Merkintöjä

$\mathbb{N} = \{1,2,3,\dots\}$ (luonnolliset luvut)
$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ (kokonaisluvut)

1. JAOLLISUUS, ALKUTEKIJÖIHIN JAKO JA S.Y.T.

Määr. Olk. $a, b \in \mathbb{Z}$. Luku a *jakaa* luvun b (eli a on b:n *tekijä*) jos
$b = ka$, missä $k \in \mathbb{Z}$.
Tällöin merkitään $a \mid b$.

Esim. $3 \mid 6$, $0 \mid 0$, $2 \nmid 5$ ('ei jaa'), $81 \mid 124$, $7 \nmid 47$.

Huom. jatkossa $a, b, \dots, x, y, \dots$ ovat aina kokonaislukuja ellei toisin mainita!

Lause 1.1 (i) jos $c \mid b$ ja $b \mid a$, niin $c \mid a$.

(ii) jos $a \mid b \Rightarrow a \mid bc$ kaikilla c

(iii) jos $a \mid b_1, \dots, a \mid b_n \Rightarrow a \mid (b_1 + \dots + b_n)$

Tod. HT

Määr. Jos $p \in \mathbb{N}$, $p \geq 2$ ja ehdosta $k \mid p$, $k \in \mathbb{N}$ seuraa $k \in \{1, p\}$, sanomme että p on alkuluku. Merkitään $p \in P$. Siis

$$P = \{2, 3, 5, 7, \dots\}$$

Määr. Luvut $m \geq 2$, $m \notin P$, ovat yhdistettyjä lukuja.

[Lause 1.2. Jokainen luonnollinen luku (≥ 2) on esitettävissä alkulukujen tulona.

Tod. Vastaoletus: olkoon n pienin kokonaisluku, $n > 1$, jota ei voi esittää alkulukujen tulona. Erityisesti $n \notin P$, joten $n = n_1 n_2$, missä $n_1, n_2 > 1$. Nyt n_1 ja n_2 ovat alkulukujen tuloja, joten n on myös. ↯ ← ristiriidan merkki! □

[Lause 1.3 (Euklides, n. 300 e.a.a) On olemassa ääretön monta alkulukua.

Tod. Vastaoletus: $P = \{p_1, p_2, \ldots, p_k\}$.
Merk. $m = p_1 p_2 \cdots p_k + 1$.
Silloin $p_j \nmid m$, $1 \leq j \leq k$. Lauseen 1.2 nojalla on olemassa $p \in P$ jolle $p \mid m$, mikä on mahdotonta. ↯ □

[Lause 1.4. (jakojäännöslause) Olkoon $b \geq 1$ ja $a \in \mathbb{Z}$. Silloin on olemassa yksikäs. luvut $q, r \in \mathbb{Z}$ joille $a = qb + r$, $0 \leq r < b$.

Tod. Merkitään

$$U = \{a - ub \mid a - ub \geq 0,\ u \in \mathbb{Z}\}$$

Selvästi U on epätyhjä (miksi?) Olkoon r joukon U pienin alkio, ja kirjoitetaan $r = a - u_1 b$. Siis $r \geq 0$. Jos $r \geq b$, niin

$$a - (u_1 + 1)b = r - b \geq 0,$$

mikä on vastoin r:n määritelmää. Siis $0 \leq r < b$ ja voimme valita $q = u_1$.

Yksikäsitteisyys: jos $0 \le r_1, r_2 < b$, ja
$r_1 = a - u_1 b$, $r_2 = a - u_2 b$, niin

$b \mid (r_1 - r_2)$. Jos $r_1 \neq r_2$, tästä seuraa $|r_1 - r_2| \ge b$, mikä ei ole mahdollista koska $-b < r_1 - r_2 < b$. □

Seuraava tulos voi tuntua ilmeiseltä, mutta kun asiaa mietti tarkasti (tee se!), se osoittautuukin varsin syvälliseksi havainnoksi.

Lause 1.5. Olkoon $a \neq 0$ tai $b \neq 0$. On olemassa 1-käsitteinen kokonaisluku d (lukujen a ja b 'suurin yhteinen tekijä'), jolle pätee:
(i) $d \mid a$ ja $d \mid b$
(ii) jos $d' \mid a$ ja $d' \mid b$ $\Rightarrow$ $d' \mid d$
(iii) $d \ge 1$

Tod. Määritellään suoraan

(1) $$d = \min\{ax + by \mid ax + by \ge 1,\ x, y \in \mathbb{Z}\},$$

eli d on lukujoukon $\{ax + by \mid x, y \in \mathbb{Z}\}$ (selvästi epätyhjän) pienin positiivinen alkio.
Olkoon $d = ax_0 + by_0$ jollakin $x_0, y_0 \in \mathbb{Z}$.
Selvästi d toteuttaa ehdot (iii) ja (i) (mikä jälkimmäinen?). Ehdon (i) todistamiseksi oletetaan, että $d \nmid a$. Silloin jakojäännöslauseen nojalla $a = dq + r$, $0 < r < d$. Saadaan

$$1 \le r = a - dq = a(1 - qx_0) + b(-qy_0) < d,$$

mikä on vastoin d:n määritelmää. Siis $d \mid a$ ja vastaavasti näytetään, että $d \mid b$.

Yksikäsitteisyys seuraa ehdoista (i) ja (ii):
jos d_1 ja d_2 toteuttavat (i)–(iii), niin
$d_1, d_2 \ge 1$, $d_1 \mid d_2$ ja $d_2 \mid d_1 \Rightarrow d_1 = d_2$. □

Määr. • a:n ja b:n suurinta yhteistä tekijää merkitään s.y.t(a,b), tai yksinkertaisemmin (a,b).

• jos $(a,b)=1$ ovat a ja b *suhteellisia alkulukuja* (eli keskenään jaottomia).

Seuraus 1.6. Olkoon $a \neq 0$ tai $b \neq 0$ ja $d=(a,b)$. Silloin

(i) $d = x_0 a + y_0 b$ joillakin $x_0, y_0 \in \mathbb{Z}$.

(ii) $\{xa+yb \mid x,y \in \mathbb{Z}\} = \{kd \mid k \in \mathbb{Z}\}$

Tod. (i) seuraa suoraan määritelmästä (1) s. 5.

(ii) Edellisen kohdan nojalla "vasen puoli" $\supset$ "oikea puoli". Toinen suunta seuraa lauseen 1.5 kohdasta (i). □

Esim. $(8,22)=2$, $2 = -8\times 8 + 3\times 22$.

Seuraus 1.7. Jos $a \mid bc$ ja $(a,b)=1$, niin $a \mid c$

Tod. Seur. 1.6 $\Rightarrow \exists x_0, y_0$ joille $1 = x_0 a + y_0 b$. Nyt $c = acx_0 + bcy_0$, ja tässä $a \mid acx_0$ ja $a \mid bcy_0$. □

Seuraus 1.8. Jos $p \in P$ ja $p \mid ab$, niin $p \mid a$ tai $p \mid b$.

Tod. Ilmeinen. □

Induktiolla seuraa edellisestä (HT):

jos $p \mid q_1 \cdots q_k \Rightarrow p \mid q_j$ jollakin j.

[**Seuraus 1.9.** Jos $p \mid q_1 \cdots q_k$, $p, q_1, \ldots, q_k \in P$, niin $p = q_j$ jollakin $1 \le j \le k$.

Tod. Nyt $p \mid q_j \Leftrightarrow p = q_j$ koska $p, q_j \in P$. □

Olemme nyt valmiit todistamaan aritmetiikan peruslauseen:

[**Lause 1.10.** (Alkutekijöihin jaon 1-käsitteisyys) Jokainen positiivinen kokonaisluku $n \ge 2$ voidaan kirjoittaa muodossa

$$n = p_1 p_2 \cdots p_r \quad , \quad r \ge 1 \, ,$$

missä $p_1, \ldots, p_r \in P$ ja esitys on 1-käsitteinen tekijöiden järjestystä lukuunottamatta.

Tod. Lauseen 1.2 nojalla jokainen $n \ge 2$ voidaan esittää alkulukujen tulona. Olkoon $n \ge 2$ pienin luku jolla on <u>eri</u> esitykset

$$n = \prod_{j=1}^{m} p_j^{\alpha_j} = \prod_{j=1}^{m} p_j^{\beta_j} \quad , \quad \alpha_j, \beta_j \ge 0$$

(Tässä $p_1, \ldots, p_m$ ovat eri alkulukuja – ne jotka esiintyvät jommassa kummassa esityksessä. Huomaa, että α_j:t ja β_j:t voivat saada arvon nolla). Olkoon esim. $\alpha_1 \ge \beta_1$. Tällöin $\beta_1 = 0$, koska muuten $n / p_1^{\beta_1}$ olisi pienempi luku jolla on kaksi eri esitystä. Tällöin

$$p_1 \mid \prod_{j=2}^{m} p_j^{\beta_j} \, ,$$

mikä on mahdotonta seuraus 9:n nojalla koska $p_j \ne p_1$ kun $j \ge 2$.

Määr. Olkoot $a_1, \dots, a_n$ kokonaislukuja (eivät kaikki nollia). Silloin

$$d = s.y.t.(a_1, \dots, a_n) = (a_1, \dots, a_n)$$

on se 1-käsitteinen kokonaisluku, jolle

(i) $d \mid a_k$ kun $k = 1, \dots, n$

(ii) jos $d' \mid a_k$ kun $k = 1, \dots, n$, niin $d' \mid d$

(iii) $d > 0$.

$s.y.t.(a_1, \dots, a_n)$:n olemassaolo on HT.

Aritmetiikan peruslauseen nojalla jokainen $n \in \mathbb{N}$ voidaan kirjoittaa yksikäsitteisesti muotoon

$$n = \prod_{k=1}^{\infty} p_k^{\alpha_k}, \quad \alpha_k \geq 0,$$

missä $p_1 = 2, p_2 = 3, p_3 = 5, \dots$ ovat alkuluvut kasvavassa järjestyksessä ja $\alpha_k = \alpha_k(n) = 0$ suurilla k. Jos $m = \prod_{k=1}^{\infty} p_k^{\beta_k}$, niin (HT)

$$(n, m) = \prod_{k=1}^{\infty} p_k^{\gamma_k}, \text{ missä } \gamma_k = \min(\alpha_k, \beta_k).$$

Lause 1.11 Olk. $a, b \geq 1$. On olemassa luku

$$h = p.y.j.(a, b) \quad (\text{'pienin yhteinen jaettava'})$$

jolle

(i) $a \mid h$, $b \mid h$

(ii) $a \mid h'$, $b \mid h' \Rightarrow h \mid h'$

(iii) $h \geq 1$

Tod. HT.

Huom. Pätee kaava $p.y.j.(a, b) = \dfrac{ab}{(a, b)}$ (HT).

Sovellus: 2. muuttujan lineaarinen Diofantoksen yhtälö

Lause 1.12. Olkoon $a \neq 0$ tai $b \neq 0$. Yhtälöllä

$$ax + by = c$$

on kokonaisratkaisu jos ja vain jos $d \mid c$, missä $d = (a,b)$. Jos (x_0, y_0) on jokin ratkaisu, kaikki ratkaisut saadaan kaavasta

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases}, \quad t \in \mathbb{Z}.$$

Tod. Jos ratkaisu on olemassa, selvää suoraan yhtälöstä, että $d \mid c$. Käänteen, jos $d \mid c$, voimme jakaa yhtälön kertoimet d:llä, eli yhtäpitävästi

$$a'x + b'y = c',$$

missä $a' = a/d$, $b' = b/d$ ja $c' = c/d$. Tällöin $(a', b') = 1$ (HT). Riittää siis tarkastella tapausta $d = 1$.

Oletetaan, että $d = 1$. Seurauksen 1.6 nojalla on olemassa x_1, y_1 joille $ax_1 + by_1 = 1$. Silloin $acx_1 + bcy_1 = c$, eli pari x_0, y_0 on ratkaisu kun valitaan $x_0 = cx_1$, $y_0 = cy_1$. Olkoon x, y toinen ratkaisu. Silloin

$$ax + by = ax_0 + by_0,$$

eli $a(x - x_0) = -b(y - y_0)$. Koska $(a,b) = 1$ seuraa tästä (Seur. 1.7) $b \mid (x - x_0)$, eli $x = x_0 + tb$ jollakin $t \in \mathbb{Z}$. Tällöin $y = y_0 - ta$. Käänteen, tällaiset parit toteuttavat aina yhtälön. □

Edellisen lauseen antaa ratkaisun teoriassa. Miten käytännössä ratkaisemme vaikkapa yhtälön

$$127x - 87y = 1.$$

Yksi mahdollisuus on kokeilla x:n paikalle luvut $1, 2, \ldots, 87$ ja katsoa milloin yhtälö tulee tosiseksi (mieti miksi riittää kokeilla näin?). Nopeamman ratkaisun pääsee soveltamalla (myös teoreettisesti tärkeää) Euklideen algoritmia:

EUKLEIDEEN ALGORITMI (a, b):n etsimiseksi: Kirjoitetaan jakojäännöslauseen nojalla peräkkäin (oletamme $a > b \geq 1$)

$$\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < b \\
b &= r_1 q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2 \\
&\vdots & \vdots \\
r_{k-2} &= r_{k-1} q_k + r_k, & 0 < r_k < r_{k-1} \\
r_{k-1} &= q_{k+1} r_k & \text{(jako menee taas ensimmäisen kerran)}
\end{aligned}$$

[Lause 1.13 $r_k = (a, b)$.

Tod Viim. yht. $\Rightarrow$ $r_k \mid r_{k-1}$, jolloin

2. viim. yht $\Rightarrow$ $r_k \mid r_{k-2}$,

3. viim. yht $\Rightarrow$ $r_k \mid r_{k-3}$,

$\vdots$

2. yhtälö $\Rightarrow$ $r_k \mid b$

1. yhtälö $\Rightarrow$ $r_k \mid a$.

Käänteen, jos $d=(a,b)$, niin

1. yht. $\Rightarrow d \mid r_1$, 2. yht. $\Rightarrow d \mid r_2$,
..., 2. viim. yhtälö $\Rightarrow d \mid r_k$.

Siis $r_k \mid a$, $r_k \mid b$ ja $d \mid r_k$, $r_k \geq 1$, eli $r_k = d$. □

Euklideen algoritmia voi myös soveltaa yhtälön $ax+by=d=(a,b)$ ratkaisemiseen:

1. yht. $\Rightarrow r_1 = a - bq_1 \overset{\text{merk.}}{=} u_1 a + v_1 b$

2. yht. $\Rightarrow r_2 = b - q_2(u_1 a + v_1 b) = u_2 a + v_2 b$

$\vdots$ $\qquad\qquad\qquad\qquad\qquad\qquad$ $\vdots$

2. viim yht. $\Rightarrow d = r_k = r_{k-2} - r_{k-1} q_k$

$= (u_{k-2} a + v_{k-2} b) - q_k (u_{k-1} a + v_{k-1} b)$

$= x_0 a + y_0 b$.

Tietenkään käytännössä ei tarvitse harrastaa yo. kompleksia notaatiota.

Esim. $(127,87)=1$. Tarkistetaan tämä Euklideen algoritmin avulla:

$$127 = 87 \cdot 1 + 40 \quad , \quad 87 = 40 \cdot 2 + 7$$
$$40 = 7 \cdot 5 + 5 \quad , \quad 7 = 5 \cdot 1 + 2$$
$$5 = 2 \cdot 2 + 1 \quad ; \quad (127,87) = 1.$$

Ratkaistaan sitten yhtälö $127x - 87y = 1$ (vrt. s. 10.). Merkitään $127=a$ ja $87=b$ ja ratkaistaan peräkkäin:

$40 = a - b$, $\quad 7 = b - 2(a-b) = 3b - 2a$,

$5 = (a-b) - 5(3b-2a) = 11a - 16b$

$2 = (3b-2a) - (11a-16b) = 18b - 13a$

$1 = (11a-16b) - 2(18b-13a) = \underline{37a - 54b}$

Löysimme ratkaisun $(x_0, y_0) = (+37, +54)$, jolloin yhtälön $127x - 87y = 1$ yleinen ratkaisu on

$$\begin{cases} x = 37 + k87 \\ y = 54 + k127 \end{cases}, \quad k \in \mathbb{Z}.$$

Eukleideen algoritmi voi vaikuttaa kömpelöltä, mutta itseasiassa se on varsin tehokas suurilla luvuilla:

Lause 1.14 Eukleideen algoritmin tarvitsema askelmäärä $\leq 3 \log a + 2$ (kun $a \geq b$)

Tod. HT □

(2) KONGRUENSSIT JA RENGAS $\mathbb{Z}_m$.

Gauss otti käyttöön kongruenssin käsitteen. Se helpottaa huomattavasti jaollisuustarkasteluja.

Määr. Olkoon $m \neq 0$. Jos $m \mid (a-b)$, sanomme että a on kongruentti b:n kanssa modulo m. Merkitsemme tällöin $a \equiv b \pmod{m}$.
('modoli')

Huom. Lyhyesti sanoen siis
$$a \equiv b \pmod{m} \iff m \mid (a-b).$$

Seuraava havainto osoittaa, että $\equiv$ on ekvivalenssirelaatio!

Lause 2.1. Kongruenssi (mod m) toteuttaa:
(i) $a \equiv a \pmod{m}$
(ii) $a \equiv b \iff b \equiv a \pmod{m}$
(iii) $a \equiv b$ ja $b \equiv c \Rightarrow a \equiv c \pmod{m}$.

Tod. Seuraa suoraan määritelmästä.

Seuraavat kolme lausetta sisältävät kongruenssien peruslaskusäännöt:

Lause 2.2. (i) Jos $a \equiv b \pmod{m}$, niin kaikilla k pätee $a+k \equiv b+k$ ja $ka \equiv kb \pmod{m}$
(ii) Jos $a \equiv b$ ja $c \equiv d \pmod{m}$, niin
$a+c \equiv b+d \pmod{m}$ ja $ac \equiv bd \pmod{m}$

Tod. Seuraava helposti määritelmästä (tee!), viimeistä väitettä varten on hyödyllistä havaita $ac - bd = a(c-d) + d(a-b)$. □

Lause 2.3. Jos $P(x)$ on kokonaiskertoiminen polynomi, niin $a \equiv b \pmod m \Rightarrow P(a) \equiv P(b) \pmod m$.

Tod. Olkoon $P(x) = a_0 + a_1 x + \dots + a_n x^n$.
Iteroimalla edellistä lausetta saamme
$a^k \equiv b^k \pmod m$ kaikilla $k \geq 0$.

Erityisesti $a_j a^k \equiv a_j b^k \pmod m$, $k = 0, 1, \dots, n$.
Väite seuraa summaamalla yli $k:n$, $k = 0, 1, \dots, n$. □

Vastaavanti todistetaan:

Lause 2.4. Jos P on $k:n$ muuttujan kokonaiskertoiminen polynomi, niin

$$P(x_1, \dots, x_k) \equiv P(y_1, \dots, y_k) \pmod m$$

mikäli $x_j \equiv y_j \pmod m$ kun $j = 1, \dots, k$.

Esim. $7 \equiv -13 \pmod{20}$
$200 \equiv -10 \pmod 3$

Esim Osoita, että luku
$n = 52(169^9 + 87^7) + 6$ on jaollinen luvulla 11.

Ratk. $169 \equiv 4 \pmod{11}$, $52 \equiv 8 \pmod{11}$,
$87 \equiv -1 \pmod{11}$.

Lisäksi

$4^2 = 16 \equiv 5$, $4^4 = 5^2 \equiv 3$, $4^8 \equiv 3^2 = 9 \pmod{11}$,
sitten $4^9 \equiv 36 \equiv 3 \pmod{11}$. — Saamme

$$n \equiv 8 - (3 + (-1)^7) + 6 = 8 - 2 + 6 = 22 \equiv 0 \pmod{11}. \quad \square$$

Huom. Laskettaessa $a^k \equiv ? \pmod{m}$, on edullista laskea ensin peräkkäisten suureet a^1, a^2, a^4, a^8 jne ja lausua annettu potenssi näiden tulona. Esim.

$$a^{23} = a^{16} \cdot a^4 \cdot a^2 \cdot a^1.$$

Esim. Patee $10 \equiv 1 \pmod{9}$, jotenkin jos

$S(n) :=$ luvun n numeroiden summa, niin

saamme $9 \mid n \iff 9 \mid S(n) \iff 9 \mid S(S(n))$ jne..

Esim. Olkoon $n = 5476289$. Silloin
$S(n) = 5+4+7+6+2+8+9 = 41$, $S(S(n)) = 5 \not\equiv 0 \pmod{9}$,
jotenkin $9 \nmid n$.

Määr. Jos $a \equiv b$ ei ole voimassa, merkitsemme
$a \not\equiv b \pmod{m}$.

Lyhyt kertaus: Ryhmät, renkaat, kunnat

'kaltaialkio'

Määr. $(S, \circ)$ on ryhmä jos laskutoimitus $\circ$ toteuttaa ($\circ : S \times S \to S$, merkitään $\circ(a,b) = a \circ b$):

(1) $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in S$. (assosiatiivisuus)

(2) $\exists e \in S$ jolle $a \circ e = e \circ a = a \quad \forall a \in S$.

(3) Jokaiselle $a \in S$ on 'käänteisalkio' $\bar{a} \in S$, jolle $\bar{a} \circ a = a \circ \bar{a} = e$.

Huom. Jos (1) ja (2) voimassa, kyseessä monoidi

Esim (i) $\mathbb{Z}$ (tai $\mathbb{Q}$ tai $\mathbb{R}$) ovat ryhmiä luonnol. lisäyslaskun suhteen.

(ii) $\mathbb{Q} \setminus \{0\}$ on ryhmä kun laskutoimituksena on tavallinen kertolasku.

(iii) $(\{0,1\}, \oplus)$ on kahden alkion ryhmä kun määritellään

$\oplus$	0	1
0	0	1
1	1	0

Määr. $(S,\circ)$ on vaihdannainen (= kommutatiivinen, Abel) ryhmä jos
$$a \circ b = b \circ a \quad \forall\ a,b \in S.$$
← kaksiargumenttinen laskutoimitus

Määr. $(S, +, \cdot)$ on kommutatiivinen rengas, jos

(1) $(S,+)$ on kommutatiivinen ryhmä (merkitään sen neutraalialkiota 0:lla)

(2) $(S,\cdot)$ on kommutatiivinen monoidi (merkitään neutraalialkiota 1:llä)

(3) $1 \neq 0$

(4) $a(b+c) = ab + ac \quad \forall\ a,b,c \in S$ (liitännäisyys)

Määr. $(S,+,\cdot)$ on kunta jos se on kommutatiivinen rengas ja $(S \setminus \{0\}, \cdot)$ on ryhmä (eli jokaisella alkiolla $a \neq 0$ on käänteisalkio laskutoimituksen $\cdot$ suhteen)

Määr. Kommutatiivinen rengas on kokonaisalue jos $ab=0 \Rightarrow a=0$ tai $b=0$.

(Huom. jokainen kunta on kokonaisalue (miksi?))

Esim. $\mathbb{Z}$ on rengas, $\mathbb{Q}$ ja $\mathbb{R}$ (luonnollisilla laskutoimituksilla) ovat kuntia.

Esim. $(\{a,b\}, \oplus, \odot)$ on kunta jos (HT)

$\oplus$	a	b
a	a	b
b	b	a

$\odot$	a	b
a	a	a
b	a	b

($\oplus$:n neutraalialkio on a
$\odot$:n — " — on b)

Meille riittää hyvä intuitiivinen ym. käsitteiden ymmärrys. Myöhemmin tarkastamme lukuteoriaan kuuluvia esimerkkejä.

Jäännösluokkien rengas $\mathbb{Z}_m$

Lauseen 14 mukaan $\equiv$ on ekvivalenssirelaatio. Vastaavia ekvivalenssiluokkia kutsutaan jäännösluokiksi (mod m).

[Lemma 2.5. Jäännösluokkia (mod m) on m kappaletta.

Tod. Jakojäännöslause $\Rightarrow$ jokainen $n \in \mathbb{Z}$ voidaan kirjoittaa muotoon $n = km + r$, $r \in \{0,1,\dots,m-1\}$. Luvut $0,1,\dots,m-1$ ovat selvästi epäkongruentteja. Toisaalta jos $n = km+r$, niin $n \equiv r \pmod m$. □

[Määr. Luvun $a \in \mathbb{Z}$ määräämä jäännösluokka (mod m) on

$$[a] = \{a + km \mid k \in \mathbb{Z}\}.$$

Määr. $\mathbb{Z}_m = \{[a] \mid a \in \mathbb{Z}\} = \{[0],[1],\ldots,[m-1]\}$. *)

Lause 2.6. $(\mathbb{Z}_m, +, \cdot)$ on kommutatiivinen m:n alkion rengas kun yhteenlasku ja tulo määritellään kaavalla

$$[a]+[b] = [a+b], \quad [a][b] = [ab].$$

Tod. Selvästi $\mathbb{Z}_m$:ssä 0-alkio on $[0]$, 1-alkio $[1]$ (esim. $[0]+[a] \overset{\text{määr.}}{=} [0+a] = [a]$). Renkaan määritelmän muut ehdot todetaan vastaavasti. Esim.

$$([a]+[b])[c] \overset{\text{määr.}}{=} [a+b][c] \overset{\text{määr.}}{=} [(a+b)c] = [ac+bc]$$
$$\overset{\text{määr.}}{=} [ac]+[bc] \overset{\text{määr.}}{=} [a][c]+[b][c].$$

Muut vastaavasti. Mutta, olemaisia on tarkistaa, että tulon ja summan määritelmät ovat hyvin asetettuja, eli että ne eivät riipu käytetyistä jäännösluokkien edustajista. Olkoon siis

$$[a] = [a'] \quad \text{ja} \quad [b] = [b'],$$

eli $a \equiv a'$ ja $b \equiv b' \pmod m$. Lauseen 2.2 nojalla silloin

$$a+b \equiv a'+b' \quad \text{ja} \quad ab \equiv a'b' \pmod m,$$

joten $[a+b] = [a'+b']$ ja $[ab] = [a'b']$. □

Määr. Jakojäännöslause $\Rightarrow$ $n \in \mathbb{Z}$ void. kirj. $n = qm+r$, $0 \le r \le m-1$. Sanomme, että r on luvun n **pienin positiivinen jäännös** $\pmod m$.

