todistamme väitteen induktiolla eksponentin α suhteen. Tapaus $\alpha = 0$ on selvä; onhan jokainen neliö kongruentti yhden luvuista 0, 1 ja 4 kanssa modulo 8. Jos taas $\alpha > 0$ ja väite on jo todistettu pienemmille eksponenteille, niin päättelemme seuraavasti: jos

$$x^2 + y^2 + z^2 = 4^\alpha (8\ell + 7),$$

missä $x, y, z \in \mathbb{Z}$ ja $\ell \in \{0\} \cup \mathbb{Z}_+$, niin $x^2 + y^2 + z^2 \equiv 0 \pmod{4}$, ja koska jokainen neliö on kongruentti toisen luvuista 0 ja 1 kanssa modulo 4, on lukujen x, y ja z oltava parillisia, eli

$$\left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2 = 4^{\alpha-1}(8\ell + 7).$$

43. Olkoon g primitiivinen juuri modulo p^α. Jos g on parillinen, niin $g + p^\alpha$ on pariton primitiivinen juuri modulo p^α, ja voimme siis olettaa, että g on pariton. Nyt

$$\varphi(2p^\alpha) = \varphi(p^\alpha) = \operatorname{ord}_{p^\alpha} g \leqslant \operatorname{ord}_{2p^\alpha} g \leqslant \varphi(2p^\alpha)\,,$$

eli g kuuluu eksponenttiin $\varphi(2p^\alpha)$ modulo $2p^\alpha$ ja olemme valmiit.

44. Olkoot $p_1, p_2, \ldots, p_{2\cdot 10^{100}}$ pareittain erisuuria alkulukuja. Kiinalaisen jäännöslauseen nojalla löytyy luonnollinen luku x, jolle

$$\begin{cases} x \equiv -1 \pmod{p_1 p_2}, \\ x \equiv -2 \pmod{p_3 p_4}, \\ x \equiv -3 \pmod{p_5 p_6}, \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots \\ x \equiv -10^{100} \pmod{p_{2\cdot 10^{100}-1} p_{2\cdot 10^{100}}}. \end{cases}$$

45. Valitaan polynomiksi $P(x)$ polynomi $(2x+1)(3x+1)$, jolla ei tietenkään ole kokonaislukunollakohtia. Olkoon annettu luku $n \in \mathbb{Z}_+$. Kirjoitetaan se muodossa $n = 2^\alpha \ell$, missä $\alpha \in \{0\} \cup \mathbb{Z}_+$ ja $\ell \in \mathbb{Z}_+$ on pariton. Kiinalaisen jäännöslauseen nojalla löytyy $x \in \mathbb{Z}_+$, jolle

$$2x \equiv -1 \pmod{\ell} \quad \text{ja} \quad 3x \equiv -1 \pmod{2^\alpha}.$$

46. Riittää siis osoittaa, että $a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$ aina kun $a \in \mathbb{Z}$ on luvun m kanssa yhteistekijätön.

Jos m ei ole luvun kaksi potenssi, niin $m = bc$ joillakin keskenään yhteistekijättömillä lukua yksi suuremmilla luonnollisilla luvuilla b ja c. Varmasti nyt $\varphi(m) = \varphi(b)\,\varphi(c)$, ja epäilemättä luvut $\varphi(b)$ ja $\varphi(c)$ ovat molemmat parillisia.

Olkoon nyt $a \in \mathbb{Z}$ yhteistekijätön luvun m kanssa. Tällöin

$$a^{\frac{\varphi(m)}{2}} \equiv \left(a^{\frac{\varphi(b)}{2}}\right)^{\varphi(c)} \equiv 1 \pmod{b},$$

ja

$$a^{\frac{\varphi(m)}{2}} \equiv \left(a^{\frac{\varphi(c)}{2}}\right)^{\varphi(b)} \equiv 1 \pmod{c},$$

eli

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}.$$

Tilanne, jossa $m = 2^\alpha$ jollakin kokonaisluvulla $\alpha \geqslant 3$, on oikeastaan helpompi. On helppo tarkistaa, ettei ole olemassa primitiivistä juurta modulo 8. Mutta jos jokin $g \in \mathbb{Z}$ olisi primitiivinen juuri modulo $2^{\alpha+1}$, niin se olisi myös primitiivinen juuri modulo 2^α.

47. a) Jos $x = a^2 + b^2$ joillakin $a, b \in \mathbb{Z}$, niin $2x = (a+b)^2 + (a-b)^2$.

b) Jos $x = a^2 + b^2$ ja $y = c^2 + d^2$ joillakin $a, b, c, d \in \mathbb{Z}$, niin

$$xy = \left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac - bd)^2 + (ad + bc)^2\,.$$

c) Oletetaan, että $q \nmid a$ tai $q \nmid b$. Tällöin varmasti $q \nmid a$ ja $q \nmid b$. Olkoon $c \in \mathbb{Z}$ sellainen, että $bc \equiv -1 \pmod{q}$. Kertomalla kongruenssi $a^2 \equiv -b^2 \pmod{q}$ puolittain luvulla c^2 saadaan $(ac)^2 \equiv -1 \pmod{q}$, mikä on mahdotonta sillä -1 on neliönepäjäännös modulo -1.

d) Koska $2 = 1^2 + 1^2$, on Fermat'n ja Girardin lauseen sekä kohdan b) perusteella jokainen positiivinen kokonaisluku, jonka kaikkia alkulukutekijät ovat kongruentteja lukujen 2 tai 1 kanssa modulo 4, kahden neliön summa. Koska alkuluvuilla q, joilla $q \equiv 3 \pmod 4$, on $q^2 = q^2 + 0^2$, on kohdan b) nojalla kaikki ne positiiviset kokonaisluvut kahden neliön summia, joiden kanonisessa alkutekijähajotelmassa niiden alkulukujen, jotka ovat kongruentteja luvun 3 kanssa modulo 4, potenssien eksponentti on parillinen. Toisaalta, jos positiivinen kokonaisluku n on kahden neliöluvun a^2 ja b^2 summa, ja jos q on sen sellainen tekijä, että $q \equiv 3 \pmod 4$, niin c)-kohdan nojalla $q \mid a$ ja $q \mid b$. Erityisesti siis

$$q \mid \frac{n}{q^2} = \left(\frac{a}{q}\right)^2 + \left(\frac{b}{q}\right)^2 .$$

Jos luvun n kanonisessa tekijähajotelmassa olisi alkulukua q vastaava eksponentti pariton, olisi myös luvun $\frac{n}{q^2}$ tekijähajotelmassa alkuluvun q potenssin eksponentti on edelleen pariton, ja yllä esitettyä c)-kohdan sovellusta voidaan toistaa loputtomiin.

Täten kahden neliöluvun summia ovat täsmälleen luku nolla sekä kaikki ne positiiviset kokonaisluvut, joiden kanonisessa alkutekijähajotelmassa niiden alkulukutekijöiden, jotka ovat kongruentteja luvun kolme kanssa modulo neljä, eksponentit ovat kaikki parillisia.

48. Tarkastelkaamme sitä eksponenttia $\operatorname{ord}_{2^\alpha} 5$, johon luku viisi kuuluu modulo 2^α. Tämän eksponentin on oltava luvun $\varphi(2^\alpha) = 2^{\alpha-1}$ tekijä, eli muotoa 2^β jollakin $\beta \in \{2, 3, \ldots, \alpha - 1\}$. Tehtävän 46 nojalla viisi ei voi olla primitiivinen juuri modulo 2^α, eli $\beta \leqslant \alpha - 2$. Osoitamme, että itse asiassa $\beta = \alpha - 2$.

Tarkastellaan nyt potenssia 5^{2^β}. Kirjoitetaan $5 = 1 + 2^2$. Induktiolla nähdään helposti, että kaikilla $\gamma \in \mathbb{Z}_+$ pätee

$$5^{2^\gamma} = 1 + 2^{\gamma+2}\,(1 + 2\ell)\,,$$

jollakin $\ell \in \mathbb{Z}_+$. Erityisesti siis

$$5^{2^\beta} = 1 + 2^{\beta+2}k,$$

jollakin parittomalla $k \in \mathbb{Z}_+$. Koska on oltava $2^\alpha \mid \left(5^{2^\beta} - 1\right)$, on oltava $\beta \geqslant \alpha - 2$. Yhdistämällä tämä aiempiin havaintoihin saadaan $\beta = \alpha - 2$.