Esim. • $\mathbb{Z}_5$:ssä $[3][6] = [18] = [3]$, $[-5] = [0]$.

• Luvun -23 pienin positiivinen jäännös $\pmod{17}$ on 11 $(-23 = -2\cdot 17 + 11)$

---

*) Oikeampi merkintä jäännösluokkien renkaalle olisi $\mathbb{Z}/m\mathbb{Z}$!

- $\mathbb{Z}_6$: nyt $[2] \neq [0]$, $[3] \neq [0]$, mutta
$$[2][3] = [6] = [0].$$

Siis $\mathbb{Z}_6$ ei ole kokonaisalue, erityisesti se ei ole kunta. Milloin $\mathbb{Z}_m$ on kunta?

Lause 2.7. Olk. $m \geq 2$. $\mathbb{Z}_m$ on kunta jos ja vain jos m on alkuluku.

Tod Jos $m = m_1 m_2$, $2 \leq m_1, m_2 \leq m-1$ (eli $m \notin P$), niin $[m_1] \neq [0] \neq [m_2]$, mutta $[m_1][m_2] = [m] = [0]$, eli tällöin $\mathbb{Z}_m$ ei ole edes kokonaisalue.

Olkoon sitten $m \in P$. Jos $[a] \neq [0]$, niin $[a, m] = 1$. Seurauksen 1.6 nojalla on olemassa x, y joille $xa + ym = 1$, jolloin $xa \equiv 1 \pmod{m}$, eli $[x][a] = [1]$. Siis $[x]$ on $[a]$:n käänteisalkio tulon suhteen. Jokaisella $[0]$:sta eroavalla alkiolla on käänteisalkio tulon suhteen, joten $\mathbb{Z}_m$ on kunta. □

Määr. Olk. $m \geq 1$. Joukko $\{a_1, \ldots, a_m\}$ on täydellinen jäännösjoukko (mod m), mikäli
$$\{[a_1], [a_2], \ldots, [a_m]\} = \mathbb{Z}_m.$$

Lause 2.8. Olkoon $m \geq 2$ ja $U \subset \mathbb{Z}$. Silloin U on täydellinen jäännösjoukko (mod m) jos ja vain jos ainakin kaksi seuraavista ehdoista on voimassa:

(i) U:ssa on m lukua

(ii) U:n alkiot ovat keskenään epäkongruentteja (mod m)

(iii) Jokaisella $a \in \mathbb{Z}$ on olemassa $u \in U$ jolle $a \equiv u \pmod{m}$

Tod. HT. □

Seuraus 2.9. Olkoon $\{a_1, \dots, a_m\}$ täyd. jäännösysteemi $(\bmod m)$, ja $(k,m)=1$, $b \in \mathbb{Z}$. Silloin myös $\{ka_1+b, \dots, ka_m+b\}$ on täyd. jäännösysteemi.

Tod. Riittää näyttää, että Lauseen 2.8 ehdot (i) ja (ii) ovat voimassa. Ehto (i) on ilmeinen. Oletetaan, että $ka_j+b \equiv ka_\ell+b \pmod m$. Silloin $m \mid k(a_j-a_\ell)$, josta (Seur. 1.7) $m \mid (a_j-a_\ell)$, eli $a_j \equiv a_\ell \pmod m$. Täyd. jäännösyst. määr. nojalla $a_j = a_\ell$. □

Seuraava lause on lukuteorian perustuloksia.

Lause 2.10 (Fermat'n pieni lause)

Jos p on alkuluku ja $p \nmid a$, niin $a^{p-1} \equiv 1 \pmod p$.

Tod. $\{0,1,\dots,p-1\}$ on täyd. jäännösysteemi $(\bmod p)$. Koska $(a,p)=1$, samoin on $\{0, a, 2a, \dots, (p-1)a\}$ edellisen Seurauksen nojalla. Siispä luvut $\{a, 2a, \dots, (p-1)a\}$ ovat jossain järjestyksessä kongruentit lukujen $\{1, \dots, p-1\}$ kanssa. Erityisesti

$$1 \cdot 2 \cdot \dots \cdot (p-1) \equiv a \cdot 2a \cdot \dots \cdot (p-1)a \pmod p$$

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

Koska $((p-1)!, p)=1$, seuraa tästä $1 \equiv a^{p-1} \pmod p$. □

Huom. Sovelsimme edellä helppoa havaintoa:

Lemma 2.11 Jos $ka \equiv kb \pmod m$ ja $(k,m)=1$, niin $a \equiv b \pmod m$.

Tod. HT. □

Seuraus 2.12. Jos $p \geq 2$ on alkuluku, niin
$a^p \equiv a \pmod{p}$ kaikilla $a \in \mathbb{Z}$.

Esim. $p \mid (2^p - 2)$ kaikilla $p \in \mathbb{P}$.

Tehtävä. Olkoon p alkuluku, $p \neq 2, 5$. Osoita, että p jakaa ääretön monta luonnollisten lukujen jonon
$1, 11, 111, 1111, \ldots$ jäsentä.

Ratk. $\underbrace{111\ldots1}_{k \text{ kpl}} = 10^{k-1} + 10^{k-2} + \ldots + 1 = (10^k - 1)/9$.

Tapaus 1. $p \neq 3$. Nyt $p \geq 7$. Riittää osoittaa, että $10^k \equiv 1 \pmod{p}$ äärettömän monella k. Fermat'n pieni lause $\Rightarrow 10^{p-1} \equiv 1 \pmod{p}$, koska $(10, p) = 1$. Korottamalla potenssiin saamme
$10^{\ell(p-1)} \equiv 1 \pmod{p}$ kaikilla $\ell \geq 1$.

Tapaus 2. $p = 3$. Nyt $10^j \equiv 1^j \equiv 1 \pmod{3}$, eli
$10^{k-1} + \ldots + 1 \equiv k \cdot 1 = k \pmod{3}$.

Siispä kyseinen luku on jaollinen kolmella aina kun $3 \mid k$. □

Eulerin φ-funktio ja sovitettuja jäännösryhmäesimerkkejä

Määr. (Eulerin φ-funktio) Asetetaan $\varphi(1) = 1$ ja kun $m \geq 2$, merkitsemme $\varphi(m)$ on niiden luonnollisten lukujen $a \in \{1, 2, \ldots, m\}$ lukumäärä, joille $(a, m) = 1$.

Esim $\varphi(2) = 1$, $\varphi(6) = 2$, $\varphi(7) = 6$, yleisesti $\varphi(p) = p - 1$ jos $p \in \mathbb{P}$.

[Määr. Lukuteor. funktio on kuvaus $F: \mathbb{Z} \to \mathbb{R}$ ($\mathbb{C}$) tai $F: \mathbb{N} \to \mathbb{R}$ ($\mathbb{C}$)

[Määr. Lukuteor. funktio $F: \mathbb{N} \to \mathbb{C}$ on <u>multiplikatiivinen</u> jos $F(mn) = F(m)F(n)$ aina kun $(m,n) = 1$

[<u>Lause 2.13</u> φ on multiplikatiivinen

<u>Tod.</u> Oletetaan, että $m,n \geq 2$ ja $(m,n) = 1$. Tarkastellaan taulukkoa

0	1	2	...	$m-1$
m	$m+1$	$m+2$	...	$2m-1$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$(n-1)m$	$(n-1)m+1$	$(n-1)m+2$	...	$nm-1$

- Johainen pystyrivi koostuu luvuista jotka ovat kongruentteja (mod m). Katsomalla ensimmäistä vaakariviä näemme: on olemassa tasan $\varphi(m)$ pystyriviä joiden kaikki alkiot ovat suhteellisia alkulukuja m:n suhteen. Muiden pystyrivien yhdelläkään luvulla ei ole tätä ominaisuutta.

- Johainen pystyrivi muodostaa täydellisen jäännösryhmän mod n Seurauksen 2.9 ja tiedon $(m,n) = 1$ nojalla. Siis jokaisella pystyrivillä on tarkalleen $\varphi(n)$ suhteellista alkulukua n:n suhteen.

- Yhdistetään ed. havainnot $\Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$ □

Lause 2.14. $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$ ← tulo yli n:n alkulukujoiden

Tod. Jos $n = p_1^{\partial_1} \cdots p_\ell^{\partial_\ell}$ on n:n alkulukuhajotelma, saamme iteroimalla lausetta 2.13:

$$\varphi(n) = \prod_{j=1}^{\ell} \varphi(p_j^{\partial_j})$$

Luonnista $1, 2, \ldots, p^\partial$ ($\partial \in P$) p:llä jaollisia ovat luvut $p, 2p, \ldots, p^\partial$ joita on $p^{\partial-1}$ kpl. Siis $\varphi(p^\partial) = p^\partial - p^{\partial-1} = p^\partial\left(1 - \frac{1}{p}\right)$. Siis

$$\varphi(n) = \prod_{j=1}^{\ell} p_j^{\partial_j}\left(1 - \frac{1}{p_j}\right) = n \prod_{j=1}^{\ell}\left(1 - \frac{1}{p_j}\right). \quad \square$$

Esim. $\varphi(60) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$

$\varphi(pq) = (p-1)(q-1)$ jos $p, q \in P$ ja $p \neq q$.

INTERMEZZO: Todistus lauseelle 2.13. Oletamme tunnetuksi 'inklusion ja eksklusion periaatteen':

$$\#(A_1 \cup A_2 \cup \ldots \cup A_\ell) = \sum_j \#(A_j) - \sum_{j<k} \#(A_j \cap A_k)$$
$$+ \sum_{j<k<m} \#(A_j \cap A_k \cap A_m) - \ldots + (-1)^{\ell-1} \#(A_1 \cap \ldots A_\ell)$$

Jos $n = p_1^{\partial_1} \cdots p_\ell^{\partial_\ell}$ ($\partial_1, \ldots, \partial_\ell \geq 1$) on n:n alkulukuhajotelma. Ayt. sovelletaan edellistä asettamalla

$$A_j = \{k \in \{1, \ldots, n\} : p_j \mid k\}$$

Silloin $\varphi(n) = n - \#(A_1 \cup \ldots \cup A_\ell)$

Sovitusti $\varphi(A_{j_1} \cap A_{j_2} \cap \ldots A_{j_k}) = \frac{n}{p_{j_1} \cdots p_{j_k}}$

Saamme: $\varphi(n) = n - \sum_{j=1}^{\ell} \frac{n}{p_j} + \sum_{1 \leq j < k \leq \ell} \frac{n}{p_j p_k} - \ldots$

$$+ (-1)^\ell \frac{n}{p_1 \cdots p_\ell} = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\ell}\right). \quad \square$$

Lause 2.15. Sanomme, että $[U] \in \mathbb{Z}_m$ on *yksikkö* jos se on käänteyvä, eli on olemassa $[U]^{-1} \in \mathbb{Z}_m$. Merkitään $\mathbb{Z}_m^\times = \{[U] \in \mathbb{Z}_m : [U] \text{ on yksikkö}\}$.
Pätee: $[U]$ on yksikkö $\Leftrightarrow (U,m) = 1$. Lisäksi
$$\#(\mathbb{Z}_m^\times) = \varphi(m).$$

Tod. $[X] = [U]^{-1} \Leftrightarrow XU \equiv 1 \pmod m$
$\Leftrightarrow XU + ym = 1$ jollakin y.

Kyseisellä yhtälöllä on ratkaisu jos ja vain jos $(U,m) = 1$. Viimeinen väite seuraa suoraan φ-funktion määritelmästä. □

Määr. Olk. $m \geq 2$, $\emptyset \subset \mathbb{Z}$. Sanomme, että $\emptyset$ on ryhmäteoreettinen jäännösjoukko (mod m) jos $\emptyset$ sisältää täsmälleen yhden edustajan jokaisesta $\mathbb{Z}_m^\times$:in jäännösluokasta.

Lause 2.16. Joukko $\emptyset$ on ryhmäteoreettinen jäännösjoukko (mod m) jos ja vain jos
(i) $\emptyset$:ssa on $\varphi(m)$ alkiota, ja kaikki suhteellisia alkulukuja m:n suhteen
(ii) $\emptyset$:n alkiot ovat keskenään epäkongruentteja (mod m).

Tod. Ehdot selvästi välttämättömiä, riittävyys:
(ii) $\Rightarrow$ $\emptyset$:n alkiot edustavat eri jäännösluokkia (i) $\Rightarrow$ — " — $\mathbb{Z}_m^\times$ alkioita, ja niiden lukumäärä on $\varphi(m)$. Väite seuraa lauseesta 2.15. □

Esim.
- $m = 12$: voimme valita $\emptyset = \{1,5,7,11\}$.
- $m = 7$: — " — — " — $\emptyset = \{1,2,\dots,6\}$

Lause 2.17 Olkoon $\{a_1, \ldots, a_{\varphi(m)}\}$ supistettu jäännösjärjestelmä (mod m) ja $(k,m)=1$. Silloin myös $\{ka_1, \ldots, ka_{\varphi(m)}\}$ on supistettu jäännösjärjestelmä (mod m).

Tod. Tarkastetaan lauseen 2.16 ehdot: (i) Seuraa havaitsemalla, että $(ka_j, m) = 1$ kaikilla j koska $(k,m) = (a_j, m) = 1$. (ii): jos $ka_j \equiv ka_{j'} \pmod m$, niin (Lemma 2.11) $a_j \equiv a_{j'}$, eli $a_j = a_{j'}$ oletuksen nojalla. □

Edellinen lause voidaan formuloida $\mathbb{Z}_m$:ssä, esitämme sille samalla uuden todistuksen.

Lause 2.18. Jos $[k] \in \mathbb{Z}_m^*$, niin kuvaus $[u] \mapsto [k][u]$ on bijektio $\mathbb{Z}_m^* \to \mathbb{Z}_m^*$.

Tod. ① Kyseessä on lauseen 2.17 uudelleenformulointi. □

② Koska $[k] \in \mathbb{Z}_m^*$, sillä on käänteisalkio $[k]^{-1}$. Jos $[u] \in \mathbb{Z}_m^*$, niin $[k][u] \in \mathbb{Z}_m^*$, koska $([k][u])^{-1} = [k]^{-1}[u]^{-1}$. Kuvaus on selvästi bijektio, koska sillä on käänteiskuvaus

$$[u] \to [k]^{-1}[u] \; . \; \square$$

Voimme nyt esittää Eulerin yleistyksen Fermat'n pienelle lauselle.

Lause 2.19 (Euler) Olkoon $(a,m)=1$. Silloin

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

Tod. Siis $[a] \in \mathbb{Z}_m^*$. Luetellaan:

$\mathbb{Z}_m^\times = \{[u_1], \dots, [u_{\varphi(m)}]\}$. Lauseen 2.18 mukaan silloin myös $\mathbb{Z}_m^\times = \{[a][u_1], \dots, [a][u_{\varphi(m)}]\}$.
Eritysesti $\prod_{j=1}^{\varphi(m)} [a][u_j] = \prod_{j=1}^{\varphi(m)} [u_j]$.
Jakamalla puolittain luvulla $\prod_{j=1}^{\varphi(m)} [u_j]$ saamme $[a]^{\varphi(m)} = [1]$, eli $a^{\varphi(m)} \equiv 1 \pmod m$. □

Huom. Todistuksen voi myös perustaa lauseeseen 2.17 ilman $\mathbb{Z}_m$:n käyttöä (HT).

Esim. $p^2 \mid (a^{p^2-p}-1)$ jos $(a,p)=1$, $p \in P$.

Tarvitsemme jatkossa funktiota φ koskevan identiteetin (Lause 2.20 alla). Otetaan käyttöön lukuteoriassa hyödyllinen merkintä:

Määr. Jos $n \geq 1$ ja $f: \mathbb{N} \to \mathbb{R}$ (tai $\mathbb{C}$), niin merkintä $\sum_{d \mid n} f(d)$ tarkoittaa lukua $\sum_{\substack{d \in \{1,\dots,n\} \\ d \mid n}} f(d)$. Siis kyseessä on summa yli n:n positiivisten tekijöiden.

Esim. $\sum_{d \mid 6} f(d) = f(1) + f(2) + f(3) + f(6)$.

[Lause 2.20 Jos $n \geq 2$ niin $\sum_{d \mid n} \varphi(d) = n$.

Tod. Jos $d \geq 1$ ja $d \mid n$, merkitään

$$A_d = \{k \in \{1,\dots,n\} : (k,n) = d\}.$$

Selvästi $\#A_d = \varphi(\frac{n}{d})$ (perustele itsellesi!).
Toisaalta, $\{1,\dots,n\} = \bigcup_{d \mid n} A_d$, ja kyseessä on eritän. Täten

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

Väite seuraa kun huomaamme, että d:n jokaisen yli n:n eri positiivisten tekijöiden, samoin tekee n/d, eli

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d). \quad \square$$

SOVELLUS: RSA-salausmenetelmä

- Valitaan kaksi suurta (n. 1000-numeroista) alkulukua p ja q. Merkitään

$$\boxed{n = pq}$$

- Valitaan luku e $(1 < e < n)$ jolle $(e, (p-1)(q-1)) = 1$. Tämän jälkeen voimme ratkaista (mieti: miksi, miten) luvun d, $1 < d < n$, jolle

$$\boxed{de \equiv 1 \pmod{(p-1)(q-1)}}$$

- Pari (n,d) on henkilön A yksityinen avain, (n,e) on A:n julkinen avain.

Oletetaan nyt, että henkilö B haluaa lähettää viestin m (tekstit koodataan luvuiksi $m \in \{1, \ldots, n-1\}$) henkilölle A. Silloin B toimii seuraavasti: hän soveltaa julkista avainta (n,e) (joka on kaikkien saatavilla!) ja laskee luvun

$$\boxed{m' \equiv m^e \pmod{n}}$$

Luku $\boxed{m'}$ on nyt salakirjoitettu viesti, jonka B lähettää A:lle.

Vastaanotettuaan viestin m' A dekoodaa sen seuraavasti: hän laskee luvun

m'', jolle $\boxed{m'' \equiv m'^d \pmod{n}}$, $m'' \in \{1, \ldots, n-1\}$

Tämä avaa viestin, sillä

<u>Lause 2.21</u> $\boxed{m'' = m}$

<u>Tod.</u> Havaitsemme aluksi $\varphi(n) = (p-1)(q-1)$.
Nyt pätee $de = \ell(p-1)(q-1)+1$. Siispä
Eulerin lauseen nojalla jos $(m,n)=1$

$$m'' \equiv m'^d \equiv (m^e)^d = m^{de} = (m^{\varphi(n)})^{\ell} \cdot m$$
$$\equiv 1 \cdot m = m \pmod{n}.$$

Jos taas <u>vaikka</u> $p|m$, niin (huomaa: $\varphi(q) = q-1$)

$$m'' \equiv m'^d \equiv m^{de} \pmod{n}$$

$$\Rightarrow \quad m'' \equiv m^{de} \pmod{q}, \text{ joten}$$

$$m'' \equiv (m^{q-1})^{\ell(p-1)} m \equiv m \pmod{q}$$

Siis $q | (m - m'')$. Lisäksi $p|m \Rightarrow p|m' \Rightarrow p|m''$, eli
$p | (m''-m)$. Yhteensä $n | (m''-m)$, eli
tässäkin tapauksessa $m'' \equiv m \pmod{n}$.
Koska $m'' \in \{1, .., n\}$, saadaan $m'' = m$. □

- Voi soveltaa myös digitaaliseen allekirjoitukseen
- Oikeat käytössä olevat systeemit pieniä modifikaatioita ylläesitetystä.
- Mieti: miksi RSA 'sortuu' jos keksitään efektiivinen tapa faktoroida suuria lukuja alkutekijöihinsä.

Kiinalainen jäännöslause

Kootaan lemmatkin useita sovelluksia lebesgeja havaintoja:

Lemma 2.22 (i) Jos $(a_i, m) = 1$ kaikilla $i = 1, \dots, \ell$, silloin $(a_1 a_2 \dots a_\ell, m) = 1$.

(ii) Jos $(a_i, a_j) = 1$ kun $i \neq j$ ja $a_i \mid m$ kun $i = 1, \dots, \ell$, silloin $a_1 \dots a_\ell \mid m$.

Tod. HT □

Lause 2.23 (*Kiinalainen jäännöslause*)

Oletetaan, että $(m_i, m_j) = 1$, $1 \leq i < j \leq \ell$.
Kongruenssisysteemillä ($b_1, \dots, b_\ell$ mielivaltaisia)

$$(1) \quad \begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \vdots \\ x \equiv b_\ell \pmod{m_\ell} \end{cases}$$

on aina ratkaisu. Jos x_0 on (1):n eräs ratkaisu, niin kaikki ratkaisut saadaan kaavasta

$$x = x_0 + k m_1 m_2 \dots m_\ell \quad (k \in \mathbb{Z})$$

Tod. Oletetaan ensin, että $b_1 = 1$ ja $b_2 = b_3 = \dots = b_\ell = 0$.
Merkitään $m' = m_2 m_3 \dots m_\ell$.

Jos x on muotoa km', se toteuttaa myös automaattisesti 2., 3., ... ja ℓ:nnen kongruenssin ryhmässä (1). Lisäksi 1. kongruenssi toteutuu jos

$$km' \equiv 1 \pmod{m_1}.$$

Tällainen k voidaan aina valita, koska

oletuksen (ja Lemman 2.22) mukaan $(m_j, m_i) = 1$.
Siis tässä tapauksessa kongruenssilla (1) on ratkaisu. Tilanteen symmetrisyyden ansiosta samoin nähdään, että vastaavassa tilanteessa, jossa $b_j = 1$ ja $b_i = 0$ kun $j \neq i$ on systeemillä (1) aina ratkaisu, olkoon x_j sellainen.
Siis $x_j \equiv 1 \pmod{m_j}$ ja $x_j \equiv 0 \pmod{m_i}$ jos $i \neq j$.
Suora tarkastus osoittaa, että systeemin (1) ratkaisee yleisessä tapauksessa luku

$$x_0 = \sum_{j=1}^{\ell} b_j x_j .$$

Lisäksi selvästi $x_0 + k m_1 m_2 \dots m_\ell$ on aina ratkaisu. Käänteisen, jos x_1 on toinen ratkaisu, niin $m_j \mid (x_1 - x_0)$ $\forall j = 1, \dots, \ell$. Lemman 2.22(ii) nojalla siis $m_1 m_2 \dots m_\ell \mid (x_1 - x_0)$. □

Esim. Etsi kaikki luvut $x \geq 1$ jolla pätee:
jakojäännös jaettaessa { luvulla 5 on 3, luvulla 7 on 2, luvulla 11 on 1 }

Ratk. Yhtäpitävästi
$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \\ x \equiv 1 \pmod{11} \end{cases}$$

Sovelletaan lauseen 2.23 todistuksen antamaa ratkaisutapaa: Jos oikea puoli on $\begin{pmatrix}1\\0\\0\end{pmatrix}$, saamme kongruenssin $77k \equiv 1 \pmod 5$, jolle $k = 3$ on ratkaisu. Siis $x_1 = 3 \cdot 77 = 231$.
Jos oikea puoli on $\begin{pmatrix}0\\1\\0\end{pmatrix}$, saamme kongruenssin $55k \equiv 1 \pmod 7$, jonka eräs ratkaisu on $k = -1$. Voimme valita $x_2 = -55$.
Viimeksi, jos oikea puoli on $\begin{pmatrix}0\\0\\1\end{pmatrix}$, saamme $35k \equiv 1 \pmod{11}$, jolla ratkaisu $k = 6$, eli $x_3 = 210$.

Lopulta $x_0 = 3 \cdot 231 - 2 \cdot 55 + 210 = 793$ on eräs ratkaisu. Yleinen ratkaisu on

$$x = 793 + k \cdot 385 \,, \quad k \in \mathbb{Z},$$

josta ratkaisut voi kirjoittaa muotoon

$$x = 23 + k \cdot 385, \quad k \geq 0. \qquad \square$$

Huom 1. Aiempi lauseemme (lause 1.12) voidaan kirjoittaa muotoon:

Kongruenssilla $ax \equiv b \pmod m$ on ratkaisu jos ja vain jos $(a,m) \mid b$. Tällöin yhtälöllä on (a,m) epäkongruenttia ratkaisua $(\bmod m)$, ja x on ratkaisu vain jos

$$x \equiv x_0 \pmod{\tilde{m}}, \quad \tilde{m} = \frac{m}{(a,m)}$$

Edellisen nojalla systeemillä

$$(2) \quad \begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \vdots \\ a_\ell x \equiv b_\ell \pmod{m_\ell} \end{cases}$$

on ratkaisu vain jos $(a_\ell, m_\ell) \mid b_\ell \;\forall\, \ell$ ja systeemillä

$$(1') \quad \begin{cases} x \equiv x_{0,1} \pmod{\tilde{m}_1} \\ \vdots \quad\quad \vdots \\ x \equiv x_{0,\ell} \pmod{\tilde{m}_\ell} \end{cases}$$

on ratkaisu. Tämä on muotoa (1), jotenkin ainakin jos $(\tilde{m}_i, \tilde{m}_j) = 1$, $i \neq j$, systeemillä (1') on ratkaisu.