Nyt luvut

$$1, \quad 5, \quad 5^2, \quad 5^3, \quad \ldots, \quad 5^{2^{\alpha-2}-1}$$

ovat $\frac{\varphi(2^\alpha)}{2}$ pareittain epäkongruenttia lukua modulo 2^α. Samoin

$$-1, \quad -5, \quad -5^2, \quad -5^3, \quad \ldots, \quad -5^{2^{\alpha-2}-1}$$

ovat $\frac{\varphi(2^\alpha)}{2}$ pareittain epäkongruenttia lukua modulo 2^α. Koska edelliset ovat kaikki $\equiv 1 \pmod 4$ ja jälkimmäiset $\equiv 3 \pmod 4$, ovat kyseiset luvut yhteensä $\varphi(2^\alpha)$ pareittain epäkongruenttia lukua modulo 2^α. Olemme nyt valmiit, lukuunottamatta merkkiä $(-1)^{\frac{n-1}{2}}$, joka on helppo tarkistaa.

49. a) $4 = -(1+i)^4$.

b) Luku 103 on alkuluku, ja koska se on $\equiv 3 \pmod 4$, on se myös Gaussin alkuluku. Siis kysytty alkutekijähajotelma on $103 + 103i = (1+i)\,103$.

c) Osoittautuu, että luku 2011 on alkuluku, ja koska se on $\equiv 3 \pmod 4$, on sen oltava myös Gaussin alkuluku.

d) Luvun $11 + 23i$ normi on $11^2 + 23^2 = 650 = 2 \cdot 5^2 \cdot 13$. Tekijän 13 vuoksi on hyvä kokeilla alkutekijöiksi Gaussin alkulukuja $2 \pm 3i$. Suoralla laskulla

$$\frac{11+23i}{2+3i} = 7 + i.$$

Luku $7 + i$ on jaollinen luvulla $1 + i$, sillä

$$\frac{7+i}{1+i} = 4 - 3i.$$

Lopuksi, tekijän 5^2 vuoksi on hyvä kokeilla alkutekijöiksi Gaussin alkulukuja $2 \pm i$. Osoittautuu, että $4 - 3i = -i\,(2+i)^2$.

Kysytyksi alkutekijähajotelmaksi saadaan siis

$$11 + 23i = -i\,(1+i)(2+i)^2\,(2+3i)\,.$$

50. Lasketaan ensin

$$\frac{11+23i}{7+2i} = \frac{11+23i}{7+2i} \cdot \frac{7-2i}{7-2i} = \frac{77+46+(161-22)\,i}{53} = \frac{123+139i}{53} = 2 + \frac{17}{53} + 2i + \frac{33i}{53}.$$

Luvuksi κ kelpaavat siis korkeintaan luvut $2+2i$, $2+3i$, $3+2i$ ja $3+3i$.

Lasketaan seuraavaksi:

$$\begin{cases} (7+2i)(2+2i) = 10+18i = 11+23i-(1+5i)\,, \\ (7+2i)(2+3i) = 8+25i = 11+23i-(3-2i)\,, \\ (7+2i)(3+2i) = 17+20i = 11+23i-(-6+3i)\,, \\ (7+2i)(3+3i) = 15+27i = 11+23i-(-4-4i)\,. \end{cases}$$

Koska $N(1+5i) = 26 < 53 = N(7+2i)$, $N(3-2i) = 13 < 53$, $N(-6+3i) = 45 < 53$ ja $N(-4-4i) = 32 < 53$, ovat kaikki neljä yhtälöä kelvollisia jakoyhtälöitä. Siis lukupariksi $\langle \kappa, \rho \rangle$ kelpaavat

$$\langle 2+2i, 1+5i \rangle\,, \quad \langle 2+3i, 3-2i \rangle\,, \quad \langle 3+2i, -6+3i \rangle\,, \quad \text{sekä} \quad \langle 3+3i, -4-4i \rangle\,.$$

51. Aloitetaan kirjoittamalla jakoyhtälöt

$$\begin{cases} 11+23i = (2+3i)(7+2i)+3-2i \\ 7+2i = (1+2i)(3-2i)-2i \\ 3-2i = (1+i)(-2i)+1 \end{cases}$$

Näistä saadaan, että

$$\begin{cases} 3-2i = 11+23i-(2+3i)(7+2i)\,, \quad \text{ja} \\ -2i = 7+2i-(1+2i)\big(11+23i-\,(2+3i)(7+2i)\big) \\ \qquad\quad = (-3+7i)(7+2i)-(1+2i)(11+23i)\,, \end{cases}$$

ja edelleen, että

$$\begin{aligned} 1 &= 11+23i-(2+3i)(7+2i)-(1+i)\big((-3+7i)(7+2i)-\,(1+2i)(11+23i)\big) \\ &= 3i\,(11+23i)-(-8+7i)(7+2i)\,. \end{aligned}$$

52. Koska

$$\frac{x+yi}{1+i} = \frac{x+yi}{1+i} \cdot \frac{1-i}{1-i} = \frac{x+y-(x-y)\,i}{2},$$

on $(1+i) \mid (x+yi)$ täsmälleen silloin, kun $2 \mid (x \pm y)$, eli täsmälleen silloin kun $x \equiv y \pmod 2$.