Huom 2. Voidaan osoittaa, että yleisesti (siis ilman ehtoa $(m_i, m_j) = 1$, $i \neq j$, systeemillä (1) on ratkaisu jos ja vain jos $(m_i, m_j) \mid (b_i - b_j)$ kaikilla i, j.

Huom 3. Lauseen 35 avulla voidaan osoittaa, että luonnollisella luvulla n on isomorfinen 'suoran summan' $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \dots \oplus \mathbb{Z}_{m_\ell}$ kanssa, mikäli $m = m_1 \cdots m_\ell$ ja $(m_i, m_j) = 1$, $i \neq j$. (Ohjattu HT).

3. YLEISET POLYNOMIKONGRUENSSIT, PRIMITIIVISET JUURET

Lagrangen lause

Palautetaan mieleen algebran peruslause, jonka mukaan n:n asteen polynomilla on enintään n juurta (itseasiassa tarkalleen n kun sallitaan kompleksijuuret ja useamsikertaiset lasketaan kertalukunsa mukaan).

Tutkimme kysymystä: kuinka monta juurta voi olla kongruenssilla ($a_0, \dots, a_n \in \mathbb{Z}$, $x \in \mathbb{Z}$)

$$a_n x^n + \dots + a_0 \equiv 0 \pmod m \; ?$$

[Sanomme, että kaksi ratkaisua ovat *eri* juuria mikäli ne ovat epäkongruentteja (mod m).

Esim. $x^2 + 1 \equiv 0 \pmod 5$?
Kokeilemalla löydämme juuret $\{2, 3\}$.
Muita eri juuria ei ole (mod 5).
Toisin sanoen: yhtälöllä $x^2 + [1] = [0]$ on juuret $x \in \{[2], [3]\}$ $\mathbb{Z}_5$:ssä!
Havaitsemme myös, että

$$x^2 + [1] = (x - [2])(x - [3]) \quad \text{$\mathbb{Z}_5$:ssä.}$$

[**Lause 3.1.** (Lagrange) Olkoon $p \in \mathbb{P}$ alkuluku ja $f(x) = a_n x^n + \dots + a_0$, $a_i \in \mathbb{Z}$ $\forall i$.
Jos $p \nmid a_n$, on kongruenssilla

$$f(x) \equiv 0 \pmod p$$

enintään n ratkaisua.

Tod. Voimme olettaa, että $n \le p$. Todistamme väitteen induktiolla n:n suhteen. Selvästi väite on tosi kun $n=0$ (miksi?). Oletetaan, että väite on osoitettu todeksi polynomin arteilla $0,1,\dots,n-1$. Tarkastellaan n. arteen polynomikongruenssia

$$(1) \quad f(x) = a_n x^n + \dots + a_0 \equiv 0 \pmod{p},$$

missä $p \nmid a_n$.

Vastaoletus: kongruenssilla (1) eri juuret $x_1, \dots, x_{n+1}$. Kirjoitetaan

$$g(x) = f(x) - a_n(x-x_1)\cdots(x-x_n).$$

Kongruenssilla $g(x) \equiv 0 \pmod{p}$ on n ratkaisua $x_1, \dots, x_n$! Sen arte $< n$, joten induktio-oletuksen nojalla jokaisen g:n kertoimen on oltava jaollinen p:llä, muuten voisimme kirjoittaa $g(x) \equiv b_\ell x^\ell + \dots + b_0$, missä $p \nmid b_\ell$, $\ell < n$, ja n:n eri ratkaisun olemassaolo olisi vastoin induktio-oletusta. Siis g:n kertoimet kaikki jaollisia p:llä, eritysisesti identtisesti pätee (identtisesti)

$$(2) \quad f(x) \equiv a_n(x-x_1)\cdots(x-x_n) \pmod{p}$$

[Huomaa, että johdimme (2):n vain tiedosta että (1):llä eri juuret $x_1, \dots, x_n$.]

Otamme nyt käyttöön $(n+1)$. juuren x_{n+1} olemassaolon ja oletuksen että $p \nmid a_n$. Sijoitetaan (2):een $x = x_{n+1}$, jolloin saamme

$$0 \equiv a_n(x_{n+1}-x_1)(x_{n+1}-x_2)\cdots(x_{n+1}-x_n) \pmod{p}$$

Oikean puolen mikään termi ei ole jaollinen p:llä, mikä on mahdotonta. □

Edellisellä lauseella (ja sen todistuksella) on mielenkiintoisia seurauksia:

Seuraus 3.2. Olkoon $F(x) = a_n x^n + \dots + a_0$ ja olkoon kongruenssilla $f(x) \equiv 0 \pmod p$ missä $p \in P$, eri juuret $x_1, \dots, x_n$. Tällöin identtisesti $\forall x \in \mathbb{Z}$

$$F(x) \equiv a_n (x - x_1) \cdots (x - x_n) \pmod p.$$

Tod. Katso lauseen 3.1 tod., erityisesti huomautus kaavan (2) jälkeen. □

Seuraus 3.3. Jos $p \in P$, $n < p$, niin kongruenssilla $a_n x^n + \dots + a_0 \equiv 0 \pmod p$ on joko enintään n juurta tai sitten se on voimassa identtisesti ja $p \mid a_j$ kaikilla $j = 0, 1, \dots, n$.

Tod. Merkitään $g(x) = \sum_{p \nmid a_j} a_j x^j$.

Jos g ei ole nollapolynomi, sovelletaan lausetta 3.1, että kongruenssilla $g(x) \equiv 0 \pmod p$ on enintään n juurta, eli sama pätee kongruenssille $a_n x^n + \dots + a_0 \equiv 0$. Jos g on nollapolynomi, silloin $p \mid a_j$ $\forall j = 0, \dots, n$ ja $a_n x^n + \dots + a_0 \equiv 0$ identtisesti. □

Esim. Kongruenssilla $x^{p-1} - 1 \equiv 0 \pmod p$ on maksimimäärä juuria, eli $p-1$ kpl (juuret $x = 1, 2, \dots, p-1$ Fermatin pienen lauseen nojalla).

Esim. Juuria voi olla vähemmän kuin maksimimäärä:

- Kongruenssilla $x^2 + 1 \equiv 0 \pmod 3$ ei ole juuria.

• kongruenssilla $x^5 \equiv 1 \pmod{13}$ on vain yksi juuri. Tämän näkee kokeilemalla, kun FPL:een avulla: jos $13 \nmid x$,

$$x^5 \equiv 1 \Rightarrow (x^5)^5 \equiv 1 \Leftarrow (x^{12})^2 \cdot x \equiv 1$$
$$\Rightarrow x \equiv 1 \pmod{13}$$

Lagrangen lause $\mathbb{Z}_p$:n avulla

Halmotlemme nyt Lagrangen lausetta polynomeista $\mathbb{Z}_p$:n tarkasteluilla.

$$F(x) \equiv 0 \pmod{p}, \quad p \in \mathbb{P}, \quad p \nmid a_n$$

$$\Leftrightarrow \quad [F]([x]) = [0] \quad \mathbb{Z}_p\text{:ssä},$$

missä $[F](y) = [a_n]y^n + \dots + [a_0]$, $y \in \mathbb{Z}_p$.
Merkitään $\mathbb{Z}_p$-kertoimista polynomia yksinkertaisuuden vuoksi $[F] = F$ ja $[a_j] = b_j \in \mathbb{Z}_p$, $0 \le j \le n$, eli

$$F(x) = b_n x^n + b_{n-1}x^{n-1} + \dots + b_0, \quad b_n \neq [0].$$

missä $b_0, b_1, \dots, b_n \in \mathbb{Z}_p$ ja $x \in \mathbb{Z}_p$.

Lemma 3.4. Jos $F(a) = [0]$, $a \in \mathbb{Z}_p$, niin on olemassa $(n-1)$-asteinen polynomi g (kertoimet $\mathbb{Z}_p$:ssä), jolle

$$F(x) = (x-a)g(x)$$

Huom Kyseinen identiteetti tarkoittaa että kun oikealla puolella oleva tulo lasketaan auki ja yhdistetään samanasteiset termit, niin saadaan vasemman puolen polynomi!

Tod. HT (esim. sovella identiteettiä
$x^n - a^n = (x-a)(x^{n-1} + x^{n-2}a + \dots + a^{n-1})$). □

Lagrangen lauseen uusi tod. Oletetaan, että yhtälöllä $F(x) = \sum_{k=0}^{n} b_k x^k = [0]$
($b_0, \dots, b_n \in \mathbb{Z}_p$, $p \in \mathbb{P}$, $b_n \neq [0]$) on eri juuret $x_1, x_2, \dots, x_n \in \mathbb{Z}_p$. Lemman 3.4 nojalla

$$F(x) = (x-x_1)g_1(x), \qquad g(x) = b_n x^{n-1} + \dots$$

Nyt $x_2 - x_1 \neq [0]$, joten $g_1(x_2) = 0$. Voimme soveltaa samaa päättelyä polynomiin g_1, jolloin tulee

$$F(x) = (x-x_1)(x-x_2)g_2(x),$$

ja iteroimalla saamme lopulta

$$F(x) = b_n(x-x_1)(x-x_2)\dots(x-x_n).$$

Nyt $F(x_{n+1}) = b_n(x_{n+1}-x_1)\dots(x_{n+1}-x_n) \neq [0]$, mikä on mahdotonta. ↯

Johdamme muutaman mielenkiintoisen seurauksen Lagrangen lauseelle.

Seuraus 3.5 Jos $p \in \mathbb{P}$, $d \mid (p-1)$, $d \geq 1$, niin kongruenssilla $x^d \equiv 1 \pmod p$ on täsmälleen d juurta.

Tod. Jos $d \mid (p-1)$, niin $p-1 = dd_1$ ja

$$(*) \quad x^{p-1} - 1 = (x^d - 1)(x^{(d_1-1)d} + x^{(d_1-2)d} + \dots + 1)$$
$$= (x^d - 1)\,g(x),$$

missä $g(x) = x^{(d_1-1)d} + \dots + 1$ on astelukua $(p-1)-d$. Koska kaikki kertoimet eivät ole

jaollisia p:llä, on kongruenssilla $g(x) \equiv 0 \pmod p$ enintään $(p-1)$-d juurta. Toisaalta Fermatin pieni lause $\Rightarrow$ kongruenssilla $x^{p-1} - 1 \equiv 0$ on täsmälleen $p-1$ juurta! Siispä identiteetin (*) sivulla 37 nojalla kongruenssil. la $x^{d-1} \equiv 0$ täytyy olla ainakin $(p-1) - ((p-1)-d) = d$ juurta. Lagrangen lauseen nojalla niitä on enintään d, joten niitä on täsmälleen d kappaletta. □

Lause 3.6. (Wilson) *Kokonaisluku $p > 1$ on alkuluku jos ja vain jos*

$$(p-1)! \equiv -1 \pmod p$$

Tod. Tapaus $p = 2$ ok. Jos $p \geq 3$ on alkuluku, niin Fermatin pienen lauseen ja seurauksen 3.2 mukaan

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod p$$

kaikilla $x \in \mathbb{Z}$. Sijoittamalla $x = 0$ saamme

$$-1 \equiv (-1)(-2)\cdots(-(p-1)) = (-1)^{p-1}(p-1)!$$
$$= (p-1)! \pmod p.$$

Käänteinen suunta on HT. □

Polynomikongruenssit yhdistetyn modulin suhteen

Kuinka monta juurta voi kongruenssilla

$$f(x) \equiv 0 \pmod m$$

olla kun $m \notin \mathbb{P}$.

Esim. $x^2 + x \equiv 0 \pmod 6$
Tällä kongruenssilla on 4 eri ratkaisua:
$x \in \{0,2,3,5\}$. Siispä Lagrangen lause ei päde yhdistetyille moduleille!

On luonteenomaista demonstroida yleinen menetelmä, jolla kongruenssin $f(x) \equiv 0 \pmod m$ voi palauttaa kongruenssiehtoihin jotka ovat vain alkuluvumodulin suhteen. Kuvaamme sen seuraavaksi.

Olkoon $\boxed{m = p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}}$ $(e_1, \ldots, e_\ell \geq 1)$
modulin m alkulukuhajotelma.

ASKEL 1 $f(x) \equiv 0 \pmod m$
on ekvivalentti systeemin

$$(3) \quad \begin{cases} f(x) \equiv 0 \pmod{p_1^{e_1}} \\ f(x) \equiv 0 \pmod{p_2^{e_2}} \\ \vdots \\ f(x) \equiv 0 \pmod{p_\ell^{e_\ell}} \end{cases}$$

kanssa. Oletetaan, että jokaisella näistä on ratkaisuja; olkoon j. kongruenssilla systeemissä (3) ratkaisut (yht. $s_j \geq 1$ kappaletta)

$$x \equiv a_{j1}, \; x \equiv a_{j2}, \ldots, x \equiv a_{js_j} \pmod{p_j^{e_j}}$$

Tällöin kongruenssin (3) ratkaisut saadaan ratkaisemalla

$$S := s_1 \times s_2 \times \ldots \times s_\ell \quad \text{kpl}$$

lineaarisia systeemejä

$$\begin{cases} x \equiv a_{11} \text{ tai } a_{12} \text{ tai } \ldots \text{ tai } a_{1s_1} \pmod{p_1^{e_1}} \\ \vdots \\ x \equiv a_{\ell 1} \text{ tai } a_{\ell 2} \text{ tai } \ldots \text{ tai } a_{\ell s_\ell} \pmod{p_\ell^{e_\ell}} \end{cases}$$

Näistä jokaisella on 1-käs ratkaisun (mod m) kiinalaisen jäännöslauseen nojalla! Siispä systeemin (3) ratkaisujen lukumäärä on

$$s_1 \times s_2 \times \dots \times s_\ell .$$

ASKEL 2. Kongruenssin $\boxed{f(x) \equiv 0 \pmod{p^e}}$ (4)

pystyy ratkaisemaan iteratiivisesti kunhan vain tiedämme kongruenssin $f(x) \equiv 0 \pmod p$ ratkaisut! Menetelmä toimii induktiolla eksponentin e suhteen:

Oletetaan, että $e \geq 2$ ja että kongruenssilla $f(x) \equiv 0 \pmod{p^{e-1}}$ on ratkaisut

$$x_1, x_2, \dots, x_r \pmod{p^{e-1}}.$$

Jos x ratkaisee kongruenssin (4), on oltava $f(x) \equiv 0 \pmod{p^{e-1}}$, joten

(5) $\boxed{x \equiv x_j \pmod{p^{e-1}}}$ jollakin $j \leq r$!

Jotta löytäisimme kaikki ratkaisut kongruenssille (4) mod p, huomaamme, että eri jäännösluokat (mod p^e) joille (5) toteutuu koostuvat luvuista (miet!)

$$x = x_0 + t p^{e-1}, \quad t \in \{0,1,\dots,p-1\}, \quad x_0 \in \{x_1,\dots,x_r\}.$$

Kiinnitetään $x_0 \in \{x_1,\dots,x_r\}$ ja tutkitaan milloin $x_0 + t p^{e-1}$ on (4):n ratkaisu. Taylorin kaavan nojalla

$$\begin{aligned} f(x_0 + t p^{e-1}) &= f(x_0) + f'(x_0)\, t p^{e-1} + \frac{f''(x_0)}{2} t^2 p^{2(e-1)} \\ &\quad + \dots + \frac{f^{(n)}(x_0)}{n!} t^n p^{n(e-1)} \\ &\equiv f(x_0) + f'(x_0)\, t p^{e-1} \pmod{p^e}, \end{aligned}$$

missä oletimme, että f:n aste on n, ja sovelsimme tietoa, että $f^{(j)}(x_0)/j! \in \mathbb{Z}$ (HT) aina kun f on kokonaiskertoiminen.
Koska oletuksen mukaan $p^{e-1} \mid f(x_0)$, niin

$$f(x_0 + t p^{e-1}) \equiv 0 \pmod{p^e}$$

$$\Leftrightarrow \quad \boxed{\frac{f(x_0)}{p^{e-1}} + t f'(x_0) \equiv 0 \pmod{p}} \qquad (6)$$

On olemassa <u>3 vaihtoehtoa</u>:

1) $p \nmid f'(x_0)$ (<u>ei-singulaarinen tapaus</u>).
Silloin (6):lla on tasan 1 ratkaisu $\pmod p$, eli tasan 1 t:n arvoista $t \in \{0, 1, \ldots, p-1\}$ tuottaa ratkaisun $x_0 + t p^{e-1}$.

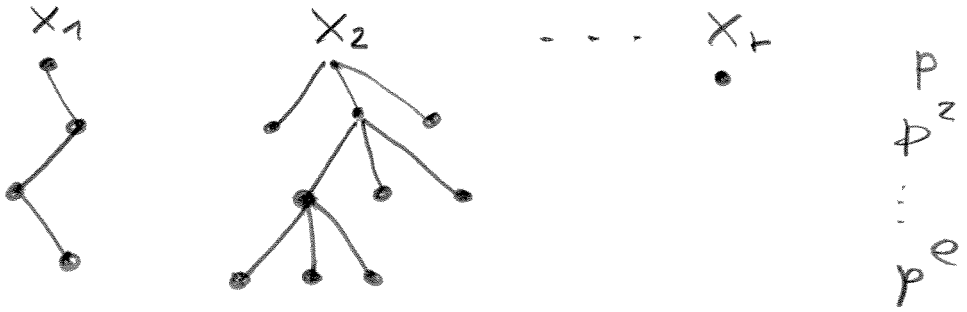
2) $p \mid f'(x_0)$ ja $p^e \mid f(x_0)$ (1. singulaarinen tapaus)
Nyt (4):n ratkaisevat <u>kaikki</u> t:n arvot $t \in \{0, 1, \ldots, p-1\}$, eli luvut $x_0 + t p^{e-1}$ antavat p kpl eri ratkaisuja kongruenssille (4).

3) $p \mid f'(x_0)$ ja $p^e \nmid f(x_0)$ (2. singulaarinen tapaus).
Tällöin (6):lla ei ole ratkaisuja, ja luvut $x_0 + t p^{e-1}$ eivät tuota ratkaisuja.

<u>Huom 1.</u> Siispä jokainen tason p^{e-1} ratkaisu x_0 antaa k ratkaisua tasolla p^e, missä

- vaihtoehdossa 1) $k = 1$
- — " — 2) $k = p$
- — " — 3) $k = 0$

Ratkaisuja eri tasoilla voi havainnollistaa puulla:



Huom 2. Suurilla p:n arvoilla voi olla vaikea päätellä millaisia kongruensseilla $f(x) \equiv 0 \pmod{p}$ on ratkaisuja, saati löytää ne, vaikka asteluku n olisi pieni. Ratkaisemme myöhemmin tämän ongelman täydellisesti kun $n = 2$.

Esim. $f(x) = x^4 + x + 6 \equiv 0 \pmod{45}$

Todetaan ensin: $45 = 3^2 \cdot 5$

(1o) $f(x) \equiv 0 \pmod 5$

$\Leftrightarrow \quad x^4 + x + 1 \equiv 0 \pmod 5$

Kokeilemalla $x \in \{0, \pm 1, \pm 2\}$ saamme ratkaisun

$$\boxed{x \equiv -2 \pmod 5}$$

(2oa) $f(x) \equiv 0 \pmod 3$

$\Leftrightarrow \quad x(x^3 + 1) \equiv 0 \pmod 3$

Kokeilemalla $x \in \{0, \pm 1\}$ saamme ratkaisut

$$\boxed{\begin{cases} x \equiv 0 \pmod 3 \\ x \equiv -1 \pmod 3 \end{cases}}$$

(2.b) $f(x) \equiv 0 \pmod{3^2}$

a) $x_0 = 0$ $\quad f'(x_0) = 1 \not\equiv 0 \pmod 3$.

Kyseessä ei-singulaarinen tapaus. Ratkaistaan

$$t\, f'(x_0) + \frac{f(x_0)}{3} \equiv 0 \pmod 3, \quad t \in \{0,1,2\}$$

$$\Leftrightarrow \quad t + 2 \equiv 0 \pmod 3$$

Saamme $t = 1$. Lopputulos ratkaisuun

$$\boxed{x = 0 + 1 \cdot 3 = 3 \pmod 9}$$

b) $x_0 = -1$ $\quad f'(x_0) = -3 \equiv 0 \pmod 3$;
kyseessä singulaarinen tapaus. Nyt $f(x_0)/3 = 2$, joten tarkemmin ottaen kyseessä on 2. singulaarinen tapaus ja lyseinen x_0 ei generoi ratkaisua tasolla 3^2.

(3.) Yhteenveto Siis ainoa ratkaisu toteuttaa kongruenssit $\begin{cases} x \equiv -2 \pmod 5 \\ x \equiv 3 \pmod 9 \end{cases}$,

joten alkuperäisen kongruenssin (ainoa) ratkaisu on

$$\boxed{x \equiv 3 \pmod{45}}.$$

Huom. • Joga edellisenä esimerkinä (mod 9) on edellä kuvatte algoritmi tehokkaampi tapa etsiä juuret kuin pelkkä tokeilu

• Algoritmi on läheisenä yhteydessä ns. padistes kuhujen teoriaan!

Primitiiviset juuret

Esim. Kuinka monta eri jäännösluokkaa voi jono $\{1, a, a^2, \ldots\}$ sisältää $(\mathrm{mod}\ p)$, $p \in \mathbb{P}$? Kokeillaan tapauksessa $p = 7$:

$2^0 \equiv 1,\ 2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 1$ (jono toistaa $(\mathrm{mod}\ 7)$ itseään)
3 kpl

$3^0 \equiv 1,\ 3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5 \quad (\mathrm{mod}\ 7)$
6 kpl

Tässä tapauksessa 6 kpl on mahdinmäärä (tulee olla $(a,7)=1$). Potenssilla $3^0, 3, \ldots, 3^5$ on erityinen ominaisuus, jonka johdosta sanomme: 3 on primitiivinen juuri $(\mathrm{mod}\ 7)$. Katso tarkemmin määr. sivulla ja lause 3.9 alla.

$m \geq 2$ ja

Määr. Olkoon $(a,m)=1$. Luku $\mathrm{ord}_m(a)$ on pienin positiivinen eksponentti $k \geq 1$ jolle
$$a^k \equiv 1 \pmod m.$$

Huom. • Yhtäpitävästi $\mathbb{Z}_m$:ssä
$$\mathrm{ord}_m(a) = \min\{k \geq 1 : [a]^k = [1]\}$$

• Jos $\mathrm{ord}_m(a) = k$, sanomme että luku a kuuluu eksponenttiin k $(\mathrm{mod}\ m)$

Lause 3.7. Olkoon $(a,m)=1$ ja $k = \mathrm{ord}_m(a)$.
(i) Olk. $n \geq 0$. Tällöin $a^n \equiv 1 (\mathrm{mod} m) \Leftrightarrow k \mid n$.
(ii) $k \mid \varphi(m)$ (iii) Olk. $n_1, n_2 \geq 0$. Silloin
$$a^{n_1} \equiv a^{n_2} \pmod m \Leftrightarrow k \mid (n_1 - n_2).$$
(iv) Jos $n \geq 1$, niin $\mathrm{ord}_m(a^n) = k/(n,k)$.

Tod (i) Kirjoitetaan n muotoon $n = kt + r$, missä $k \geq 0$ ja $0 \leq r < t-1$. Saadaan
$$a^n = (a^t)^k a^r \equiv 1^k a^r = a^r \pmod m.$$
Luvun t määritelmän nojalla ja koska $r < t$, pätee $a^r \equiv 1$ vain jos $r = 0$, eli $t \mid n$.

(ii) Eulerin kaavan nojalla $a^{\varphi(m)} \equiv 1 \pmod m$, joten väite seuraa (i)-kohdasta.

(iii) Olk. $n_2 \geq n_1 \geq 0$ ja $a^{n_2} \equiv a^{n_1} \pmod m$.
Koska $(a^{n_1}, m) = 1$, voimme jakaa kongruenssin luvulla a^{n_1}, jolloin yhtäpitävästi $a^{n_2 - n_1} \equiv 1 \pmod m$, joka toteutuu (i)-kohdan nojalla vain kun $t \mid (n_2 - n_1)$.

(iv) Merk. $s = \operatorname{ord}_m(a^n)$. (i)-kohdan mukaan s on pienin luku $s \geq 1$ jolle $t \mid sn$.
Helposti (HT) nähdään, että $s = t/(t,n)$. □

Määr. a on *primitiivinen juuri* $\pmod m$ jos $(a, m) = 1$ ja $\operatorname{ord}_m(a) = \varphi(m)$

Huom. • Jos a on primit. juuri mod m, niin luvut $1, a, a^2, \ldots, a^{\varphi(m)-1}$ ovat keskenään epäkongruentteja (Lause 3.7.(iii)) ja toisaalta $(a^j, m) = 1$, $\forall j \geq 0$, ja kys. lukuja on $\varphi(m)$ kpl. Siispä kaikkien
$$\{1, a, \ldots, a^{\varphi(m)-1}\}$$
on supistettu jäännösluokka $\pmod m$.

- Toinen tapa saada edellinen on: jos a on primitiivijuuri (mod m), niin
$$\mathbb{Z}_m^* = \{[a]^j : 0 \le j \le \varphi(m)-1\}.$$

- Jos $p \in \mathbb{P}$ on alkuluku (tärkeä tapaus), niin a on primit. juuri (mod p) jos ja vain jos (muista: $\varphi(p) = p-1$)
$$\{[1],[2],\dots,[p-1]\} = \{[1],[a],[a]^2,\dots,[a]^{p-2}\}$$
eli Aasian sanoen: luvut $\{0,1,a,a^2,\dots,a^{p-2}\}$ muodostavat täydellisen jäännösjärjestelmän (mod p)!

Lemma 3.8. Olkoon $p \in \mathbb{P}$, $t \ge 1$.

(i) Jos $t \nmid (p-1)$, ei mikään kokonaisluku voi olla eksponenttina t.

(ii) Jos $t \mid (p-1)$, on eksponenttina t olevien luokkien määrä (tarkemmin sanoen: eksponenttina t olevien jäännösluokkien lukumäärä) joko 0 tai $\varphi(t)$.

Tod. (i) Koska $\varphi(p) = p-1$, seuraa lauseesta 3.7(iii), että kaikilla a joille $(a,p)=1$ pätee $\operatorname{ord}_p(a) \mid (p-1)$.

(ii) Oletetaan, että $t \mid (p-1)$ ja $^{*)}$ on olemassa ainakin yksi luku a ($(a,p)=1$), jonka kertaluku eksponenttina t, eli $\operatorname{ord}_p(a) = t$. Silloin luvut
$$1, a, a^2, \dots, a^{t-1}$$
---
voimme olettaa $t \ge 2$, tapaus $t=1$ triviaali.

ovat keskenään epäkongruentteja (mod p) luvun k määritelmän ja lauseen 3.7 (iii) nojalla. Lisäksi jokaisella $j \in \{0,1,\dots,k-1\}$ pätee

$$(a^j)^k = (a^k)^j \equiv 1^j = 1 \pmod p.$$

Siis polynomikongruenssilla $x^k \equiv 1 \pmod p$ on k kpl eri ratkaisuja (mod p). Lagrangen lauseen nojalla muita ratkaisuja ei ole. Lauseen 3.7 (iii) mukaan näistä juuri ne luvut a^j ($1 \le j \le k-1$ — 1 ei voi kuulua eksponenttiin $k \ge 2$!) joille $(j,k)=1$, eli yhteensä $\varphi(k)$ kpl. □

Olemme nyt valmiit todistamaan:

Lause 3.9. Olkoon $k \ge 1$ $k \mid (p-1)$, missä $p \in \mathbb{P}$. Silloin luvuista $(1,2,\dots,p-1)$ kuhun eksponenttiin k täsmälleen $\varphi(k)$ kpl. Erityisesti primitiivisten juurten (mod p) määrä on $\varphi(p-1) \ge 1$.

Tod. Olkoon $\psi(k)$ (kun $k \ge 1$ ja $k \mid (p-1)$) niiden kpl:jen $a \in \{1,2,\dots,p-1\}$ määrä, jotka kuuluvat eksponenttiin k. Saamme

$$\begin{cases} \sum_{k \mid (p-1)} \psi(k) = (p-1) & \text{(Lause 3.7 (ii))} \\ \psi(k) \le \varphi(k) \quad \forall\, k \mid (p-1) & \text{(Lause 3.8 (ii))} \\ \sum_{k \mid (p-1)} \varphi(k) = (p-1) & \text{(Lause 2.20)} \end{cases}$$

Ainoaksi vaihtoehdoksi jää: $\psi(k) = \varphi(k) \ \forall\, k \mid (p-1)$. □

Esim. $p = 7$

$p - 1 = 6$, $\ell \mid 6$
$\iff \ell \in \{1, 2, 3, 6\}$

ℓ	$\varphi(\ell)$	luvut, jotka kuuluvat eksponenttiin ℓ
1	1	$\{1\}$
2	1	$\{6\}$
3	2	$\{2, 4\}$
6	2	$\{3, 5\}$

a	a^2	a^3	a^4	a^5	a^6	$\operatorname{ord}_7(a)$
1	1	1	1	1	1	1
2	4	1	2	4	1	3
3	2	6	4	5	1	6
4	2	1	4	2	1	3
5	4	6	2	3	1	6
6	1	6	1	6	1	2

$\pmod 7$

Siispä primitiivisiä juuria $\pmod 7$ ovat luvut 3 ja 5.

Seuraus 3.10 Jos $p \in \mathbb{P}$, niin $\mathbb{Z}_p^*$ on syklinen. □

(palautetaan mieleen, että äärellinen ryhmä G on syklinen, jos on olemassa $a \in G$ jolle $G = \{a^j : 0 \le j \le \ell - 1\}$, missä väl ttämättä $\ell = \#(G)$)

Milloin $\mathbb{Z}_m$ on syklinen?

Lause 3.11 $\mathbb{Z}_m^*$ on syklinen (eli mollä on primitiivinen juuri) jos ja vain jos $m = 2$, $m = 4$, $m = p^e$ tai $m = 2p^e$, missä $p \in \mathbb{P} \setminus \{2\}$ ja $e \ge 1$.

Tod Sivuutetaan (emme novella tätä tietoa jatkossa) □

Primitiivisiä juuria voi käyttää muotoa $x^n \equiv b \pmod p$ olevien kongruenssien ratkaisemisessa.

Esim. Montako juurta on yhtälöllä
$x^{28} \equiv 1 \pmod{71}$?

Ratk. Olkoon $a \in \{1, \dots, 70\}$ jokin primitiivinen juuri (mod 71). Jos $x \equiv a^j$ $(j \in \{0, \dots, 69\})$, niin
$$x^{28} \equiv 1 \iff a^{28j} \equiv 1 \iff 70 \mid 28j$$
$\iff 5 \mid 2j$, eli $j = 5k$, $k \geq 0$. Eri ratkaisuja on 14: $a^0 = 1, a^5, a^{10}, \dots, a^{65}$. □

Huom. Jos edellä tietäisimme prim. juuren, saisimme ratkaisuja x:ää!

Primitiiviset juuret liittyvät kiehtovalla tavalla luvun $1/n$ desimaalikehitelmän jakson pituuteen. Katsotaan ensin esimerkkejä: (oletetaan että $(n, 10) = 1$)

$1/3 = 0,\underline{3}33\dots$ (jakson pituus 1)
$1/7 = 0,\underline{142857}142857\dots$ (" 6)
$[1/9 = 0,\underline{1}11\dots$ (" 1)] $9 \notin \mathbb{P}$
$1/11 = 0,\underline{09}0909\dots$ (" 2)
$1/13 = 0,\underline{076923}076923$ (" 6)
$1/17 = 0,\underline{0588235294117647}05\dots$ (" 16)

Huomaamme, että osa jaksoista on poikkeuksellisen pitkiä, eli joillakin $p \in \mathbb{P}$ pätee: jakson pituus on $p-1$. Selitykseen havainnolle tarjoaa:

Lause 3.12 Olkoon $p \in \mathbb{P}$ ja $p \geq 7$. Luvun $\frac{1}{p}$ desimaalikehitelmän jakson pituus on $\mathrm{ord}_p(10)$. Erityisesti pituus on mahdollisimman, eli $p-1$, täsmälleen silloin kun 10 on primitiivinen juuri $(\mathrm{mod}\ p)$.

Tod. Olk. $\ell = \mathrm{ord}_p(10)$ ja olkoon $j \geq 1$ luvun $1/p$ desimaalikehitelmän jakson pituus.

① $j \leq \ell$ Luvun ℓ määritelmän nojalla

$$a := (10^\ell - 1)/p \in \mathbb{N}$$

ja selvästi $1 \leq a \leq 10^\ell - 1$. Täten

$$\frac{1}{p} = \frac{a}{10^\ell - 1} = \frac{a}{10^\ell(1-10^{-\ell})} = \frac{a}{10^\ell} + \frac{a}{10^{2\ell}} + \frac{a}{10^{3\ell}} + \dots,$$

mistä näemme, että $1/p$:llä on jaksollinen kehitelmä, jakson pituus $j \leq \ell$.

② $j \geq \ell$ Kirjoitetaan $1/p$:n jaksollinen kehitelmä muotoon

$$\frac{1}{p} = \frac{b}{10^k} + \frac{a}{10^{k+j}} + \frac{a}{10^{k+2j}} + \dots,$$

missä $b \in \{0,1,\dots,10^{k-1}\}$ $(k \geq 0)$ on desimaali. kehitelmän mahdollinen alkuosa, ja jakso on $a \in \{1,2,\dots,10^j - 1\}$, missä $j \geq 1$ on jakson pituus $(a \neq 0$, miksi?$)$. Summaamalla geometrisen sarjan saamme

$$b10^{-k} + 10^{-k}\frac{a}{10^j - 1} = \frac{1}{p}, \text{ eli}$$

$$p(b(10^j - 1) + a) = 10^k(10^j - 1)$$

Siis $p \mid 10^k(10^j - 1)$, eli $p \mid (10^j - 1)$ (koska $(p, 10) = 1$). Täten $\ell \mid j$ (Lause 3.7 (i)), joten $j \geq \ell$. $\square$

Avoin ongelma (Gauss) Onko olemassa ääretön monta alkulukua p, joille $1/p$:n desimaalikehitelmän jakso on mahdollisimman eli sen pituus on $p-1$. Yhtäpitävästi: onko olemassa ääretön monta alkulukua p joille 10 on primitiivinen juuri (mod p)?

Huom. Vastaus on positiivinen jos oletetaan n.s. yleistetty Riemannin hypoteesi (Hooley 1969). 1980-luvulla on todistettu, että on olemassa enintään 2 alkulukua, jotka eivät ole primitiivisiä juuria (mod 9) ääretön monella 9:n arvolla.

4. NELIÖNJÄÄNNÖKSET JA 2. ASTEEN KONGRUENSSIT

Luvun keskeisin aihe on 2. asteen kongruenssien ratkaiseminen. Niillä on luonnollisia yhteyksiä muihin lukuteorian kysymyksiin. 2. asteen yhtälön ratkaisuna epätriviaalein osa on neliöjuuren otto. Vastaavasti 2. asteen kongruenssien ydinkysymys on

Q1: Olkoon $(a,m)=1$. Milloin $x^2 \equiv a \pmod m$ ratkeaa?

Yhtäpitävästi

Q1': Olkoon $(a,m)=1$. Milloin alkiolla $[a]$ on neliöjuuri $\mathbb{Z}_m$:ssä?

Osoitamme aluksi, että ongelma voidaan palauttaa tapaukseen $m \in \mathbb{P}$. Lisäksi tapaus $(a,m)>1$ voidaan helposti palauttaa tilanteeseen $(a,m)=1$.

Tarkastelemme ensin tapausta $m = 2^e$.

Lemma 4.1. Olkoon a pariton (eli $(2,a)=1$) ja $e \geq 1$. Silloin kongruenssi

(1) $x^2 \equiv a \pmod{2^e}$

ratkeaa jos ja vain jos

(i) $e=1$ (ratkaisuja 1)

(ii) $e=2$ ja $a \equiv 1 \pmod 4$ (ratkaisuja 2)

(iii) $e \geq 3$ ja $a \equiv 1 \pmod 8$ (ratkaisuja 4)

Tod. (i) Selvästi $x \equiv 1 \pmod 2$ on (ainoa) ratkaisu.

(ii) Ratkaisun tulee olla pariton, eli $x \equiv \pm 1 \pmod 4$. Nyt $(\pm 1)^2 \equiv 1 \pmod 4$, joten tulee olla $a \equiv 1 \pmod 4$ ja tällöin ratkaisuja on kaksi: $x \equiv \pm 1 \pmod 4$.

(iii) Olkoon ensin $e = 3$. Kokeilemalla $x \equiv \pm 1$ tai $x \equiv \pm 3$ näemme, että tulee olla $a \equiv 1 \pmod 8$ ja tällöin kaikki nämä neljä jäännösluokkaa antavat ratkaisun.

Yleinen tapaus $e \geq 3$ & $a \equiv 1 \pmod 8$ seuraa kun todistamme induktiolla väitteen:

VÄITE: jos $e \geq 3$ ja $a \equiv 1 \pmod 8$, niin kongruenssilla (1) on 4 ratkaisua joukossa $\{0, 1, \ldots, 2^e - 1\}$, joista tasan 2 ratkaisee (1):n myös modulin 2^{e+1} suhteen.

Väitteen tod. (ei vaadita kokeessa!) Kun $e = 3$, ratkaisuja olivat ± 1 ja ± 3. Jos $a = 1 \pmod{16}$, näistä ± 1 ratkaisevat (1):n myös (mod 16). Jos $a = 9 \pmod{16}$, näistä ± 3 ratkaisevat (1):n myös (mod 16). Siis väite pätee kun $e = 3$.

Oletetaan sitten, että väite on voimassa arvolla $e \geq 3$, eli luvuista $\{0, 1, \ldots, 2^e - 1\}$ tasan 4 (olkoot ne x_1, x_2, x_3, x_4) ratkaisee (1):n (mod 2^e) ja näistä kaksi (olkoot ne x_1 ja x_2) ratkaisevat (1):n (mod 2^{e+1}).

Koska jokainen ratkaisu (1):lle (mod 2^{e+1}) on myös ratkaisu (mod 2^e), niin löytyvät kongruenssin (2) $x^2 \equiv a \pmod{2^{e+1}}$

ratkaisut luvuista $x_1, x_2, x_3, x_4, x_1+2^e$, x_2+2^e, x_3+2^e ja x_4+2^e joukosta. Induktio-oletuksen mukaan x_3 ja x_4 eivät ole ratkaisuja. Silloin myös x_3+2^e ja x_4+2^e eivät ole, koska

$$(3)\quad (x_j+2^e)^2 = x_j^2 + 2^{e+1}x_j + 2^{2e} \equiv x_j^2 \pmod{2^{e+1}} \quad j=1,2,3,4.$$

Lisäksi (3):n mukaan x_1+2^e ja x_2+2^e ovat ratkaisuja. Yhteensä: kongruenssilla (3) on ratkaisut $x_1, x_2, x_1+2^e, x_2+2^e$.

Väitteen todistusta seuraa kun havaitsemme että tasan yksi luvuista x_j ja x_j+2^e (nyt $j=1,2$) toteuttaa kongruenssin

$$(4)\quad x^2 \equiv a \pmod{2^{e+2}}.$$

Tämä seuraa huomaamalla, että (muista, että x_j on pariton!)

$$\begin{aligned}&[(x_j+2^e)^2 - a] - (x_j^2 - a)\\ &= 2^{e+1}x_j + 2^{2e} = 2^{e+2}\left(\frac{x_j-1}{2} + 2^{e-2}\right) + 2^{e-1}\\ &\equiv 2^{e-1} \pmod{2^{e+2}}\end{aligned}$$

. □

Seuraavaksi tarkastelemme tapausta, missä $m = p^e$, $p \in \mathbb{P}$, $p \geq 3$. Tällöin Q1:n ratkaisu palautetaan tapaukseen $e=1$.

Lemma 4.2. Olkoon $p \geq 3$, $p \in \mathbb{P}$, $e \geq 1$ ja $(a,p)=1$. Kongruenssilla $x^2 \equiv a \pmod{p^e}$ on ratkaisu vain jos kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisu, jolloin ratkaisuja on tasan 2 kappaletta.

Tod. Ehdon välttämättömyys on selvä. Oletetaan sitten, että kongruenssilla $x^2 \equiv a \pmod p$ on ainakin yksi ratkaisu:

$$x_1^2 \equiv a \pmod p.$$

Jos x_2 on toinen ratkaisu, niin $x_1^2 \equiv x_2^2 \pmod p$, eli $p \mid (x_1 - x_2)(x_1 + x_2)$. Koska $p \nmid (x_1 - x_2)$, niin $p \mid (x_1 + x_2)$ eli $x_2 \equiv -x_1 \pmod p$.
Lisäksi $-x_1 \not\equiv x_1 \pmod p$ (koska $p \geq 3$ ja $p \nmid x_1$), joten kongruenssilla $x^2 \equiv a \pmod p$ on tasan 2 ratkaisua: luvut $\pm x_1$.

Osoitetaan seuraavaksi, että tarkasteltavanamme kysymyksenä kongruenssilla $x^2 \equiv a \pmod{p^e}$ on tasan kaksi ratkaisua. Edellisen nojalla tämä on totta kun $e = 1$. Oletetaan, että se on totta kun $e \geq 1$, eli kongruenssilla $x^2 \equiv a \pmod{p^e}$ on kaksi ratkaisua. Jos toinen niistä on x_1, niin toinen on $-x_1$, jonka näemme kuten edellä. Kongruenssin

$$x^2 \equiv a \pmod{p^{e+1}}$$

ainoat mahdolliset ratkaisut löytyvät joukosta

$$x = \pm x_1 + k p^e, \quad k \in \{0, 1, \ldots, p-1\}.$$

Nyt $(\pm x_1 + k p^e)^2 \equiv a \pmod{p^{e+1}}$

$$\iff p \mid \left(\frac{x_1^2 - a}{p^e} \pm 2 k x_1 \right),$$

ja tällä on 1-käsitteinen $k \in \{0, 1, \ldots, p-1\}$ ratkaisuna kummallakin etumerkillä, sillä $(p, 2x_0) = 1$. □

H7: Yritä todistaa edellinen lemma sivujen 40-41 tarkastelujen avulla!

Voimme nyt koota aiemmat havaintomme yhdeksi lauseeksi:

Lause 4.3. Olkoon $(a,m)=1$, $m \geq 2$.

(i) Kongruenssilla $\boxed{x^2 \equiv a \pmod m}$ (*)

on ratkaisu vain jos sillä on ratkaisu jokaisen parittoman alkulukumoduulin $p \mid m$ suhteen ja lisäksi $a \equiv 1 \pmod 4$ jos $4 \mid m$ ja $a \equiv 1 \pmod 8$ jos $8 \mid m$.

(ii) Olkoon $m = 2^e p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$, missä $e, e_1, \dots, e_\ell \geq 1$ ja $2 < p_1 < p_2 < \dots < p_\ell$ ovat alkulukuja. Jos kongruenssilla (*) on ratkaisuja, on niiden lukumäärä $2^{\ell+E}$, missä

$$E = \begin{cases} 0 & \text{jos } e \leq 1 \\ 1 & \text{jos } e = 2 \\ 2 & \text{jos } e \geq 3. \end{cases}$$

Tod. Voite seuraa suoraan Lemmoista 4.1, 4.2 sekä sivujen 39–41 tarkastelusta ('ASKEL 1'). □

Määr. Olkoon $m \geq 2$ ja $(a,m)=1$. Luku a on *neliönjäännös* $\pmod m$ jos kongruenssilla $x^2 \equiv a$ on ratkaisu. Muussa tapauksessa a on *neliönepäjäännös* *) $\pmod m$.

---

*) Englanniksi: 'quadratic residue', quadratic nonresidue.

Esim. $m=7$. Laskemalla luvuille $(\pm 3)^2, (\pm 2)^2, (\pm 1)^2$ jäännösluokat saamme, neliönjäännökset; siis x on neliönjäännös jos $x \equiv 1$ tai $x \equiv 2$ tai $x \equiv 4 \pmod 7$. Luku x on neliönepäjäännös $\pmod 7$ jos $x \equiv 3$, $x \equiv 5$ tai $x \equiv 6 \pmod 7$.

Huom. Lauseen 4.3 avulla voimme määrätä neliönjäännökset jos saamme sen $\pmod p$, missä p on pariton alkuluku. Loppuosan tätä lukua tutkimmekin tätä tapausta.

Legendren symboli ja Eulerin kriteerio.

Määr. (Legendren symboli) Olkoon $p \in P$, $p \geq 3$. Asetetaan:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{jos } a \text{ on neliönjäännös } \pmod p \\ -1 & \text{jos } a \text{ on neliön epäjäännös } \pmod p \\ 0 & \text{jos } p \mid a. \end{cases}$$

Esim. $1 = \left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right)$, $0 = \left(\frac{a}{7}\right)$,

$-1 = \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right)$ (vrt. edell. esim.). □

Lause 4.4. Olkoon $p \geq 3$, $p \in P$. Neliönjäännöksiä ja neliönepäjäännöksiä $\pmod p$ on yhtä paljon, eli kumpiakin $\frac{p-1}{2}$ kpl.

Tod. Koska $p \geq 3$ on pariton, on $\{0, \pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}\}$ täydellinen jäännösjoukko $(\bmod p)$! Siinä neliönjäännöksiä ovat luvut, jotka ovat kongruentteja jonkin luvuista

$$\{1^2, 2^2, \ldots, \left(\tfrac{p-1}{2}\right)^2\}$$ kanssa.

Nämä ovat eri luokkia $(\bmod p)$, sillä jos $k,j \in \{1,2,\dots,\frac{p-1}{2}\}$ ja $k^2 \equiv j^2 \pmod p$, niin $p \mid (k-j)(k+j)$. Tämä $2 \le k+j \le p-1$, joten $p \mid (k-j)$, eli $k=j$. Siis relionjäännöksiä on $\frac{p-1}{2}$ kpl, ja -epäjäännöksiä $p-1-\frac{p-1}{2} = \frac{p-1}{2}$ kpl. □

Lause 4.5. (Eulerin kriteerio) Jos $p \in \mathbb{P}$, $p \ge 3$, niin kaikilla $a \in \mathbb{Z}$ pätee $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

Tod. Jos $p \mid a$, väite on ilmeinen. Seurauksen 3.5 nojaan kongruenssilla

$$(*) \qquad x^{\frac{p-1}{2}} \equiv 1 \pmod p$$

on tasan $\frac{p-1}{2}$ juurta. Jos a on relionjäännös $\pmod p$, niin $a \equiv k^2 \pmod p$ jollakin k (ja $p \nmid k$), joten

$$a^{\frac{p-1}{2}} \equiv k^{p-1} \equiv 1 \pmod p$$

Fermat'n pienen lauseen nojalla, eli a toteuttaa $(*)$:n. Epäkongruentteja relionjäännöksiä on $\frac{p-1}{2}$ kpl, joten $(*)$:n ratkaisuina ovat tämänlaiset kaikki relionjäännökset.

Jos taas a on relionepäjäännös, niin Fermatin pieni lause $\Rightarrow$

$$p \mid (a^{p-1}-1) \iff p \mid (a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1)$$
$$\iff p \mid (a^{\frac{p-1}{2}}-1) \text{ tai } p \mid (a^{\frac{p-1}{2}}+1)$$

Edellisen nojalla ensimmäinen vaihtoehto ei voi toteutua, joten nyt $p \mid (a^{\frac{p-1}{2}}+1)$. □

Seuraus 4.6. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Tod. Eul krit $\Rightarrow \left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$, jolloin ainoa vaihtoehto on että $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Seuraavissa tehtävissä näytetään, että aritmeettiset jonot $4n \pm 1$ kumpikin sisältävät ∞ monta alkulukua. Dirichlet todisti 1837 nerokkaan analyysia soveltavan todistuksen, kautta, että aritmeettinen jono $an+b$ $(n \geq 1)$ sisältää ∞ monta alkulukua, jos $(a,b)=1$.

[Teht. Osoita, että jono $4n-1$ $(n \geq 1)$ sisältää ∞ monta alkulukua.

Ratk. Vastaoletus: vain alkuluvut $p_1, \dots, p_s$ ovat tätä muotoa. Tarkastellaan lukua $b := 4p_1p_2 \cdots p_s - 1$. Nyt b:n jokainen alkutekijä on muotoa $4n+1$, jolloin b myös tulona on muotoa $4n+1$, mikä on ristiriita.

Teht. Osoita, että jono $4n+1$ $(n \geq 1)$ sisältää ∞ monta alkulukua.

Ratk. Vastaoletus: vain alkuluvut $p_1, \dots, p_s$ ovat tätä muotoa. Tarkastellaan lukua

$$a := (2p_1 \cdots p_s)^2 + 1.$$

Olkoon $q \in P$ luvun a alkutekijä. Silloin $q \geq 3$ ja $q \notin \{p_1, \dots, p_s\}$, eli q on muotoa $4n-1$. Toisaalta $q \mid ((2p_1 \cdots p_s)^2 + 1)$ tarkoittaa sitä, että luku -1 on neliönjäännös (mod q). Seurauksen 4.6 nojalla siis $(-1)^{(q-1)/2} = 1$ eli q on muotoa $4n+1$, mikä on ristiriita. $\square$

Huom Edellisen tulos oli epätriviaali: Mieti mitä väite sanoo – on olemassa x jolle $p \mid (x^2+1)$ vain jos alkuluku p on muotoa $4n+1$ (huomaa, että jokaisen parittoman alkuluvun on muotoa $4n \pm 1$). Sen sijaan havainto $\left(\frac{1}{p}\right)=1$ on triviaali (miksi?) !

Lause 4.7. Olk. $p \geq 3$, $p \in \mathbb{P}$. Tällöin

(i) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad \forall\, a,b \in \mathbb{Z}$

(ii) $\left(\frac{a^2}{p}\right) = 1$ jos $p \nmid a$.

Tod. (i) Eulerin kriteerion nojalla

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

Koska $\left(\frac{\bullet}{p}\right) \in \{-1,0,1\}$, täytyy olla voimassa yhtäsuuruus.