53. Annetuista relaatioista jälkimmäisestä seuraa, että $\overline{\pi} \mid \alpha$. Koska $\pi \not\sim \overline{\pi}$, seuraa jaollisuuksista $\pi \mid \alpha$ ja $\overline{\pi} \mid \alpha$, että $N\pi = \pi\overline{\pi} \mid \alpha$.

54. Olkoon p se yksikäsitteinen tavallinen alkuluku, jonka π jakaa. Jaamme todistuksen kolmeen eri tapaukseen Gaussin alkulukujen luokittelun mukaan, eli sen mukaan, onko $p \equiv 1$, $\equiv 2$ vai $\equiv 3 \pmod 4$.

Olkoon ensin $p \equiv 2 \pmod 4$. Tällöin $\pi \sim (1+i)$. Voimme tietysti olettaa, että $\pi = 1+i$. Pitää siis todistaa, että $\alpha \equiv 1 \pmod{1+i}$. Jakoyhtälön nojalla löytyy luvut $\kappa, \rho \in \mathbb{Z}[i]$, joille

$$\alpha = \kappa\,(1+i) + \rho \quad \text{ja} \quad N\rho < 2.$$

Tietysti $N\rho > 0$, ja luvun ρ täytyy olla yksikkö, eli $\rho \in \{\pm 1, \pm i\}$. Nyt

$$\alpha \equiv -\rho \pmod{1+i},$$

ja väite seuraa siitä, että luvut ± 1 ja $\pm i$ ovat kaikki keskenään kongruentteja modulo $1+i$.

Olkoon seuraavaksi $p \equiv 1 \pmod 4$. Kongruenssi

$$(\beta+\gamma)^p \equiv \beta^p + \gamma^p \pmod p$$

pätee, paitsi tavallisille kokonaisluvuille, myös mielivaltaisille Gaussin kokonaisluvuille β ja γ. Kirjoitetaan $\alpha = x+yi$, missä $x, y \in \mathbb{Z}$. Nyt

$$\alpha^p \equiv x^p + i^p y^p \equiv x + iy \equiv \alpha \pmod p,$$

missä $i^p \equiv i \pmod p$ koska $p \equiv 1 \pmod 4$. Tästä seuraa, että $\pi \mid \alpha\left(\alpha^{p-1} - 1\right)$, ja koska $\pi \nmid \alpha$, edelleen, että $\pi \mid \left(\alpha^{p-1} - 1\right)$, mikä onkin haluttu johtopäätös, sillä $N\pi = p$.

Olkoon lopuksi $p \equiv 3 \pmod 4$. Samassa hengessä kuin aiemmin, voimme päätellä, että

$$\alpha^p \equiv x^p + i^p y^p \equiv x - iy \equiv \overline{\alpha} \pmod p,$$

missä $i^p \equiv -i \pmod p$, koska $p \equiv 3 \pmod 4$. Nyt

$$\alpha^{p^2} \equiv \overline{\alpha^p} \equiv \alpha \pmod p,$$

eli $\pi \mid \alpha\left(\alpha^{p^2-1} - 1\right)$, ja jälleen, koska $\pi \nmid \alpha$, on oltava $\pi \mid \left(\alpha^{p^2-1} - 1\right)$, mikä on haluttu tulos, sillä $N\pi = p^2$.

55. Annettu yhtälö voidaan kirjoittaa muodossa

$$(2+xi)(2-xi) = y^3.$$

Tässä vasemman puolen tekijät ovat keskenään yhteistekijättömät. Nimittäin, jos $\delta \in \mathbb{Z}[i]$ jakaa molemmat, niin $\delta \mid 4 = -(1+i)^4$, eli luvun δ täytyy olla

yksiköllä kertomista vaille Gaussin alkuluvun $1+i$ potenssi. Mutta $1+i$ ei jaa kumpaakaan luvuista $2+xi$, sillä $2 \not\equiv x \pmod 2$. (Vrt. teht. 52.)