(ii) Seuraa suoraan (i):stä (tai Legendren symbolin määritelmästä). $\square$

Jos $n = \varepsilon q_1^{e_1} q_2^{e_2} \cdots q_\ell^{e_\ell}$,

missä $\varepsilon \in \{\pm 1\}$ ja q_i:t ovat eri alkulukuja, niin edellisen lauseen nojalla

$$\left(\frac{n}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{q_1}{p}\right)^{e_1} \cdots \left(\frac{q_\ell}{p}\right)^{e_\ell}.$$

Tässä $\left(\frac{\varepsilon}{p}\right)$ määräytyy helposti seurauksen 4.6 avulla. On siis riittävää kyetä laskemaan $\left(\frac{2}{p}\right)$ ja $\left(\frac{q}{p}\right)$, missä $q \in \mathbb{P}$ on pariton.

Gaussin lemma

auttaa meitä määräämään symbolin $\left(\frac{2}{p}\right)$ ja reziprookkilauseen todistuksessa. Todistamme lemmasta kaksi versiota, joista seuraava on ensimmäinen:

Lemma 4.8 (Gauss) Olkoon $p \in \mathbb{P}$, $p \geq 3$ ja $(a,p) = 1$. Olkoon μ niiden joukon $\{a, 2a, \ldots, \frac{p-1}{2}a\}$ lukujen lukumäärä, joiden itseisarvoltaan pienin jäännös $(\bmod p)$ on negatiivinen. Silloin

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

(Huom. Luvun $a \in \mathbb{Z}$ itseisarvoltaan pienin jäännös $(\bmod p)$ on luku r, jolle

$$r \in \left\{-\tfrac{p-1}{2}, -\tfrac{p-1}{2}+1, \ldots, \tfrac{p-1}{2}\right\} \text{ ja } a \equiv r \pmod p \,)$$

Tod. Olkoot $c_1, c_2, \ldots, c_{\frac{p-1}{2}}$ lukujen $a, 2a, \ldots, \frac{p-1}{2}a$ itseisarvoltaan pienimmät jäännökset. Kertomalla luvut keskenään tulee

$$1 \cdot 2 \cdot \ldots \cdot \left(\tfrac{p-1}{2}\right) a^{\frac{p-1}{2}} \equiv (-1)^{\mu} |c_1||c_2| \ldots |c_{\frac{p-1}{2}}| \pmod p.$$

Jos näytämme, että luvut $|c_1|, |c_2|, \ldots, |c_{\frac{p-1}{2}}|$ ovat luvut $1, \ldots, \frac{p-1}{2}$ jossakin järjestyksessä, voimme jakaa kongruenssin puolittain luvulla $\left(\frac{p-1}{2}\right)!$ (vrt. Lemma 2.11) ja saamme suoraan Eulerin kriteerion.

Koska joka tapauksessa $1 \leq |c_j| \leq \frac{p-1}{2}$, riittää osoittaa, että $|c_j| \neq |c_k|$ jos $j \neq k$. Jos olisi $|c_j| = |c_k|$, olisi $c_j \equiv \pm c_k \pmod p$, eli $p \mid (j \pm k)a$. Nyt $|j \pm k| \leq p-1$, joten tulee olla $j = k$. □

= "x:n lokeroisuus"

Otetaan käyttöön merkintä: jos $x \in \mathbb{R}$, niin $\lfloor x \rfloor = n$, missä $n = \max\{j \in \mathbb{Z} \mid j \leq x\}$

(voi nimittä selkeisiin jäännösluokkien merkinnän kanssa, mutta yleensä selvää asiayhteydestä.

Gaussin lemman avulla voimme määritellä symbolin $\left(\frac{2}{p}\right)$.

Lause 4.9. $\left(\frac{2}{p}\right) = 1$ jos $p \equiv \pm 1 \pmod 8$

$\left(\frac{2}{p}\right) = -1$ jos $p \equiv \pm 3 \pmod 8$.

Toisin sanoen, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Tod. Valitaan Gaussin lemmassa $a = 2$. Silloin on tarkasteltava lukujen $2, 4, \ldots, (p-1)$ itseisesti pienimpiä jäännöksiä. Näistä positiivisia ovat ne joille

$$2j \leq \frac{p-1}{2},$$

ja tällaisia j on $\left\lfloor \frac{p-1}{4} \right\rfloor$ kpl, eli negatiivisia itseisesti pienimpiä jäännöksiä on

$$\mu = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor \text{ kpl.}$$

Jokainen alkuluku $p \geq 3$ on muotoa

$$8k + a, \qquad a \in \{1, 3, 5, 7\}.$$

Jos $a = 1$, niin $\mu = 4k - 2k = 2k \equiv 0 \pmod 2$
Jos $a = 3$, niin $\mu = 4k+1 - 2k = 2k+1 \equiv 1 \pmod 2$
Jos $a = 5$, niin $\mu = 4k+2 - (2k+1) = 2k+1 \equiv 1 \pmod 2$
Jos $a = 7$, niin $\mu = 4k+3 - (2k+1) = 2k+2 \equiv 2 \pmod 2$,

mistä väite seuraa Gaussin lemman nojalla. Kaava $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ seuraa nyt testaamalla eri a:n arvot. □

Esim. $x^2 \equiv 2 \pmod{113}$ ratkaisu, sillä $113 \equiv 1 \pmod 8$ - pienin ratkaisu $x \equiv 51$ (hokeilemalla!).

Reziprookkilauseetta varten on hyödyllistä esittää uusi versio Lemmasta 4.8.

Lemma 4.10 (Gaussin lemman toinen versio)
Olkoon $p \in \mathbb{P}$, $p \geq 3$, a pariton ja $(a,p)=1$. Silloin
$$\left(\frac{a}{p}\right) = (-1)^t, \text{ missä } t = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor .$$

Tod. Havaitaan ensin, että kun $j \in \{1, \dots, \frac{p-1}{2}\}$,
$$ja = p\left\lfloor \frac{ja}{p} \right\rfloor + r_j \quad , \quad r_j \in \{1,2,\dots,p-1\}$$
(huomaa, että $p \nmid a$). Kirjoitetaan
$$\{r_1, \dots, r_{\frac{p-1}{2}}\} = \{s_1, s_2, \dots, s_\mu\} \cup \{t_1, \dots, t_\nu\},$$
missä $\mu+\nu = \frac{p-1}{2}$ ja $s_j > \frac{p-1}{2}$ sekä $t_k < \frac{p-1}{2}$ jokaisella k,j. Toisin sanoen, luvuja $s_1, \dots, s_\mu$ vastaavat ne tapaukset, joissa luvun ja itseisarvoltaan pienin jäännös on negatiivinen. Siis luvuilla ja $(1 \leq j \leq \frac{p-1}{2})$ itseisarvoltaan pienimmät jäännökset ovat luvut
$$s_1 - p, s_2 - p, \dots s_\mu - p, t_1, t_2, \dots, t_\nu$$
ja Gaussin lemman todistuksessa (s. 60) osoitimme, että
$$\{1,2,\dots,\tfrac{p-1}{2}\} = \{p-s_1, p-s_2, \dots, p-s_\mu\} \cup \{t_1, t_2, \dots, t_\nu\}$$
Voimme nyt laskea $\pmod 2$ pitäen mielessä havainnot: $\boxed{-1 \equiv 1 \pmod 2}$, $\boxed{a \equiv 1 \pmod 2}$ (oletus) ja $\boxed{p \equiv 1 \pmod 2}$ $(p \in \mathbb{P}, p \geq 3)$:

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{\mu} (p - s_i) + \sum_{k=1}^{\nu} t_k$$

$$\equiv \mu p + \sum_{i=1}^{\mu} s_i + \sum_{k=1}^{\nu} t_k$$

$$= \mu p + \sum_{j=1}^{(p-1)/2} r_j$$

$$= \mu p + \sum_{j=1}^{(p-1)/2} (ja - p\lfloor \tfrac{ja}{p} \rfloor)$$

$$\equiv \mu + \sum_{j=1}^{(p-1)/2} j - \sum_{j=1}^{(p-1)/2} \lfloor \tfrac{ja}{p} \rfloor$$

Vertaamalla alkua ja loppua saamme

$$\mu \equiv \sum_{j=1}^{(p-1)/2} \lfloor \tfrac{ja}{p} \rfloor \,,$$

ja väite seuraa lemmasta 4.5. □

Kvadraattinen reziprookkilause

Olemme nyt valmiit esittämään yhden lukuteorian päätuloksista. Gauss löysi sille ensimmäisen todistuksen – hän kutsui teoreemaa nimellä 'Theorema Aureum'. Kyseinen tulos omaa kaikki 'kullan' tuoksuun kuuluvat tunnusmerkit: se on helppo lausua, on erittäin yllättävä ja todistus aivan epätriviaali. Lisäksi tulos on sovellusrelevanssi sekä konkreettisella että teoreettisella tasolla. Artinin yleisen reziprookkilauseen kautta tulos on yhteydessä ns. Langlandsin ohjelmaan, joka on eräiden tunnettujen matematiikkojen mielestä 'The Holy Grail of Number Theory today'.

Lause 4.11 (Kvadraattinen reziprookkilause)
Olkoot p ja q erisuuria parittomia alkulukuja. Silloin
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Huom. Toisin sanoen, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ paitsi jos sekä p että q ovat muotoa $4n-1$.

Tod. Tavoitteemme on lopussa käyttää soveltaa Lemmaa 4.10. Olkoon S niiden kokonaislukuparien $(x,y) \in \mathbb{Z}^2$ joukko, joille
$$1 \le x \le \frac{p-1}{2}, \quad 1 \le y \le \frac{q-1}{2}.$$
Silloin $\#(S) = \frac{p-1}{2}\cdot\frac{q-1}{2}$. Olkoon
$$S_1 := \{(x,y) \in S \mid qx > py\} \quad \text{ja}$$
$$S_2 := \{(x,y) \in S \mid qx < py\}.$$

Nyt $S = S_1 \cup S_2$, sillä $qx = py \Rightarrow (x,y) \notin S$.
Jos $x \in \{1, \dots, \frac{p-1}{2}\}$, niin pari $(x,y) \in S_1$ kun $y < \frac{q}{p}x \Leftrightarrow y \le \frac{q}{p}x$, sillä $\frac{q}{p}x$ ei ole kokonaisluku kyseessä tulevilla x:n arvoilla. Tällaisten parien lukumäärä on siis $\lfloor \frac{xq}{p} \rfloor$, *) eli voimme laskea:
$$\#(S_1) = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor.$$

Vastaavasti $\#(S_2) = \sum_{k=1}^{\frac{q-1}{2}} \lfloor \frac{kp}{q} \rfloor$.
Gaussin lemman toisen version (Lemma 4.10) nojalla siis
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\#(S_1)}\,(-1)^{\#(S_2)} = (-1)^{\#(S_1)+\#(S_2)}$$
$$= (-1)^{\#(S)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \quad \square$$

*) On myös syytä havaita, että $\left\lfloor \frac{p-1}{2}\cdot\frac{q}{p} \right\rfloor \le \frac{q-1}{2}$ (HT)

Reziprookkilauseen avulla voi mm. laskea konkreettisesti Legendren symbolin arvoja suurillakin moduleilla.

Esim. $\left(\frac{2819}{4177}\right)$? Tässä $4177, 2819 \in \mathbb{P}$, $4177 \equiv 1 \pmod 4$

Käyttämällä toisistuvarti lauseita 4.9 ja 4.11 voimme laskea:

$$\left(\frac{2819}{4177}\right) = \left(\frac{4177}{2819}\right) = \left(\frac{1358}{2819}\right) \qquad 2819 \equiv 3 \pmod 8$$

$$= \left(\frac{2}{2819}\right)\left(\frac{7}{2819}\right)\left(\frac{97}{2819}\right) = (-1)\cdot\left(-\left(\frac{2819}{7}\right)\right)\cdot\left(\frac{2819}{97}\right)$$

$$= \left(\frac{5}{7}\right)\left(\frac{6}{97}\right) = \left(\frac{7}{5}\right)\left(\frac{2}{97}\right)\left(\frac{3}{97}\right)$$

$$= \left(\frac{2}{5}\right)\left(\frac{2}{97}\right)\left(\frac{97}{3}\right) = (-1)\cdot 1\cdot \underbrace{\left(\frac{1}{3}\right)}_{=1} = -1.$$

Siispä 2819 ei ole neliönjäännös 4177. □

Tarkastellaan lopuksi yleistä 2. asteen kongruenssia

$$(1)\quad ax^2 + bx + c \equiv 0 \pmod p,$$

missä $p \in \mathbb{P} \setminus \{2\}$ ja $p \nmid a$. Nyt $\mathbb{Z}_p$ on kunta ja voimme laskea yhtäpitävästi:

$$[a][x]^2 + [b][x] + [c] = [0]$$

Merkitsemme 1-kertaisuuden summia $[0] = 0$, $[2] = 2$, $[4] = 4$ jne. Lisäksi merkitsemme $[x] = z$. Voimme kertoa puolittain $4[a]$:lla, sillä oletuksesta seuraa $4[a] \neq 0$.

$$[a]z^2+[b]z+[c]=0$$
$$\Leftrightarrow \quad 4[a]^2z^2+4[a][b]z+4[a][c]=0$$
$$\Leftrightarrow \quad (2[a]z+[b])^2=[b]^2-4[a][c]$$

Merkitään $\Delta := b^2-4ac$ ('diskriminantti').
Jos $[\Delta]$ on neliö $\mathbb{Z}_p$:ssä, eli $[\Delta]=[y]^2$ jollekin $[y]\in\mathbb{Z}_p$, niin saamme ratkaisut

$$[x]=z=\frac{-[b]\pm[y]}{2[a]} \quad \left(=(2[a])^{-1}(-[b]\pm[y])\right).$$

Kun huomioimme että Formaalisti $[y]=\text{"}\sqrt{[\Delta]}\text{"}$, muistutta edellinen täysin toisaalla 2. asteen yhtälön ratkaisukaavaa.
Jos $[\Delta]$ ei ole neliö (eli $\sqrt{[\Delta]}$ ei ole määritelty) ei ratkaisuja ole.

Luonnollisestikin $[\Delta]$ on neliö täsmälleen silloin kun $y^2\equiv\Delta \pmod p$ jollekin y, eli jokko $p\mid\Delta$ tai Δ on neliöjäännös $(\bmod p)$.
Olemme todistaneet:

Lause 4.12 Jos $p\geq 3$, $p\in\mathbb{P}$, $p\nmid a$, niin kongruenssilla $ax^2+bx+c\equiv 0 \pmod p$ on ratkaisuja

- ei yhtään jos $\left(\frac{\Delta}{p}\right)=-1$
- yksi jos $\left(\frac{\Delta}{p}\right)=0$
- kaksi jos $\left(\frac{\Delta}{p}\right)=1$

Esim. Tutki onko kongruenssilla

$$x^2+12x-43\equiv 0 \pmod{151}$$

ratkaisuna.

Ratk. 151 on P. Diskriminantille pätee
$\Delta = 12^2 - 4\cdot(-43) = 316 \equiv 14 \pmod{151}$. Siis

$$\left(\frac{\Delta}{151}\right) = \left(\frac{2}{151}\right)\left(\frac{7}{151}\right) = 1 \cdot \left(-\left(\frac{151}{7}\right)\right) = -\left(\frac{4}{7}\right) = -\left(\frac{2}{7}\right)^2 = -1.$$

Ei ratkaisuja!

Esim. Kuinka monta ratkaisua on kongruenssilla $x^2 \equiv 113 \pmod{196}$?

Ratk. Nyt $196 = 2^2 \cdot 7^2$.

- Kongruenssilla $x^2 \equiv 113 \pmod 7$ on ratkaisu, sillä $\left(\frac{113}{7}\right) = \left(\frac{1}{7}\right) = 1$
- Kongruenssilla $x^2 \equiv 113 \pmod 4$ on ratkaisu sillä $113 \equiv 1 \pmod 4$ (kts. Lemma 4.7)
- $\Rightarrow$ (Lause 4.3) ratkaisuja on $2 \times 2 = 4$ kpl. □

5. DIOFANTEEN APPROKSIMAATIOTEORIA

Kuinka hyvin annettua reaalilukua voi approksimoida rationaaliluvuilla? Kysymys kuulostaa epämääräiseltä, koska $\mathbb{Q}$ on tiheässä $\mathbb{R}$:ssä. Kuitenkin voimme sanoa, että p/q on hyvä approksimaatio x:lle jos virhe $|p/q - x|$ on pieni suhteessa nimittäjään q kohoon (voimme tehdä oletuksen, että $(p,q)=1$).

Esim. Jos $x \in (0,1)$ ja $q \geq 1$, $q \in \mathbb{N}$, voimme jakaa välin $(0,1)$ osiin

$$\left(0, \tfrac{1}{q}\right), \left[\tfrac{1}{q}, \tfrac{2}{q}\right), \ldots, \left[\tfrac{q-1}{q}, 1\right).$$

Jos $x \in \left[\frac{k}{q}, \frac{k+1}{q}\right)$, niin $\left|x - \frac{k}{q}\right| < \frac{1}{q}$. Siispä valitulla nimittäjällä q saadaan virhe aina pienemmäksi kuin $1/q$.

Edellisen esimerkin tulosta ei voi oleellisesti parantaa kiinteällä q (valitse esim. $x = \frac{1}{2q}$). Sen sijaan, jos katsomme kaikkia nimittäjiä $q \leq t$, missä t on kiinnitetty, on voimassa huomattavasti parempi tulos:

Lause 5.1. (Dirichlet) Jos $x \in \mathbb{R}$ ja $t \in \mathbb{N}$, niin on olemassa kokonaisluvut n, m joille

$$|mx - n| \leq \frac{1}{t+1}, \quad 1 \leq m \leq t.$$

Tod. Voimme olettaa, että $x > 0$. Tarkastellaan desimaaliosia

(1) $x - \lfloor x \rfloor$, $2x - \lfloor 2x \rfloor$, $\ldots$, $tx - \lfloor tx \rfloor$.

Jaetaan väli $[0,1)$ $(t+1)$:een yhtäsuureen osaan

$$I_1 = \left[0, \tfrac{1}{t+1}\right), \ldots, I_{t+1} = \left[\tfrac{t}{t+1}, 1\right).$$

Jos jokin desimaalivisista on välillä I_1, esim. $kx - \lfloor kx \rfloor \in I_1$, voimme valita $m = k$, $n = \lfloor kx \rfloor$. Jos taas jokin luvuista väliin I_{t+1}, esim. $kx - \lfloor kx \rfloor \in I_{t+1}$, voimme valita $m = k$, $n = \lfloor kx \rfloor + 1$. Muissa tapauksessa desimaaliosat ovat väleillä $I_2, \dots, I_t$. Koska näitä välejä on $t-1$ kpl, desimaaliosia t kpl, tulee kahden niistä luvulla samalle välille (lokerikkoperiaate!) On siis olemassa luvut j_1, j_2 joille $1 \le j_1 < j_2 \le t$ ja

$$|(j_2 x - \lfloor j_2 x \rfloor) - (j_1 x - \lfloor j_1 x \rfloor)| \le \frac{1}{t+1}.$$

Nyt voimme valita $m = j_2 - j_1$ ja $n = \lfloor j_2 x \rfloor - \lfloor j_1 x \rfloor$.

Seuraus 5.2. (i) Olkoon $x \in \mathbb{R}$. Jokaisella $t \in \mathbb{N}$ on olemassa $p, q \in \mathbb{Z}$, joille $1 \le q \le t$ ja

$$|x - \frac{p}{q}| \le \frac{1}{(t+1)q} < \frac{1}{q^2}.$$

(ii) Olkoon x irrationaalinen: $x \in \mathbb{R} \setminus \mathbb{Q}$. On olemassa lukupareja $p, q \in \mathbb{Z}$, $q \ge 1$, joille q on mielivaltaisen suuri ja $|x - \frac{p}{q}| < \frac{1}{q^2}$.

Tod. (i) Lause 5.1 antaa luvut p, q $(1 \le q \le t)$ joille $|qx - p| \le 1/(t+1)$. Silloin

$$|x - \frac{p}{q}| \le \frac{1}{(t+1)q} < \frac{1}{q^2}.$$

(ii) Valitaan (i)-kohdassa jokaisella $k \in \mathbb{N}$ vastaavat luvut $p_k, q_k \in \mathbb{Z}$, joille

$$|x - \frac{p_k}{q_k}| \le \frac{1}{(k+1)q_k} < \frac{1}{q_k^2}$$

Tässä $\frac{1}{(k+1)q_k} \le 1/(k+1) \xrightarrow[k \to \infty]{} 0$, joten myös $|x - \frac{p_k}{q_k}| \xrightarrow[k \to \infty]{} 0$. Siispä $q_k \to \infty$ kun $k \to \infty$, koska $x \notin \mathbb{Q}$. □

Huom. Lauseen 5.2 (ii)-kohdan eksponenttia ei voi parantaa ! Esim, jos $x = \sqrt{2}$, niin on olemassa vain äärellisen monta paria (p,q), joille $|\sqrt{2} - \frac{p}{q}| \leq \frac{c}{q^{2+\varepsilon}}$ | $c, \varepsilon > 0$.
Tämä seuraa havaitsemalla, että itse asiassa aina pätee $|\sqrt{2} - \frac{p}{q}| > \frac{1}{4q^2}$! (Hodi HT)

Pellin yhtälö

Pellin yhtälöksi kutsutaan Diofantoksen yhtälöä

$$\boxed{x^2 - Dy^2 = 1} \qquad (D \in \mathbb{N},\ \sqrt{D} \notin \mathbb{Q})$$

Yhtälön tutkimuksella on yllättävän pitkä historia: babylonialaiset, Arkhimedes (?), Kiina, Intia, Arabia, Wallis, Brouncker, Fermat, Lagrange... . Sillä on monella tapaa tärkeä merkitys, mm. kunnan $\mathbb{Q}[\sqrt{D}]$ teoriassa.
Sovellamme lausetta 5.1 seuraavassa apulauseessa:

Lemma 5.3 Olkoon $D \geq 2$, $\sqrt{D} \notin \mathbb{Q}$. Silloin on olemassa $k \in \mathbb{Z} \setminus \{0\}$, jolle $|k| \leq 2\sqrt{D} + 1$ ja jolle yhtälöllä $x^2 - Dy^2 = k$ on äärettömän monta (kokonaisluku-) ratkaisua.

Tod. Valitaan lauseen 5.1 avulla jokaisella $t \geq 1$ kokonaisluvut x_t, y_t joille $1 \leq y_t \leq t$ ja

$$|y_t\sqrt{D} - x_t| \leq \frac{1}{t+1}.$$

Silloin $x_t \geq 1$ ja $x_t \leq y_t\sqrt{D} + 1 \leq t\sqrt{D} + 1$.
Siis

$$|x_k^2 - y_k^2 D| = |x_k + \sqrt{D} y_k| \, |x_k - \sqrt{D} y_k|$$
$$\leq (k\sqrt{D} + 1 + k\sqrt{D}) \frac{1}{k+1} \leq \frac{(2\sqrt{D}+1)k}{k+1}$$
$$\leq 2\sqrt{D} + 1.$$

Siis on luku $x_k^2 - y_k^2 D$ vain äärellisen monta arvoa*), jotenkin näistä toistuu ∞ monta kertaa, olkoon se k. Vastaavia ratkaisuparejoja (x_k, y_k) on myös ∞ monta, sillä kun k kasvaa, saa $|y_k\sqrt{D} - x_k|$ mielivaltaisen pieniä arvoja. □

Seuraavan lauseen todisti ensimmäisenä Lagrange:

Lause 5.4. Olkoon $D \in \mathbb{N}$, $\sqrt{D} \notin \mathbb{Q}$.

(i) Pellin yhtälöllä $x^2 - Dy^2 = 1$ (1) on aina epätriviaali kokonaislukuratkaisu (jolle $y \neq 0$).

(ii) Olkoon (x_1, y_1) yhtälön (1) pienin positiivinen ratkaisupari (siis $x_1, y_1 \geq 1$ ja y_1 pienin mahdollinen). Tällöin kaikki positiiviset ratkaisut (1):lle saadaan kaavasta

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n, \quad n \geq 1.$$

Erityisesti: Pellin yhtälöllä on aina ∞ monta ratkaisua.

Huom. (ii)-kohdan nojalla yhtälön (1) kaikki ratkaisut saadaan kaavasta

$$\pm x \pm y\sqrt{D} = (x_1 + y_1\sqrt{D})^n, \quad n \geq 0.$$

Tod. (i) Lemman 5.3 nojalla on olemassa

---

*) Se ei saa arvoa 0 (HT), jotenkin $k \neq 0$.