Siten $2+xi = \varepsilon\,(a+bi)^3$ jollakin yksiköllä ε ja joillakin $a, b \in \mathbb{Z}$. Koska $\pm 1 = (\pm 1)^3$ ja $\pm i = (\mp i)^3$, voi yksikön ε sisällyttää kuutioon, eli itse asiassa voimme olettaa, että

$$2+xi = (a+bi)^3 = a^3 - 3ab^2 + \left(3a^2b - b^3\right) i.$$

Samaistamalla reaaliosat saadaan, että

$$a^3 - 3ab^2 = 2, \quad \text{ja siis} \quad a \in \{\pm 1, \pm 2\}\,.$$

Jos olisi $a = 1$, niin olisi $1 - 3b^2 = 2$, eli $3b^2 = 1$, mikä on mahdotonta.

Jos olisi $a = -1$, niin olisi $1 - 3b^2 = -2$, eli $3b^2 = 3$, eli $b = \pm 1$. Tässä tapauksessa olisi siis myös $x = 3a^2b - b^3 = \pm 2$, mikä ei käy, sillä luvun x on oltava pariton.

Jos $a = 2$, niin $4 - 3b^2 = 1$, eli $b = \pm 1$. Tässä tapauksessa $x = 3a^2b - b^3 = \pm 11$, ja edelleen yhtälöstä $y^3 = x^2 + 4$ saadaan $y^3 = 125 = 5^3$.

Jos olisi $a = -2$, niin olisi $4 - 3b^2 = -1$, eli $3b^2 = 5$, mikä on mahdotonta.

Annetun yhtälön ainoat ratkaisut ovat täten $x = \pm 11$, $y = 5$.

56. Vasen puoli jakautuu tekijöiden $x \pm i$ tuloksi. Koska luku x on varmasti pariton, on näillä tekijöillä yhteisenä tekijänä $1+i$. Toisaalta, niiden yhteinen tekijä jakaa luvun $2i$, eli myös luvun $(1+i)^2$, ja neliö $(1+i)^2$ ei voi jakaa kumpaakaan tekijää koska tällöin myös luku kaksi jakaisi kyseisen tekijän, mikä ei käy imaginaariosien $\pm i$ takia.

Siis lukujen $x \pm i$ ainoa yhteinen tekijä on $1+i$, eli voimme kirjoittaa

$$x + i = (1+i)(a+bi)^3\,,$$

missä $a, b \in \mathbb{Z}$. Tässä mahdollisesti esiintyvä on yksikkö on jälleen sisällytetty kuutioon, kuten edellisenkin tehtävän ratkaisussa.

Imaginaariosat samaistamalla saadaan, että

$$1 = a^3 + 3a^2b - 3ab^2 - b^3 = (a-b)\left(a^2 + 4ab + b^2\right).$$

Siten

$$\text{joko} \quad \begin{cases} a - b = 1, \\ a^2 + 4ab + b^2 = 1, \end{cases} \qquad \text{tai} \quad \begin{cases} a - b = -1, \\ a^2 + 4ab + b^2 = -1. \end{cases}$$

Jälkimmäinen yhtälöpari johtaa ristiriitaan, sillä aina

$$a^2 + 4ab + b^2 = (a+2b)^2 - 3b^2 \equiv 0 \text{ tai } 1 \pmod 3.$$

Ensimmäisestä yhtälöparista seuraa, että $b = a - 1$, eli

$$1 = a^2 + 4ab + b^2 = 6a^2 - 6a + 1,$$

eli $a^2 = a$, eli $a = 1$ tai $a = 0$. Ensimmäisen yhtälöparin ratkaisut ovat siis $\langle a, b\rangle \in \{\langle 1, 0\rangle\,, \langle 0, -1\rangle\}$.

Samaistamalla lopuksi yllä mainitussa luvun $x + i$ lausekkeessa reaaliosat saadaan

$$x = a^3 - 3ab^2 - 3a^2b + b^3,$$

mistä saadaan luvulle x ainoiksi mahdollisiksi arvoiksi ± 1. Näillä arvoilla saadaan kaksi ratkaisua, joille molemmille $y = 1$.

Ainoat ratkaisut ovat siis $x = \pm 1$ ja $y = 1$.