$k \neq 0$, $k \in \mathbb{Z}$, niin että yhtälöllä $x^2 - Dy^2 = k$ on ∞ monta ratkaisua. Siispä voimme valita luvut $x_1, x_2, y_1, y_2 \geq 1$, $x_1 \neq x_2$, $y_1 \neq y_2$ joille

$$\begin{cases} x_1^2 - Dy_1^2 = k = x_2^2 - Dy_2^2 \\ x_1 \equiv x_2 \pmod{k} \\ y_1 \equiv y_2 \pmod{k} \end{cases}$$

Pätee $(x_1 - y_1\sqrt{D})(x_1 + y_1\sqrt{D}) = k = (x_2 - y_2\sqrt{D})(x_2 + y_2\sqrt{D})$.
Merkitään

$$(x_1 - \sqrt{D}y_1)(x_2 + \sqrt{D}y_2) = (x_1x_2 - Dy_1y_2) + (x_1y_2 - x_2y_1)\sqrt{D}$$
$$=: z + w\sqrt{D}.$$

Selvästi pätee (laske!)

$$(2) \qquad k^2 = (z + w\sqrt{D})(z - w\sqrt{D}) = z^2 - w^2D$$

Nyt $w = x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 = 0 \pmod{k}$, eli $k \mid w$. Yhtälön (2) nojalla tällöin $k^2 \mid z^2$, joten $k \mid z$ (HT). Kun merkitsemme

$$x = z/k \quad \text{ja} \quad y = w/k,$$

niin $x, y \in \mathbb{Z}$ ja $x^2 - Dy^2 = 1$.
On vielä osoitettava, että $y \neq 0$.
Jos $y = 0$, niin $w = 0$ eli $x_1/y_1 = x_2/y_1$.
Silloin

$$\frac{k}{y_1^2} = \frac{x_1^2}{y_1^2} - D = \frac{x_2^2}{y_2^2} - D = \frac{k}{y_2^2},$$

joten $y_1 = y_2$, mikä on mahdotonta.

(ii) Olkoon nyt (x_1, y_1) pienin positiivinen ratkaisu ($x_1, y_1 \geq 1$, y_1 pienin mahdollinen).
Määritellään luvut (x_n, y_n) asettamalla

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n, \quad n \geq 1.$$

Silloin selvästi $(x_n - y_n\sqrt{D}) = (x_1 - y_1\sqrt{D})^n$
(ajattele binomikaavaa!) ja voimme laskea

$$x_n^2 - y_n^2 D = (x_n + y_n\sqrt{D})(x_n - y_n\sqrt{D})$$
$$= ((x_1 + y_1\sqrt{D})(x_1 - y_1\sqrt{D}))^n = (x_1^2 - Dy_1^2)^n = 1^n = 1.$$

Siis (x_n, y_n) on ratkaisu ja selvästi

$$y_1 < y_2 < y_3 < \dots$$

On vielä osoitettava, että muita positiivisia ratkaisuja ole. Vastaoletus tarkoittaa sitä, että olisi olemassa $x, y \in \mathbb{Z}$, $x, y \geq 1$ ja $y > y_1$ joille $x^2 - y^2 D = 1$ ja

$$x + y\sqrt{D} \neq x_n + y_n\sqrt{D} \quad \forall n \geq 1.$$

Silloin $x + y\sqrt{D} > x_1 + y_1\sqrt{D}$, sillä $x = \sqrt{1 + y^2 D}$ $> \sqrt{1 + y_1^2 D} = x_1$. Voimme valita luvun $n \geq 1$ jolle

$$(x_1 + y_1\sqrt{D})^n < x + y\sqrt{D} < (x_1 + y_1\sqrt{D})^{n+1}.$$

Koska $(x_1 + y_1\sqrt{D})^{-n} = (x_1 - y_1\sqrt{D})^n$, saamme

$$(3) \qquad 1 < \underbrace{(x + y\sqrt{D})(x_1 - y_1\sqrt{D})^n}_{=: a + b\sqrt{D}} < x_1 + y_1\sqrt{D}$$

Tämä $a^2 - Db^2 = (a + b\sqrt{D})(a - b\sqrt{D})$
$= (x + y\sqrt{D})(x_1 - y_1\sqrt{D})^n (x - y\sqrt{D})(x_1 + y_1\sqrt{D})^n$
$= (x^2 - Dy^2)(x_1^2 - Dy_1^2)^n = 1 \cdot 1 = 1$,
joten (a, b) on Pellin yhtälön ratkaisu.
Jos näytämme, että $a, b \geq 1$, seuraa (3):sta ristiriita, sillä sen nojalla

$$b + \sqrt{1 + b^2 D} < y_1 + \sqrt{1 + y_1^2 D},$$

eli $b < y_1$ ja (x_1, y_1) ei olisikaan pienin ratkaisu.

Nyt (3) $\Rightarrow a + b\sqrt{D} \geq 1$, $a - b\sqrt{D} = \frac{1}{a + b\sqrt{D}} \in (0, 1)$, joten $a = \frac{a - b\sqrt{D} + a + b\sqrt{D}}{2} > 0$, eli $a \geq 1$ ja lisäksi

$$b = \frac{1}{2\sqrt{D}}\left(\underbrace{a + b\sqrt{D}}_{\geq 1} - \underbrace{(a - b\sqrt{D})}_{\in (0,1)}\right) > 0, \text{ eli } b \geq 1 \qquad \square$$

Esim. Pellin yhtälöiden pienimpiä ratkaisuja:

$x^2 - 2y^2 = 1$: $x_1 = 3$
$x^2 - 3y^2 = 1$: $x_1 = 2$
$x^2 - 5y^2 = 1$: $x_1 = 9$
$\vdots$
$x^2 - 61y^2 = 1$: $x_1 = 1766319049$!

Huom. Arkhimedeen kuuluisa ongelma arvingon jonalan karjan lukumäärästä johtaa Pellin yhtälön ratkaisemiseen tilanteessa, jossa perusratkaisun on tavattoman suuri.

Algebrallisista ja transkendenttisista luvuista

Määr. Reaaliluku $x \in \mathbb{R}$ on algebrallinen jos se toteuttaa yhtälön

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 = 0,$$

missä $a_0, \dots, a_n \in \mathbb{Z}$ ja $a_n \neq 0$. Pienin mahdollinen n on x:n aste. Muussa tapauksessa x on transkendenttinen.

Huom. • $\mathbb{Q} = \{x \mid x \text{ algebrallinen, astetta } 1\}$

- Astetta $n \geq 2$ olevat algebralliset luvut ovat irrationaalisia.
- Astetta 2 olevat algebralliset luvut voidaan kirjoittaa muotoon $x = \frac{a+b\sqrt{D}}{c}$, missä $a, b, c, D \in \mathbb{Z}$, $D \geq 2$ ei ole neliö, $b \neq 0$, $c \neq 0$. (HT)

- Algebrallisia lukuja on vain numeroituva määrä (HT).
- Algebralliset lukujen muodostamat $\mathbb{R}$:n aliryhmän, jonka kaikkia alkioita ei voi esittää yksinkertaisilla (kokonais $\mathbb{Z}$:n alkioista) (Abel).

Seuraava, hieman yllättävä tulos osoittaa, että algebrallisia lukuja ei voi approksimoida liian hyvin rajoja paremmin.

Lause 5.5. (Liouville) Jos $x \notin \mathbb{Q}$ on algebrallinen luku astetta $n \geq 1$, niin on olemassa vakio $c = c(x) > 0$ niin että

$$|x - \frac{p}{q}| > \frac{c}{q^n} \quad \text{kaikilla } p, q \in \mathbb{Z},\ q \geq 1.$$

Tod Olkoon $a_n x^n + \dots + a_0 = 0$, $n \geq 2$, $a_n \neq 0$, $a_0, \dots, a_n \in \mathbb{Z}$. Merkitään $f(y) = a_n y^n + \dots + a_0$. On olemassa vakio M jolle pätee

$$|f'(y)| \leq M \quad \text{kun} \quad |y - x| \leq 1.$$

Rajoitutaan tarkastelemaan lukuja $\frac{p}{q}$, joille $q \geq 1$ ja

$$|\frac{p}{q} - x| \leq \min(1, \frac{h}{2}),$$

missä h on etäisyys x:stä lähimpään toiseen f:n nollakohtaan. Silloin

$$f(\frac{p}{q}) \neq 0 \qquad (\frac{p}{q} \neq x \text{ koska } x \notin \mathbb{Q})$$

ja voimme arvioida

$$|f(\frac{p}{q})| = \frac{\overbrace{|a_n p^n + a_{n-1} p^{n-1} q + \dots + a_0 q^n|}^{\in \mathbb{Z} \setminus \{0\}}}{q^n} \geq \frac{1}{q^n}.$$

Väliarvolauseen nojalla

$$F(p/q) = F(p/q) - \overset{0}{\overset{\shortparallel}{F(x)}} = (p/q - x)\,F'(\xi),$$

missä ξ on luvujen p/q ja x välissä. Siis

$$\left|\frac{p}{q} - x\right| = \frac{|F(p/q)|}{|F'(\xi)|} \geq \frac{1}{q^n M} \quad \square$$

Seuraus 5.6 (Liouville) *Kaikilla etumerkkien valinnoilla luvut*

$$\xi = 1 \pm \frac{1}{2^{1!}} \pm \frac{1}{2^{2!}} \pm \frac{1}{2^{3!}} \pm \dots$$

ovat transkendenttisia.

Tod. Kiinnitetään etumerkit. Määritellään

$$q_n = 2^{(n!)} \quad \text{ja} \quad p_n = q_n\left(1 \pm 2^{-1!} \pm 2^{-2!} \pm \dots \pm 2^{-(n-1)!}\right)$$

Silloin p_n/q_n on kys. sarjan osasumma ja

$$\left|\xi - \frac{p_n}{q_n}\right| \leq 2^{-n!} + 2^{-(n+1)!} + \dots \leq 2^{-n!}\left(1 + \tfrac{1}{2} + \tfrac{1}{4} + \tfrac{1}{8} + \dots\right)$$
$$\leq 2\,2^{-n!} = 2q_n^{-n}$$

Koska $\xi \notin \mathbb{Q}$ (117), on ξ transkendenttinen lauseen 5.5 nojalla. $\square$

Huom. • y.o. todistus on peräisin vuodelta 1844 ja oli ensi kertaa kirjoissa transkendenttiluvuista. Cantorin diagonaaliargumentti (mahtavuuksien vertailu) on vuodelta 1874.

- Luvut π ja e ovat transkendenttisia, mutta tämän todistus on varsin tekninen.

- Kuuluisa Thue-Siegel-Roth-lause sanoo, että jos x on m.v. algebrallisen luku, niin lause 5.5 vahvenee muotoon

$$\left|x - \frac{p}{q}\right| \geq \frac{C(\varepsilon, x)}{q^{2+\varepsilon}} \qquad \forall \varepsilon > 0.$$

Tällä on sovelluksia Diofantoksen yhtälöihin.

Ketjumurtoluvut

Sovelletaan Euklideen algoritmia luvuille 67 ja 24. Saadaan

$$\begin{cases} 67 = 2\times 24 + 19 \\ 24 = 1\cdot 19 + 5 \\ 19 = 3\cdot 5 + 4 \\ 5 = 1\cdot 4 + 1 \end{cases} \iff \begin{aligned} 67/24 &= 2 + \frac{19}{24} \\ 24/19 &= 1 + 5/19 \\ 19/5 &= 3 + 4/5 \\ 5/4 &= 1 + 1/4. \end{aligned}$$

Saamme peräkkäisten (alkioiden lopusta)

$$\frac{5}{4} = 1 + \frac{1}{4} \Rightarrow 19/5 = 3 + \frac{1}{1+\frac{1}{4}}$$

$$\Rightarrow \quad 24/19 = 1 + \frac{1}{3+\frac{1}{1+\frac{1}{4}}}$$

$$\Rightarrow \quad \boxed{\frac{67}{24} = 2 + \frac{1}{1+\frac{1}{3+\frac{1}{1+\frac{1}{4}}}}}$$

(Luvun 67/24 ketjumurtoesitys)

Tälle käytetään erilaisia merkintätapoja.

Esim. $67/24 = 2 + \frac{1}{1+} \frac{1}{3+} \frac{1}{1+} \frac{1}{4}$

tai $\boxed{\frac{67}{24} = \{2; 1, 3, 1, 4\}}$ (suosimme tätä)

Myös ääriettömiin (loppuvattomiin) ketjumurtokehitelmiin päädytään luonnollisella tavalla:

Esim. $x^2 - 3x - 1 = 0$. Ratkaisulle $x > 1$ löydetään approksimaatioita havaitsemalla

$$x = 3 + \frac{1}{x} = 3 + \frac{1}{3+\frac{1}{x}} = 3 + \frac{1}{3+\frac{1}{3+\frac{1}{x}}}$$

$$= \ldots \quad \{3; 3, 3, 3, \ldots\}.$$

Menetelmä herättää monia kysymyksiä:

- suppeneeko saatu ääretön ketjumurtokehitelmä?
- onko katkaistu kehitelmä hyvä approksimaatio x:lle? $\underbrace{3+\cfrac{1}{3+\cfrac{1}{3+\cdots}}}_{n\ 3:\text{sta}}$
- voidaanko kaikki reaaliluvut kehittää tällä tavoin?

Pian ogimme, että jokaisen em. kysymyksen vastaus on positiivinen! Mainittakoon, että esim. yllä

$$\left| x - 3+\cfrac{1}{3+\cfrac{1}{3+\cfrac{1}{3}}} \right| < 10^{-4}.$$

Oletetaan, että $\lambda_1, \lambda_2, \ldots, \lambda_n > 0$ ja otetaan käyttöön merkintä

Määr. $$\lambda_0+\cfrac{1}{\lambda_1+\cfrac{1}{\cdots+\cfrac{1}{\lambda_n}}} = \{\lambda_0; \lambda_1, \lambda_2, \ldots, \lambda_n\}.$$

Sivulla 77 lasketuissa esimerkeissä tavoin näemme suoraan, että Euklideen algoritmi antaa suoraan:

Lause 5.6. Jokainen rationaaliluku $\alpha \in \mathbb{R}$ voidaan kirjoittaa äärellisenä ketjumurtolukuna

$$\alpha = \{\lambda_0; \lambda_1, \ldots, \lambda_n\},$$

missä $\lambda_0 \in \mathbb{Z}$; $\lambda_1, \ldots, \lambda_n \in \mathbb{N}$.

Huom. Edellisen lauseen esitys on 1-häiritsevä, jos oletamme, että $\lambda_n > 1$ kun $n \geq 1$.

Määr. $\{\lambda_0; \lambda_1, \ldots, \lambda_n\}$ on yksinkertainen jos $\lambda_0 \in \mathbb{Z}$ ja $\lambda_i \in \mathbb{N}$ kun $i \geq 1$.

Huom. Käsittelemme ainoastaan yksinkertaisia ketjumurtolukuja.

Tästälähtien tarkastelemme vain ääretön-miä kehitelmiä, eli pyrimme esittämään annetun irrationaaliluvun $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ketjumurtolukuna.

Seuraava lemma antaa keinon selvittää suppenevan ketjumurtoluvun kehitelmän

Lemma 5.7. Oletetaan, että on olemassa raja-arvo $\alpha = \lim_{n\to\infty} \{\lambda_0; \lambda_1, \dots, \lambda_n\}$.

Silloin $\lambda_0 = \lfloor \alpha \rfloor$ ja jos määritellemme induktiivisesti

$$\alpha_0 = \alpha$$
$$\alpha_{k+1} = \frac{1}{\alpha_k - \lfloor \alpha_k \rfloor}, \quad k \geq 0,$$

niin pätee $\lambda_k = \lfloor \alpha_k \rfloor$, $k \geq 0$.

Tod. Aina pätee $\dfrac{1}{\lambda_1 + \dfrac{1}{\dots + \dfrac{1}{\lambda_n}}} \leq \dfrac{1}{\lambda_1} \leq 1$

ja siksi (sovella tätä nimittäjän osaan $\dfrac{1}{\lambda_2 + \dfrac{1}{\dots \dfrac{1}{\lambda_n}}}$)

$$(1) \quad \frac{1}{\lambda_1 + \dfrac{1}{\dots + \dfrac{1}{\lambda_n}}} \geq \frac{1}{\lambda_1 + 1} > 0.$$

Soveltamalla tätä nimittäjän osaan $\dfrac{1}{\lambda_2 + \dfrac{1}{\dots \dfrac{1}{\lambda_n}}}$ saamme

$$(2) \quad \frac{1}{\lambda_1 + \dfrac{1}{\dots + \dfrac{1}{\lambda_n}}} \leq \frac{1}{\lambda_1 + \dfrac{1}{\lambda_2 + 1}} = \frac{\lambda_2 + 1}{\lambda_1\lambda_2 + \lambda_1 + 1} < 1$$

kun $n \geq 2$. Ottamalla raja-arvo $n \to \infty$ epäyhtälöistä (1)-(2) saamme

$$0 < \lim_{n\to\infty} \frac{1}{\lambda_1 + \dfrac{1}{\dots + \dfrac{1}{\lambda_n}}} < 1$$

Tällöin on myös olemassa raja-arvo $\lim_{n\to\infty} \frac{1}{\lambda_m + \frac{1}{\lambda_{m+1} + \frac{1}{\ddots + \frac{1}{\lambda_n}}}}$ kaikilla $m \geq 1$ ja analogisesti näille pätee

$$(3) \qquad 0 < \lim_{n\to\infty} \frac{1}{\lambda_m + \frac{1}{\lambda_{m+1} + \frac{1}{\ddots + \frac{1}{\lambda_n}}}} < 1$$

Erityisesti arvolla $m=1$ saamme

$$\lambda_0 < \alpha = \lim_{n\to\infty} \lambda_0 + \frac{1}{\lambda_1 + \frac{1}{\ddots + \frac{1}{\lambda_n}}} < \lambda_0 + 1 .$$

Siis $\lambda_0 = \lfloor \alpha \rfloor$ ja

$$\alpha_1 = \frac{1}{\alpha_0 - \lfloor \alpha \rfloor} = \frac{1}{\alpha - \lambda_0} = \lambda_1 + \lim_{n\to\infty} \frac{1}{\lambda_2 + \frac{1}{\lambda_3 + \cdots + \frac{1}{\lambda_n}}} ,$$

josta vastaavasti (3):n nojalla päätellään

$$\lambda_1 = \lfloor \alpha_1 \rfloor$$

jolloin $\alpha_2 = \frac{1}{\alpha_1 - \lfloor \alpha_1 \rfloor} = \frac{1}{\alpha_1 - \lambda_1} = \lambda_2 + \lim_{n\to\infty} \frac{1}{\lambda_3 + \frac{1}{\lambda_4 + \cdots + \frac{1}{\lambda_n}}}$.

Näemme, että induktiolla saamme yleisen tuloksen

$$\alpha_{k+1} = \frac{1}{\alpha_k - \lfloor \alpha_k \rfloor} \quad , \quad \lambda_{k+1} = \lfloor \alpha_{k+1} \rfloor . \; \square$$

Huom. Edellisen nojalla $\alpha_k > 1$ kun $k \geq 1$ ja pätee

$$\alpha_k = \lambda_k + \lim_{n\to\infty} \frac{1}{\lambda_{k+1} + \frac{1}{\lambda_{k+2} + \cdots + \frac{1}{\lambda_n}}}$$

Lemman 5.7. tuloksesta seuraa, että suppenevan ketjumurtoluvun osanimittäjät λ_k $(k \geq 0)$ määräytyvät yksikäsitteisesti rajoin arvon α avulla. Tämä auttaa aikaan määritellä

Määr. Olkoon $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Silloin α:n jatkummurtokehitelmä

$$\{\lambda_0, \lambda_1, \lambda_2, \ldots\}$$

määritellään rekursion avulla asettamalla

$$\alpha_0 = \alpha, \quad \alpha_{k+1} = \frac{1}{\alpha_k - \lfloor \alpha_k \rfloor}, \; k \geq 0$$

$$\lambda_k := \lfloor \alpha_k \rfloor.$$

Huom. Emme vielä tiedä suppenevatko jatkumurtokehitelmät. Todistamme sen pian.

Esim. Jos $x = \sqrt{2}$, saamme $\alpha_0 = \sqrt{2}$,
$\lambda_0 = \lfloor \sqrt{2} \rfloor = 1$, $\alpha_1 = \frac{1}{\alpha_0 - \lfloor \alpha_0 \rfloor} = \frac{1}{\sqrt{2}-1} = 1+\sqrt{2}$,
$\lambda_1 = \lfloor 1+\sqrt{2} \rfloor = 2$, $\alpha_2 = \frac{1}{\alpha_1 - \lfloor \alpha_1 \rfloor} = \frac{1}{\sqrt{2}-1} = 1+\sqrt{2}$,

jatkaen induktiolla $\alpha_2 = \alpha_3 = \ldots \alpha_n = \ldots = 1+\sqrt{2}$, ja $\lambda_k = \lfloor \alpha_k \rfloor = 2$ kun $k \geq 2$. Siispä (tässä vaiheessa varta muodollisesti) pätee:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}$$

Ryhdymme nyt kehittämään yleistä teoriaa **konvergenteille** $\lambda_0, \lambda_0 + \frac{1}{\lambda_1}, \ldots, \lambda_0 + \cfrac{1}{\lambda_1 + \cfrac{1}{\ldots + \cfrac{1}{\lambda_n}}}, \ldots$

Oletamme annetuksi mielivaltaisen katkeamattoman jatkumurtokehitelmän $\{\lambda_0, \lambda_1, \lambda_2, \ldots\}$.

Lause 5.8. Olkoon $\lambda_i \in \mathbb{Z}$ $\forall i \geq 0$ ja $\lambda_i \geq 1$ kun $i \geq 1$. Määritellään kokonaislukujonot $(p_k)_{k \geq 0}$ ja $(q_k)_{k \geq 0}$ asettamalla

$p_0 = \lambda_0$, $q_0 = 1$
$p_1 = \lambda_1\lambda_0 + 1$, $q_1 = \lambda_1$ ja

(1) $\begin{cases} p_n = \lambda_n p_{n-1} + p_{n-2} \\ q_n = \lambda_n q_{n-1} + q_{n-2} \end{cases}$, $n \geq 2$.

Sillloin pätee:

(i) $\forall\, n \geq 0$: $\{\lambda_0; \lambda_1, \dots, \lambda_n\} = \frac{p_n}{q_n}$,

(ii) $q_n p_{n-1} - q_{n-1} p_n = (-1)^n$ kun $n \geq 1$,

(iii) Jos merkitään $p_{-1} = 1$ ja $q_{-1} = 0$, niin jokaisella $x \in \mathbb{R}$, $x > 0$ ja arvoilla $n \geq 0$ pätee

$$\{\lambda_0; \lambda_1, \dots, \lambda_n, x\} = \frac{x p_n + p_{n-1}}{x q_n + q_{n-1}}$$

Tod. (iii) Sovelletaan induktiota n:n suhteen:

$n = 0$: $\{\lambda_0; x\} = \lambda_0 + \frac{1}{x} = \frac{x\lambda_0 + 1}{x} = \frac{x p_0 + p_{-1}}{x q_0 + q_{-1}}$.

$n = 1$: $\{\lambda_0; \lambda_1, x\} = \lambda_0 + \frac{1}{\lambda_1 + \frac{1}{x}} = \lambda_0 + \frac{x}{\lambda_1 x + 1}$

$$= \frac{(\lambda_0\lambda_1 + 1)x + \lambda_0}{\lambda_1 x + 1} = \frac{p_1 x + p_0}{q_1 x + q_0}$$

Induktio: Oletetaan väite oikeaksi arvoilla $n \geq 1$.
Sillloin

$$\{\lambda_0; \lambda_1, \dots, \lambda_n, \lambda_{n+1}, x\}$$

$$= \{\lambda_0; \lambda_1, \dots, \lambda_n, \lambda_{n+1} + \tfrac{1}{x}\}$$

(induktio-oletus)

$$= \frac{p_n(\lambda_{n+1} + \frac{1}{x}) + p_{n-1}}{q_n(\lambda_{n+1} + \frac{1}{x}) + q_{n-1}} = \frac{(p_n\lambda_{n+1} + p_{n-1})x + p_n}{(q_n\lambda_{n+1} + q_{n-1})x + q_n}$$

$$= \frac{p_{n+1}x + p_n}{q_{n+1}x + q_n} ,$$

eli väite arvolla $n+1$.

(i) Nyt $\{\lambda_0; \lambda_1, \ldots, \lambda_n\} = \lim_{x\to\infty} \{\lambda_0; \lambda_1, \ldots, \lambda_n + \frac{1}{x}\}$

$= \lim_{x\to\infty} \{\lambda_0; \lambda_1, \ldots, \lambda_n, x\} \overset{(iii)}{=} \lim_{x\to\infty} \frac{p_n x + p_{n-1}}{q_n x + q_{n-1}}$

$= p_n/q_n$.

(ii) Helppo induktio, joka perustuu suoraan kertoimien p_n ja q_n palautuskaavaan (1) s. 82. Todistus HT. □

Huom. Yhtä hyvin voisimme määritellä jonot $(p_n)(q_n)$ palautuskaavoilla (1) kun $n \geq 1$ ja alkuarvoilla $p_{-1} = 1$, $q_{-1} = 0$.

[Seuraus 5.9 n. konvergenttien esitys $\frac{p_n}{q_n}$ on supistetussa muodossa, eli $(p_n, q_n) = 1$.

Tod. Suora seuraus lauseesta 5.8 (ii). □

Seuraava tulos varmistaa konvergenssin:

Lause 5.10 Olkoon $\frac{p_n}{q_n}$ (ääretöntä) ketjumurtoluvun n. konvergentti. Silloin

(i) jono q_n on kasvava, $q_{n+1} > q_n$ kun $n \geq 1$. Lisäksi $q_n \geq 2^{n/2-1}$.

(ii) $\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$

(iii) $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \ldots < \frac{p_{2n}}{q_{2n}} < \frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2n-1}}{q_{2n-1}} < \ldots < \frac{p_1}{q_1}$.

(iv) $\exists \lim_{n\to\infty} \frac{p_n}{q_n} = \alpha \in \mathbb{R}$ ja $|\alpha - \frac{p_n}{q_n}| \leq 2^{2-n}$

Tod. (i) Selvästi (q_n) on kasvava kaavan (1) s. 82 nojalla. Lisäksi jos $n \geq 1$, niin

$$q_{n+1} = \lambda_n q_n + q_{n-1} > q_n .$$

Selvästi $q_n \geq 2^{n/2-1}$ tosi kun $n=0$ tai $n=1$.
Oletetaan todeksi arvoilla $q_0, \dots, q_n$ $(n \geq 1)$. Silloin

$$q_{n+1} = \lambda_{n+1} q_n + q_{n-1} \geq q_n + q_{n-1} \geq 2^{n/2-1} + 2^{n/2-3/2}$$
$$= \underbrace{(\sqrt{2}+1)}_{\geq 2} 2^{\frac{n-1}{2}-1} \geq 2^{\frac{n+1}{2}-1}.$$

(ii) Suora seuraus lauseesta 5.8 (ii).

(iii)+(iv) Sovelletaan analyysin kurssin tuloksia alternoivista sarjoista:

Leibnizin lause: Olkoon $u_1 \geq u_2 > \dots > u_n \to 0$ $(n \to \infty)$.
Merkitään $s_n = u_1 - u_2 + u_3 - \dots + (-1)^{n-1} u_n$, $n \geq 1$.

Silloin $0 < s_2 < s_4 < \dots < s_{2n} < s_{2n+1} < s_{2n-1} < \dots < s_1$.
Lisäksi, hyperinen sarja suppenee, eli on olemassa raja-arvo $B = \lim_{n\to\infty} s_n$ ja $|B - s_n| \leq u_{n+1}$ $\forall n \geq 1$.

Tod. Ks. analyysin kurssi (tai MT). □

Sovelletaan tätä lausetta valitsemalla

$$u_n = \frac{1}{q_n q_{n-1}} = \left| \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} \right|, \quad n \geq 1.$$

Silloin $q_{n+1} q_n > q_n q_{n-1} \geq 2^{\frac{n}{2}-1} 2^{\frac{n-1}{2}-1} \to \infty$ $(n \to \infty)$ (i)-kohdan nojalla, eli (u_n) on aidosti väheneväjä ja $\lim_{n\to\infty} u_n = 0$, joten Leibnizin lausetta sovelletaan. Väite seuraa kun huomaamme, että

$$s_n = \frac{1}{q_1 q_0} - \frac{1}{q_2 q_1} + \dots + (-1)^{n-1} \frac{1}{q_n q_{n-1}}$$
$$= \left(\frac{p_1}{q_n} - \frac{p_0}{q_0}\right) - \left(-\left(\frac{p_2}{q_2} - \frac{p_1}{q_1}\right)\right) + \dots + (-1)^{n-1}(-1)^{n-1}\left(\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right)$$
$$= \frac{p_1}{q_n} - \frac{p_0}{q_0} + \left(\frac{p_2}{q_2} - \frac{p_1}{q_1}\right) + \dots + \left(\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right)$$
$$= \frac{p_n}{q_n} - \frac{p_0}{q_0};$$

Siis $\exists\ \beta = \lim_{n\to\infty}\left(\frac{p_n}{q_n} - \frac{p_0}{q_0}\right)$. Jos merkitsemme

$\alpha = \beta + \frac{p_0}{q_0}$ saamme $\lim_{n\to\infty}\frac{p_n}{q_n} = \alpha$ ja Lisäksi

Leibnizin lauseen nojalla

$$\left|\frac{p_n}{q_n} - \alpha\right| = |s_n - \beta| \le u_{n+1} = \frac{1}{q_{n+1}q_n}$$
$$\le 2^{1-n/2}\,2^{1-\frac{n-1}{2}} = 2^{3/2-n} \le 2^{2-n}. \quad \square$$

Varmistetaan vielä, että luvun $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ ketjumurtokehitelmän rajaarvo on α.

Lause 5.11 Olkoon $\{\lambda_0; \lambda_1, \lambda_2, \ldots\}$ luvun $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ ketjumurtokehitelmä. Silloin

$$\alpha = \lim_{n\to\infty}\{\lambda_0; \lambda_1, \ldots, \lambda_n\}.$$

Lisäksi jokaisella $n \ge 0$ pätee

$$(2) \qquad \alpha = \frac{p_n\alpha_{n+1} + p_{n-1}}{q_n\alpha_{n+1} + q_{n-1}} = \{\lambda_0; \lambda_1, \ldots, \lambda_n, \alpha_{n+1}\},$$

missä luvut ovat kuten s. 81 määritelmässä, eli $\alpha_0 = \alpha$, $\alpha_{n+1} = \frac{1}{\alpha_n - \lfloor\alpha_n\rfloor}$ (jolloin $\lambda_n = \lfloor\alpha_n\rfloor$).

Tod. Todistetaan ensin induktiolla kaava

$$\alpha = \{\lambda_0; \lambda_1, \ldots, \lambda_n, \alpha_{n+1}\}, \quad n \ge 0,$$

mistä (2) seuraa lauseen 5.8(iii) nojalla.
Kun $n = 0$, väite saapo $\alpha = \{\lambda_0; \alpha_1\}$, eli $\alpha = \lambda_0 + \frac{1}{\alpha_1}$, mikä on juuri α_1:n määritelmä. Oletetaan väite todeksi arvolla $n-1$ $(n \ge 1)$. Määritelmän mukaan $\alpha_n = \lambda_n + \frac{1}{\alpha_{n+1}}$, jolloin

$$\alpha = \{\lambda_0; \lambda_1, \ldots, \lambda_{n-1}, \alpha_n\} \quad \text{(oletus)}$$
$$= \{\lambda_0; \lambda_1, \ldots, \lambda_{n-1}, \lambda_n + \frac{1}{\alpha_{n+1}}\}$$
$$= \{\lambda_0; \lambda_1, \ldots, \lambda_n, \alpha_{n+1}\}.$$

Induktio on valmis

Arvioidaan lopuksi virhettä:

$$\left|\alpha - \frac{p_n}{q_n}\right| = \left|\frac{p_n\alpha_{n+1}+p_{n-1}}{q_n\alpha_{n+1}+q_{n-1}} - \frac{p_n}{q_n}\right|$$

$$= \left|\frac{q_n p_{n-1} - q_{n-1}p_n}{q_n(q_n\alpha_{n+1}+q_{n-1})}\right| = \frac{1}{q_n(q_n\alpha_{n+1}+q_{n-1})}$$

$$\leq \frac{1}{q_n} \leq 2^{1-n/2} \xrightarrow[n\to\infty]{} 0 . \quad \square$$

[**Seuraus 5.12** Olkoon α päättymättömän kehjumurtoluvun rajaarvo. Silloin

$$\frac{1}{(q_{n+1}+q_n)q_n} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} \leq \frac{1}{q_n^2} \quad !$$

Tod. Ed. lauseen todistuksen 2. virh. piir. $\Rightarrow$

$$(3) \qquad \left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{(q_n\alpha_{n+1}+q_{n-1})q_n} .$$

Tässä $1 \leq \lambda_{n+1} = \lfloor \alpha_{n+1} \rfloor < \alpha_{n+1} < \lambda_{n+1}+1$,

joten $q_n\alpha_{n+1} + q_{n-1} > q_n\lambda_{n+1} + q_{n-1} = q_{n+1}$

ja $q_n\alpha_{n+1} + q_{n-1} < q_n(\lambda_{n+1}+1) + q_{n-1} < q_{n+1}+q_n .$

Sijoittamalla nämä arviot yhtälöön (3) seuraa väite. $\square$

[**Seuraus 5.13** Päättymättömän kehjumurtoluvun arvo on irrationaalinen.

Tod. Jos α olisi rationaalinen, ei seurauksen 5.12 epäyhtälössä $|\alpha - p_n/q_n| < q_n^{-2}$ voisi q_n olla mielivaltaisen suuri (HT). $\square$

Seuraus 5.14. (Yksinkertaisten) päättymättömien ketjumurtolukujen ja irrationaalilukujen $\mathbb{R} \setminus \mathbb{Q}$ välillä on 1-1-vastaavuus.

Tod. Yhdistä tekemämme havainnot! □

Huom. Seurauksen 5.13 ja sen todistuksen nojalla, vakioita vaille pätee

$$\left|\alpha - \frac{p_n}{q_n}\right| \sim \frac{1}{q_n q_{n+1}} \sim \frac{1}{\lambda_{n+1} q_n^2}.$$

Tässä mielessä virheen arviointi on helppoa kun kehitelmä on tiedossa!

$\Rightarrow$ Jos haluamme arvion $\left|\alpha - \frac{p_n}{q_n}\right|$ olevan erityisen tarkka (suhteessa nimittäjään q_n) kannattaa valita n niin että

(λ_{n+1} on poikkeuksellisen suuri)

Esim. $\pi = \{3; 7, 15, 1, 292, \ldots\}$.

Siispä π:n erittäin hyvä approksimaatio on

$$\pi \approx \{3; 7, 15, 1\} = 3 + \frac{1}{7 + \frac{1}{15+1}} = 3 + \frac{16}{113}$$

$$= \frac{355}{113}$$

('Ludolfin luku', virhe $\leq 3 \cdot 10^{-7}$, tunnettu Kiinassa 500-luvulla).

Ketjumurtoluvut parhaina approksimaatioina

Määr. Olkoon $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Rationaaliluku $\frac{p}{q}$ $(q \geq 1)$ on *paras approksimaatio* luvulle α jos

$$|bx - a| > |qx - p|$$

kaikilla $\frac{a}{b} \neq \frac{p}{q}$, missä $1 \leq b \leq q$.

Huom. • Jos $\frac{p}{q}$ on paras approksimaatio α:lle ja $1 \leq b \leq q$, niin silloin

$$|\alpha - \tfrac{p}{q}| = \tfrac{1}{q}|q\alpha - p| \leq \tfrac{1}{b}|q\alpha - p|$$
$$< \tfrac{1}{b}|b\alpha - a| = |\alpha - \tfrac{a}{b}| \quad \square$$

• parhaat approksimaatiot muodostavat jonon rationaalilukuja joissa nimittäjät kasvavat ja ensimmäinen nimittäjä on 1.

On merkittävää, että konvergentit ylipäätä (olennaisesti) parhaiden approksimaatioiden lauma:

Lause 5.15. Olkoot $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots$ luvun $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ketjumurtokehitelmän konvergentit. Näistä $\frac{p_n}{q_n}$ on luvun α paras approksimaatio kun $n \geq 1$. Lisäksi $\frac{p_0}{q_0}$ on paras approksimaatio tapauksessa $q_1 > 1$. Muita parhaita approksimaatioita luvulle α ei ole.

Huom. Siis luvun α parhaiden approksimaatioiden joukko on

- $\{\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots\}$ jos $q_1 = 1$
- $\{\frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots\}$ jos $q_1 > 1$.

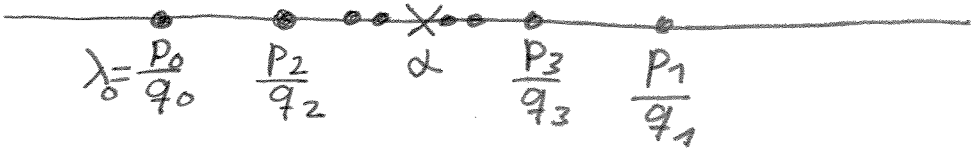
Tod. Olkoon alussa $\frac{p}{q}$ $(q \geq 1)$ luvun $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ paras approksimaatio, ja olkoot $\frac{p_k}{q_k}$, $k \geq 0$ luvun α kehitelmän konvergentit. Määritelmän mukaan pätee (1) $|q\alpha - p| < |b\alpha - a|$ jos $\begin{cases} 1 \leq b \leq q \\ \frac{a}{b} \neq \frac{p}{q} \end{cases}$ ja

Tehdään vastaoletus: $\frac{p}{q}$ ei ole konvergentti

(1°) Oletetaan ensin, että $\boxed{\frac{p}{q} < \frac{p_0}{q_0}}$. Silloin (vrt. lause)

$$|q\alpha - p| = q\left|\alpha - \frac{p}{q}\right| \geq \left|\alpha - \frac{p}{q}\right| \geq \left|\alpha - \frac{p_0}{q_0}\right| = \left|\alpha - \frac{\lambda_0}{1}\right|,$$

mikä on vastoin epäyhtälöä (1).



(2°) Olkoon sitten $\boxed{\frac{p}{q} > \frac{p_1}{q_1}}$ Tällä kertaa

$$|q\alpha - p| = q\left|\alpha - \frac{p}{q}\right| > q\left|\frac{p_1}{q_1} - \frac{p}{q}\right| \geq q\,\frac{1}{q_1 q} = \frac{1}{q_1}.$$

Seuraus 5.12 mukaan $\left|\alpha - \frac{p_0}{q_0}\right| < \frac{1}{q_1}$, ja koska tässä $q_0 = 1$, saadaan taas ristiriita (1):n kanssa.

[**Huom** (HT): Käytämme jatkuvasti helppoa havaintoa Jos $\frac{r}{s} \neq \frac{u}{v} \Rightarrow \left|\frac{r}{s} - \frac{u}{v}\right| \geq \frac{1}{sv}$]

(3°) Olkoon viimeksi $\boxed{\frac{p_0}{q_0} < \frac{p}{q} < \frac{p_1}{q_1}}$.

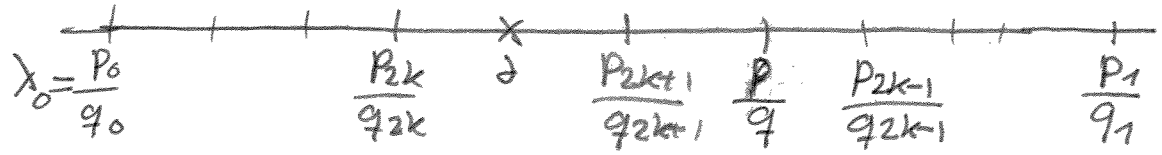
Silloin joko $\frac{p}{q} > \alpha$ tai $\frac{p}{q} < \alpha$. Tapausten käsittely on samanlainen, joten tarkastellaan vain tapausta $\frac{p}{q} > \alpha$. Silloin $\frac{p}{q}$ on kahden parittoman konvergentin välissä: oletetaan, että

$$\frac{p_{2k+1}}{q_{2k+1}} < \frac{p}{q} < \frac{p_{2k-1}}{q_{2k-1}}, \quad k \geq 1.$$

Nyt tulee olla $\boxed{q > q_{2k}}$, koska

$$\frac{1}{q_{2k+1}q_{2k}} = \left|\frac{p_{2k}}{q_{2k}} - \frac{p_{2k+1}}{q_{2k+1}}\right| > \left|\frac{p}{q} - \frac{p_{2k+1}}{q_{2k+1}}\right| \geq \frac{1}{q\,q_{2k+1}}.$$

L.5.10(ii) ↑ , kts. kuva alla ↑



Toisaalta, (kts kuva)

$$|q\alpha - p| = q\left|\alpha - \frac{p}{q}\right| > q\left|\frac{p_{2k+1}}{q_{2k+1}} - \frac{p}{q}\right| \geq q\,\frac{1}{q_{2k+1}q} = \frac{1}{q_{2k+1}}$$

Lisäksi seurauksen 5.12 nojalla

$$|q_{2k}\alpha - p_{2k}| = q_{2k}\left|\alpha - \frac{p_{2k}}{q_{2k}}\right| < \frac{q_{2k}}{q_{2k}q_{2k+1}} = \frac{1}{q_{2k+1}}.$$

Koska $q_{2k} < q$, osat juuri johdetut epäyhtälöt mistiriidassa (1) kanssa. Olemme osoittaneet, että parhaat approksimaatiot ovat konvergentteja.

Toinen suunta: osoitamme, että konvergentit $\frac{p_k}{q_k}$ $(k \geq 1)$ ovat parhaita approksimaatioita. Vastaoletus: $n \geq 1$ ja $\frac{p_n}{q_n}$ ei ole paras approksimaatio. Silloin on olemassa $q \in \{1, \ldots, q_n\}$ ja p joille (2) $|q\alpha - p| \leq |q_n\alpha - p_n|$, $\frac{p}{q} \neq \frac{p_n}{q_n}$.

Erityisesti, voimme olettaa, että $\frac{p}{q}$ on itseasiassa paras approksimaatio — minimoidaan tässä vaan puoli ehdolla $1 \leq q \leq q_n$. Edellisen osan nojalla $\frac{p}{q}$ on konvergentti, joten $\frac{p}{q} = \frac{p_k}{q_k}$, missä $k < n$. Jälleen seurauksen 5.12 nojalla ensiksi

$$|q_k\alpha - p_k| = q_k\left|\alpha - \frac{p_k}{q_k}\right| > \frac{q_k}{q_k(q_k + q_{k+1})}$$

$$= \frac{1}{q_{k+1} + q_k} \geq \frac{1}{q_{k+2}} \geq \frac{1}{q_{n+1}}$$

ja sitten $|q_n\alpha - p_n| = q_n|\alpha - \frac{p_n}{q_n}| < \frac{q_n}{q_n q_{n+1}} = \frac{1}{q_{n+1}}$.

Johdetut epäyhtälöt ovat siinä muodossa (2):n kanssa. Siis p_k/q_k on konvergentti.

Edellisenä päättelyssä käytimme hyväksi sitä, että jos $n \geq 1$ ja $\frac{p_k}{q_k} \neq \frac{p_n}{q_n}$, $q_k \leq q_n$ $\Rightarrow k < n$. Tämä ei ole voimassa arvolla $n = 0$, koska voi olla $q_1 = q_0 = 1$. Itsestäänsä, suoraan määritelmän nojalla $\frac{p_0}{q_0} = \frac{\lambda_0}{1}$ on paras approksimaatio vain jos $|\alpha - \lambda_0| < \frac{1}{2} \Leftrightarrow \alpha_1 > 2 \Leftrightarrow q_1 \geq 2$. □

[Lause 5.16. Jos $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ja $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$, niin $\frac{p}{q}$ on α:n konvergentti

Tod. Tarkastellaan tapausta $0 < \alpha - \frac{p}{q} < \frac{1}{2q^2}$ (tapaus $0 < \frac{p}{q} - \alpha < 1/2q^2$ on analoginen). Edellisen lauseen nojalla riittää osoittaa, että $\frac{p}{q}$ on paras approksimaatio α:lle.

Vastaoletus: oletetaan, että on olemassa $\frac{r}{s} \neq \frac{p}{q}$ jolle $1 \leq s \leq q$ ja $|s\alpha - r| \leq |q\alpha - p|$

(1₀) Tapaus $\frac{r}{s} < \frac{p}{q} < \alpha$. Silloin

$$0 < \frac{1}{qs} \leq \frac{p}{q} - \frac{r}{s} < \alpha - \frac{r}{s} = \frac{1}{s}|s\alpha - r|$$
$$\leq \frac{1}{s}|q\alpha - p| = \frac{q}{s}|\alpha - \frac{p}{q}| \leq \frac{q}{s}\frac{1}{2q^2} = \frac{1}{2qs}$$ ↑↓

(2₀) Tapaus $\frac{p}{q} < \frac{r}{s} < \alpha$ Vastaavanti

$$0 < \frac{1}{qs} \leq \frac{r}{s} - \frac{p}{q} < \alpha - \frac{p}{q} < \frac{1}{2q^2} \leq \frac{1}{2qs}$$ ↑↓

3. Tapaus $\frac{p}{q} < \alpha < \frac{r}{s}$. Silloin

$$0 < \frac{r}{s} - \alpha = \frac{r - s\alpha}{s} < \frac{q\alpha - p}{s} = \left(\alpha - \frac{p}{q}\right)\frac{q}{s}. \quad \text{Siis}$$

$$0 < \frac{1}{sq} \leq \frac{r}{s} - \frac{p}{q} = \left(\frac{r}{s} - \alpha\right) + \left(\alpha - \frac{p}{q}\right) < \left(\frac{q}{s} + 1\right)\left(\alpha - \frac{p}{q}\right)$$

$$< \left(\frac{q}{s} + 1\right)\frac{1}{2q^2} = \frac{q+s}{s\,2q^2} \leq \frac{1}{sq} \quad \text{↯} \quad . \square$$

Sovellus Pellin yhtälöön

Lause 5.17. Olkoon $D \geq 2$ ja $\sqrt{D} \notin \mathbb{Q}$. Jokainen positiivinen ratkaisu Pellin yhtälölle vastaa jotakin luvun $\sqrt{D}$ konvergenttia, eli $(x, y) = (p_n, q_n)$ jollakin $n \geq 1$.

Tod. Olkoon $x, y \geq 1$ ja $x^2 - Dy^2 = 1$. Silloin $\frac{x}{y} = \sqrt{D + 1/y^2} > \sqrt{D}$. Saamme

$$\left|\frac{x}{y} - \sqrt{D}\right| = \frac{1}{\left|\frac{x}{y} + \sqrt{D}\right| y^2} \leq \frac{1}{2\sqrt{D}\,y^2} < \frac{1}{2y^2}.$$

Väite seuraa välittömästi lauseesta 5.16. $\square$

Huom. Juuri todistettu lause antaa korrektiksen ja tehokkaan algoritmin perusratkaisun (x_1, y_1) (ort. Lause 5.4) löytämiseksi: lasketaan $\sqrt{D}$:n ketjumurtokehitelmän λ_k:t, lasketaan (p_k, q_k):t vaikkapa rekursiokaavojen (1) s. 82 avulla ja kokeillaan mikä on ensimmäinen pari (p_k, q_k), joka toteuttaa $p_k^2 - Dq_k^2 = 1$.

Esim. $x^2 - 21y^2 = 1$:

$$\sqrt{21} = (4) + \boxed{\sqrt{21}-4}$$

$$\frac{1}{\sqrt{21}-4} = \frac{4+\sqrt{21}}{5} = (1) + \frac{\sqrt{21}-1}{5}$$

$$\frac{5}{\sqrt{21}-1} = \frac{\sqrt{21}+1}{4} = (1) + \frac{\sqrt{21}-3}{4}$$

$$\frac{4}{\sqrt{21}-3} = \frac{\sqrt{21}+3}{3} = (2) + \frac{\sqrt{21}-3}{3}$$

$$\frac{3}{\sqrt{21}-3} = \frac{3+\sqrt{21}}{4} = (1) + \frac{\sqrt{21}-1}{4}$$

$$\frac{4}{\sqrt{21}-1} = \frac{\sqrt{21}+1}{5} = (1) + \frac{\sqrt{21}-4}{5}$$ ⇒ jaksollisuus.

$$\frac{5}{\sqrt{21}-4} = \sqrt{21}+4 = (8) + \boxed{\sqrt{21}-4}$$

$$\frac{1}{\sqrt{21}-4} = \frac{4+\sqrt{21}}{5} = (1) + \frac{\sqrt{21}-1}{5}$$

Siispä kehitelmä on jaksollinen ja

$$\sqrt{21} = \{4; \overbrace{1,1,2,1,1,8}^{\text{jakso}}, \overline{1,1,2,1,1,8}, \dots\}$$

Lasketaan peräkkäisiä konvergentteja palautuskaavoilla

$$\begin{cases} p_0 = \lambda_0, \; p_1 = \lambda_1\lambda_0 + 1 \\ q_0 = 1, \; q_1 = \lambda_1 \end{cases}$$

$$\begin{cases} p_{n+1} = \lambda_{n+1}p_n + p_{n-1} \\ q_{n+1} = \lambda_{n+1}q_n + q_{n-1} \end{cases},$$

missä $\lambda_0 = 4, \; \lambda_1 = \lambda_2 = 1, \; \lambda_3 = 2, \; \lambda_4 = \lambda_5 = 1, \; \lambda_6 = 8, \dots$

Saamme taulukon:

k	(p_k, q_k)	$p_k^2 - 21 q_k^2$
0	$(4,1)$	-5
1	$(5,1)$	4
2	$(9,2)$	-3
3	$(23,5)$	4
4	$(32,7)$	-5
5	$(55,12)$	(1)
⋮		

Siispä perusratkaisu on $(x_1, y_1) = (55, 12)$.

□

Jaksolliset ketjumurtoluvut

Tiedämme, että jokainen rationaaliluku voidaan kirjoittaa päättymättömänä jaksollisena desimaalikehitelmänä, esim.

$$\frac{1}{2} = 0{,}49999\ldots \quad , \quad \frac{1}{3} = 0{,}3333\ldots$$

ja käänteisen, jokainen jaksollinen desimaalikehitelmä edustaa rationaaliolukua. Tämän vastine ketjumurtoluvuille on seuraava yksinkertainen tulos:

Lause 5.18. (Lagrange) Olkoon α irrationaaliluku. Silloin sen ketjumurtokehitelmä

$$\alpha = [\lambda_0; \lambda_1, \lambda_2, \ldots]$$

on *jaksollinen* (eli $\lambda_{n+l_0} = \lambda_n$ kun $n \geq n_0$) jos ja vain jos α on 2. asteen algebrallinen luku (eli $\alpha \notin \mathbb{Q}$, $A\alpha^2 + B\alpha + C = 0$, $A \neq 0$, $A, B, C \in \mathbb{Z}$).

Tod. Oletetaan ensin $\{\lambda_0, \lambda_1, \lambda_2, \dots\}$ jaksolliseksi, eli olkoon $\lambda_{n+l_0} = \lambda_n$ kun $n \geq n_0$. Määritellään luvut α_k kuten määritelmässä s. 81, jolloin

$$\alpha_n = \{\lambda_n, \lambda_{n+1}, \dots\}$$

Erityisesti nyt $\boxed{\alpha_{n_0+l_0} = \alpha_{n_0}}$. Voimme olettaa, että $n_0 \geq 2$. Lauseen 5.11 kaavan (2) nojalla

$$\alpha = \frac{p_{n_0-1}\alpha_{n_0} + p_{n_0-2}}{q_{n_0-1}\alpha_{n_0} + q_{n_0-2}} = \frac{p_{n_0+l_0-1}\alpha_{n_0+l_0} + p_{n_0+l_0-2}}{q_{n_0+l_0-1}\alpha_{n_0+l_0} + p_{n_0+l_0-2}}$$

$$= \frac{p_{n_0+l_0-1}\alpha_{n_0} + p_{n_0+l_0-2}}{q_{n_0+l_0-1}\alpha_{n_0} + q_{n_0+l_0-2}} .$$

Saamme tästä α_{n_0}:lle yhtälön

$$(p_{n_0+l_0-1}\alpha_{n_0} + p_{n_0+l_0-2})(q_{n_0-1}\alpha_{n_0} + q_{n_0-2})$$
$$= (p_{n_0-1}\alpha_{n_0} + q_{n_0-2})(q_{n_0+l_0-1}\alpha_{n_0} + q_{n_0+l_0-2}) .$$

Siis α_{n_0} toteuttaa 2. asteen kokonaisdekertoimisen yhtälön, joka on epätriviaali, sillä 2. asteen termin on

$$p_{n_0+l_0-1}q_{n_0-1} - p_{n_0-1}q_{n_0+l_0-1}$$
$$= q_{n_0-1}q_{n_0+l_0-1}\left(\frac{p_{n_0+l_0-1}}{q_{n_0+l_0-1}} - \frac{p_{n_0-1}}{q_{n_0+l_0-1}}\right) \neq 0 .$$

Toisaalta (Seuraus 5.13) $\alpha_{n_0} \notin \mathbb{Q}$, joten α_{n_0} on 2. asteen algebrallisen luku. Lisäksi

$$\alpha = \frac{p_{n_0-1}\alpha_{n_0} + p_{n_0-2}}{q_{n_0-1}\alpha_{n_0} + q_{n_0-2}} \Rightarrow \alpha_{n_0} = \frac{p_{n_0-2} - q_{n_0-2}\alpha}{q_{n_0-1}\alpha - p_{n_0-1}}$$

Sijoittamalla tämä α_{n_0}:n toteuttamaan yhtälöön näemme, että myös α toteuttaa 2 asteen kokonaiskertoimisen yhtälön: jos $A\alpha_{n_0}^2 + B\alpha_{n_0} + C = 0$, niin helppo lasku antaa $A'\alpha^2 + B'\alpha + C' = 0$, missä $A' = q_{n_0-2}^2 A - Bq_{n_0-2}q_{n_0-1} + Cq_{n_0-1}^2$

$$= q_{n_0-1}^2\left(A\left(\frac{-q_{n_0-2}}{q_{n_0-1}}\right)^2 + B\left(\frac{-q_{n_0-2}}{q_{n_0-1}}\right) + C\right) \neq 0 ,$$

sillä $\alpha_n \neq \mathbb{Q}$. Siis myös α on 2. asteen algebrallinen luku.

Käänteinen suunta on syvällisempi. Oletetaan siitä varten, että $\alpha \notin \mathbb{Q}$ ja

$$A\alpha^2 + B\alpha + C = 0,$$

missä $A \neq 0$ ja $A, B, C \in \mathbb{Z}$. Olkoon $k \geq 2$ ja sijoitetaan edelliseen $\alpha = \dfrac{p_{k-1}\alpha_k + p_{k-2}}{q_{k-1}\alpha_k + q_{k-2}}$. Saadaan

$$A(p_{k-1}\alpha_k + p_{k-2})^2 + B(p_{k-1}\alpha_k + p_{k-2})(q_{k-1}\alpha_k + q_{k-2}) + C(q_{k-1}\alpha_k + q_{k-2})^2 = 0$$

Toisin sanoen,

$$(1) \qquad \boxed{A_k\alpha_k^2 + B_k\alpha_k + C_k = 0,}$$

missä

$$(2) \quad \begin{cases} A_k = A p_{k-1}^2 + B p_{k-1}q_{k-1} + C q_{k-1}^2 \\ C_k = A p_{k-2}^2 + B p_{k-2}q_{k-2} + C q_{k-2}^2 \\ B_k = 2A p_{k-1}p_{k-2} + B(p_{k-1}q_{k-2} + p_{k-2}q_{k-1}) + 2C q_{k-1}q_{k-2} \end{cases}$$

Seuraavaksi arvioimme kertoimien A_k, B_k ja C_k kokoa. Osoitamme, että on olemassa vakio $c_0 < \infty$ jolle

$$(3) \qquad |A_k|, |B_k|, |C_k| \leq c_0 \quad \forall k \geq 1,$$

eli että kyseiset kerroinjonot ovat rajoitettuja. Kirjoitetaan tätä varten

$$f(x) = Ax^2 + Bx + C.$$

Silloin $f(\alpha) = 0$. Merkitsemällä $M = \max_{x \in [\alpha-1, \alpha+1]} |f'(x)|$

(4)

Ja havaitsemalla väliarvolauseen nojalla $\boxed{A_k = q_{k-1}^2 f\left(\frac{p_{k-1}}{q_{k-1}}\right)}$ saamme

$$|A_k| \le q_{k-1}^2 \left|f\left(\frac{p_{k-1}}{q_{k-1}}\right)\right| = q_{k-1}^2 \left| f\left(\frac{p_{k-1}}{q_{k-1}}\right) - f(\alpha)\right|$$

$$\le q_{k-1}^2 \left|\frac{p_{k-1}}{q_{k-1}} - \alpha\right| |f'(\xi)| \qquad \left| \begin{array}{l} \xi \text{ d:n} \\ \text{ja } p_k/q_k\text{:n} \\ \text{välissä} \end{array}\right.$$

$$\le q_{k-1}^2 \frac{1}{q_{k-1}^2} M = M,$$

sillä Seurauksen 5.12 mukaan $\left|\frac{p_{k-1}}{q_{k-1}} - \alpha\right| \le \frac{1}{q_{k-1}^2}$.

Lisäksi, koska $C_k = A_{k-1}$, niin $|C_k| \le M$, $k \ge 2$. Olemme osoittaneet jonot (A_k) ja (C_k) rajoitetuiksi.

Jonon (B_k) rajoittuneisuus seuraa tämän jälkeen suoraan kaavasta

$$B_k^2 - 4A_kC_k = B^2 - 4AC,$$

mikä seuraa suoralla laskulla (HT) kaavoista (2) sekä relaatiosta

$$p_{k-1}q_{k-2} - p_{k-2}q_{k-1} = (-1)^k.$$

Olemme todistaneet arvion (3).

Lauseen todistus voidaan nyt päättää seuraavasti: tiedon (3) nojalla on vain äärellisen monta erilaista kolmikkoa (A_k, B_k, C_k). [k)] Erityisesti voimme valita kolme indeksiä $n_1 < n_2 < n_3$ joille pätee

$$(A_{n_1}, B_{n_1}, C_{n_1}) = (A_{n_2}, B_{n_2}, C_{n_2}) = (A_{n_3}, B_{n_3}, C_{n_3}).$$

---

k) Huomaa, että $A_k \neq 0$ (4):n nojalla

Koska 2. asteen yhtälöllä (*) on vain 2 juurta, kahden luvuista a_{n_1}, a_{n_2} ja a_{n_3} tulee olla yhtäsuuria. Joka tapauksessa jollakin n_0 ja $l_0 \geq 1$ pätee $a_{n_0} = a_{n_0+l_0}$, jolloin ketjumurtokehitelmä on jaksollinen. □

Huom. Eräille tunnetuille transsendenttiluvuille tunnetaan ketjumurtokehitelmä, esim.

$$e = \{2; 1, 2, 1, 1, 4, 1, 1, 6, \ldots, 1, 1, 2n, 1, 1, 2n+2, \ldots\}$$

Lisäksi esimerkiksi luku π voidaan esittää yleistettynä ketjumurtolukuna

$$\frac{4}{\pi} = 1 + \cfrac{1}{2 + \cfrac{9}{2 + \cfrac{25}{2 + \cfrac{49}{2 + \ddots}}}}$$

(osoittajien jono $1^2, 3^2, 5^2, \ldots$, nimittäjänä aina 2).

6. DIOFANTEEN YHTÄLÖT. GAUSSIN KOKONAISLUVUT

Diofanteen yhtälöt saivat nimensä Diophanteen teoksesta 'Arithmetica' (200-luku: 13 kirjaa, 6 säilynyt), jossa hän etsi kokonais- tai (lähinnä) rationaaliratkaisuja erilaisille yhtälöille tai yhtälöryhmille. Fermat'n kirjeenvaihto aikanaan kohotti Diofanteen yhtälöiden teorian uudelle tasolle.

Euklideen 'Elementa' piti jo sisällään epätrivaalin Diofanteen yhtälön ratkaisun: 'pythagoraan lukujen' (kts Lause 6.1 alla) määräämisen. Ennen kuin tutustumme tähän, on syytä huomata, että osa aiemmasta työstämme voidaan tulkita seuraavien Diofantoksen yhtälöiden ratkaisuna:

- $ax+by=c$ (seuraus 1.6, ktn. myös kiinalainen jäännöslause)
- $ax^2+bx+c=my$ (Lause 4.12 jos $m \in \mathbb{P}$)
- $x^2-Dy^2=1$ (Pellin yhtälö, luku 5.)

Tämän luvun päätavoite on selvittää Gaussin alkulukujen avulla, milloin yhtälöllä

$$x^2+y^2=m$$

on ratkaisu.

Pythagoraan lukukolmikot

ovat kolmikkoja (x,y,z) $(x,y,z \in \mathbb{N})$ joille

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

Toisin sanoen, kokonaisluvut x, y ja z ovat erään suorakulmaisen kolmion sivujen pituudet.

Lause 6.1 Kaikki Pythagoraan lukukolmikot saadaan kaavasta

$$(x,y,z) = t(a^2-b^2, 2ab, a^2+b^2)$$

(tai $(x,y,z) = t(2ab, a^2-b^2, a^2+b^2)$),

missä $t \geq 1$, $a > b \geq 1$

Tod. Suora lasku näyttää, että kaava tuottaa Pyth. lukuja. Käänteen, olkoon (x,y,z) Pyth. lukukolmikko. Voimme olettaa, että $(x,y,z)=1$, koska yhteisen tekijä voidaan jakaa pois. Silloin (miksi?) pätee

$$(x,y) = (y,z) = (z,x) = 1.$$

Jos sekä x ja y ovat parittomia, niin

$$z^2 \equiv 1+1 \equiv 2 \pmod 4,$$

mikä on mahdotonta. Siispä toisen on oltava parillinen, olkoon vaikka $2 \mid y$. Nyt

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

Koska myös z on pariton, pätee $z-x = 2u$, $z+x = 2v$, eli $x = v-u$, $z = v+u$. Tässä $(v,u)=1$, koska muuten $(x,z) \neq 1$. Siis

$$(y/2)^2 = uv.$$

Koska uv on neliö ja $(u,v)=1$, niin sekä u ja v ovat neliöitä (HT). Merkitään

$$v=a^2,\ u=b^2,$$

jolloin $z=a^2+b^2$, $x=a^2-b^2$ ja $y=2ab$ $(a>b)$. □

Huom. Jos haluamme johdetun kaavan esityksen olevan 1-käsitteinen, on vaadittava $(a,b)=1$, $a>b\geq 1$, jksi luvuista a,b parittoman.

Esim. Valinnat $t=1$ ja $(a,b)=(2,1)$ tai $(a,b)=(3,2)$ tuottavat tutummat $3^2+4^2=5^2$ ja $5^2+12^2=13^2$.

Seuraava esimerkki on peräisin Diofantoksen 'Arithmetica'sta:

Esim. Olkoon $p\in\mathbb{Q}$, $p\neq 0$. Määrää kaikki rationaaliluvut x,y joille

$$(*)\quad \frac{x^2+y^2}{x+y}=p.$$

Ratk. (Diofantes) Asetetaan $\frac{y}{x}=t\in\mathbb{Q}$ (kun $x=0$)

$$\Rightarrow \frac{x^2(1+t^2)}{x(1+t)}=p, \text{ eli } \begin{cases} x=\dfrac{p(1+t)}{1+t^2} \\ y=\dfrac{p(t+t^2)}{1+t^2} \end{cases}$$

Suora tarkistus osoittaa, että kaikilla $t\in\mathbb{Q}$ saatu ratkaisupari toteuttaa yhtälön $(*)$. Jos $x=0$ saamme ratkaisun $(x,y)=(0,p)$. □

Paljon vaikeampaa on päätellä milloin yhtälöllä $x^2+y^2=m$ on ratkaisu ($m \in \mathbb{N}$ annettu). Tutkimme tätä yhtälöä ottamalla käyttöön sopivan algebrallisen lukukunnan (tai renkaan). Tälle yhtälölle oikea valinta on yhtälöt $x^2=-1$ juurten (eli imaginaariyksikköjen) liittäminen kuntaan $\mathbb{Q}$. Näin saadaan kunta $\mathbb{Q}[i]$. Sen kokonaisalkioita rengasta kutsutaan nimellä

Gaussin kokonaisluvut

Osa tämän jakson todistuksista tullaan esittämään varsin tiivistetysti, lukijan on tarvittaessa täydennettävä itse yksityiskohtia. Oletamme, että kunnan $\mathbb{C}$ perusominaisuudet ovat tuttuja, jos on tarpeen, niistä on syytä herrata nyt. Yleisesti merkitsemme, jos $z = x+iy \in \mathbb{C}$ $(x,y \in \mathbb{R},\ i=\sqrt{-1})$, niin

$\bar{z} = x-iy$ (liittoluku)

$|z| = \sqrt{x^2+y^2} = \sqrt{z\bar{z}}$

Nyt pätee $\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{x-iy}{x^2+y^2}$ jne.

Määr. Kompleksiluku $a+bi \in \mathbb{C}$ on Gaussin rationaaliluku jos $a,b \in \mathbb{Q}$.
Kaikkien Gaussin rationaalilukujen joukkoa merkitsemme $\mathbb{Q}[i]$:llä.

Huom. Selvästi $\mathbb{Q}[i]$ on $\mathbb{C}$:n alikunta:

$0,1 \in \mathbb{Q}[i]$. Lisäksi, jos $z_1, z_2 \in \mathbb{Q}$
$\Rightarrow z_1+z_2, z_1z_2 \in \mathbb{Q}[i]$. Edelleen $-z_1 \in \mathbb{Q}[i]$
ja $1/z_1 \in \mathbb{Q}[i]$ jos $z_1 \neq 0$.

Määr. Gaussin kokonaislukujen rengas on
$\mathbb{Z}[i] := \{a+bi : a,b \in \mathbb{Z}\}$

Selvästi $\mathbb{Z}[i]$ on $\mathbb{Q}$:n alirengas. Palautetaan mieleen, että renkaan alkio $u \neq 0$ on yksikkö jos u^{-1} on myös renkaassa.

Lause 6.2 $\lambda \in \mathbb{Z}[i]$ on yksikkö täsmälleen kun $\lambda \in \{\pm 1, \pm i\}$.

Tod. Olkoon $\lambda = a+bi \neq 0$ $(a,b \in \mathbb{Z})$. Silloin

$$\frac{1}{\lambda} = \frac{1}{a+bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} \in \mathbb{Z}[i]$$

vain jos $\frac{a}{a^2+b^2} \in \mathbb{Z}$ ja $\frac{b}{a^2+b^2} \in \mathbb{Z}$.

$\Rightarrow a=0$ tai $|a| \geq |a|^2+|b|^2$, jolloin $b=0$.
Tapauksessa $a=0$ on $b=\pm 1$, ja jos $b=0$ niin $a=\pm 1$. □

Määr. Jos $a+ib \in \mathbb{Z}[i]$ (tai $a+ib \in \mathbb{Q}(i)$), määritellään $N(a+ib) = a^2+b^2$ (luvun $a+ib$ **normi**)

Huom. $N(\lambda) = \lambda\overline{\lambda} = |\lambda|^2$ (Euklidisen normin neliö)

Lause 6.3 (i) $N(\lambda) = \lambda\overline{\lambda}$
(ii) $N(\lambda_1\lambda_2) = N(\lambda_1)N(\lambda_2)$
(iii) $N(\lambda) = 0 \Leftrightarrow \lambda = 0$
(iv) Jos $\lambda \in \mathbb{Z}[i]$, niin $N(\lambda) = 1 \Leftrightarrow \lambda$ on yksikkö

Tod. HT □

Seuraava määritelmä on aivan sama kuin $\mathbb{Z}$:ssa.

Määr. Olk. $\lambda, \mu \in \mathbb{Z}[i]$. Luku λ jakaa luvun μ (eli λ on μ:n tekijä) jos $\mu = k\lambda$, missä $k \in \mathbb{Z}[i]$. Merkitään $\lambda | \mu$.

Lauseen 1.1 (s. 3) vastine todistetaan kuten aiemmin.

Määr. Luvun $\lambda \in \mathbb{Z}[i]$ liitännäisluvut ovat $\pm\lambda$ ja $\pm i\lambda$

(toisin sanoen: λ ja μ ovat liitännäisiä $\Leftrightarrow$ λ/μ on yksikkö).

Määr. Gaussin kokonaisluku $\lambda \in \mathbb{Z}[i]$ on ($\mathbb{Z}[i]$:n) alkuluku jos se ei ole yksikkö ja sen ainoat tekijät ovat 1 ja λ ja näiden liitännäisluvut

Huom. Huomaa, että (Gaussin) alkuluvun liitännäisluvut ovat alkulukuja.

Lause 6.4. (i) Jos $N(\lambda) = p$, $p \in \mathbb{P}$, niin λ on alkuluku $\mathbb{Z}[i]$:nä.

(ii) Jos $\lambda \in \mathbb{Z}[i]$, $\lambda \neq 0$ ja λ ei ole yksikkö, niin λ on alkulukujen tulo.

Tod. (i) Olkoon $\lambda = \lambda_1\lambda_2 \Rightarrow N(\lambda_1)N(\lambda_2) = p$
$\Rightarrow N(\lambda_1) = 1$ tai $N(\lambda_2) = 1 \Rightarrow$ joko λ_1 tai λ_2 on yksikkö.

(ii) Olkoon λ (jokin) normiltaan pienin Gaussin kokonaisluku, joka ei ole alkulukujen tulo, eikä ole yksikkö. Silloin $\lambda = \lambda_1\lambda_2$, missä λ_1 ja λ_2 eivät ole yksikköjä (koska λ ei ole itse alkuluku!). Siis

$N(\lambda_1) > 1$ ja $N(\lambda_2) > 1$. Koska $N(\lambda) = N(\lambda_1)N(\lambda_2)$, niin $N(\lambda_1), N(\lambda_2) < N(\lambda)$. Luvun λ määritelmän nojalla λ_1 ja λ_2 ovat alkulukujen tuloja. Silloin myös λ on alkulukujen tulo, ja tämä on ristiriita. □

Lause 6.5. $\mathbb{Z}[i]$ on Euklidinen kokonaisalue, eli: jos $\lambda, \mu \in \mathbb{Z}[i]$ ja $\lambda \neq 0$, niin on olemassa $k, r \in \mathbb{Z}[i]$ joille

$$\mu = k\lambda + r \quad \text{ja} \quad N(r) < N(\lambda).$$

Huom. Siirrytään Euklidisuus $\Leftrightarrow$ jakojäännöslause (Lause 1.41) yleistys!

Tod. Merkitään $\nu = \frac{\mu}{\lambda} \in \mathbb{Q}[i] \subset \mathbb{C}$ ja olkoon

$$\nu = a + ib, \quad a, b \in \mathbb{Q}.$$

Jos $\nu \in \mathbb{Z}[i]$ valitaan $k = \nu$, $r = 0$. Muussa tapauksessa valitaan $k_1, k_2 \in \mathbb{Z}$ joille

$$|k_1 - a| \leq \tfrac{1}{2} \quad \text{ja} \quad |k_2 - b| \leq \tfrac{1}{2} \quad \text{ja}$$

asetetaan $k = k_1 + ik_2$. Silloin

$$N(k - \nu) \leq \left(\tfrac{1}{2}\right)^2 + \left(\tfrac{1}{2}\right)^2 \leq \tfrac{1}{2}.$$

Jos $r = \mu - k\lambda$ pätee $\mu = k\lambda + r$ ja voimme laskea

$$\begin{aligned} N(r) &= N(\mu - k\lambda) = N(\lambda(\nu - k)) \\ &= N(\lambda)N(\nu - k) \leq \tfrac{1}{2}N(\lambda). \end{aligned}$$ □

Lemma 6.6. Jos $\lambda_1, \lambda_2 \in \mathbb{Z}[i]$ ovat $\neq 0$ ja $\lambda_1 | \lambda_2$ sekä $\lambda_2 | \lambda_1$, niin λ_1 ja λ_2 ovat liitännäisalkuja.

Tod. $\lambda_1 = k_1\lambda_2$, $\lambda_2 = k_2\lambda_1$; $k_1, k_2 \in \mathbb{Z}[i]$.
Silloin $k_1k_2 = 1$, eli k_1 ja k_2 ovat yksiköitä. □

Määr. Jos $\lambda_1, \lambda_2, \dots, \lambda_\ell \in \mathbb{Z}[i]$, asetetaan

$$I(\lambda_1, \dots, \lambda_\ell) = \{\mu_1\lambda_1 + \mu_2\lambda_2 + \dots + \mu_\ell\lambda_\ell \mid \mu_1, \dots, \mu_\ell \in \mathbb{Z}[i]\}$$

Lause 6.7. Kaikilla $\lambda_1, \dots, \lambda_\ell \in \mathbb{Z}[i]$ ($\ell \geq 1$) on olemassa $d \in \mathbb{Z}[i]$ jolle

$$I(\lambda_1, \dots, \lambda_\ell) = I(d) = \{\mu d \mid \mu \in \mathbb{Z}[i]\}$$

Tod. Voimme olettaa, että ainakin yksi luvuista λ_j on $\neq 0$ (muutoin valitsemme $d = 0$).
Valitaan $d \in I(\lambda_1, \dots, \lambda_\ell)$, jolle $d \neq 0$ ja $N(d)$ on pienin mahdollinen, erityisesti $N(d) > 0$. Tällainen voidaan valita sillä $N(d)$ saa arvoja joukosta $\mathbb{N}$. Selvästi pätee

$$(1) \qquad I(d) \subset I(\lambda_1, \dots, \lambda_\ell).$$

Jos käänteinen inkluusio ei pätisi, olisi olemassa $h \in I(\lambda_1, \dots, \lambda_\ell)$ niin että $h \notin I(d)$. Koska $\mathbb{Z}[i]$ on Euklidinen, voimme kirjoittaa

$$h = kd + r \qquad (k, r \in \mathbb{Z}[i]),\ r \neq 0,$$

niin että $N(r) < N(d)$. Silloin $r = h - kd \in I(\lambda_1, \dots, \lambda_\ell)$ ja $0 < N(r) < N(d)$, mikä on vastoin d:n valintaa. Siis (1):ssä pätee yhtäsuuruus. □

Lauseen 6.7 luku d toteuttaa s.y.t:ltä vaadittavat ominaisuudet (kts. seuraava lause ja sen todistus)

Seuraus 6.8. (i) Jos $\lambda_1, \lambda_2, \dots, \lambda_\ell \in \mathbb{Z}[i]$ (eivät kaikki nollia), on olemassa $d \in \mathbb{Z}[i]$ jolle pätee: $d \mid \lambda_j \ \forall j = 1, \dots, \ell$ ja jokainen lukujen λ_j yhteinen tekijä jakaa d:n. Tällaista lukua kutsutaan lukujen $\lambda_1, \dots, \lambda_\ell$ suurimmaksi yhteiseksi tekijäksi, merk.

$$d \in \text{s.y.t.}(\lambda_1, \dots, \lambda_\ell) \quad (\text{tai } d \in (\lambda_1, \dots, \lambda_\ell)).$$

(ii) Jos $d \in \text{s.y.t.}(\lambda_1, \dots, \lambda_\ell)$, niin $\text{s.y.t.}(\lambda_1, \dots, \lambda_\ell)$ koostuu luvuista d ja sen liitännäisluvuista.

Tod. (ii) Jos $d, d' \in \text{s.y.t.}(\lambda_1, \lambda_2, \dots, \lambda_\ell)$, niin $d \mid d'$ ja $d' \mid d \Rightarrow d$ ja d' ovat liitännäisiä (Lemma 6.6). Käänteen jokainen d:n liitännäisluku d'' selvästi toteuttaa $d'' \in \text{s.y.t.}(\lambda_1, \dots, \lambda_\ell)$.

(i) Olk. $d \in \mathbb{Z}[i]$ niin että $(d \neq 0)$

$$I(d) = I(\lambda_1, \dots, \lambda_\ell).$$

Selvästi $d \mid \lambda_j \ \forall j$ (koska $\lambda_j \in I(\lambda_1, \dots, \lambda_\ell)$).
Koska $d = \mu_1\lambda_1 + \dots + \mu_\ell\lambda_\ell$ jollakin $\mu_1, \dots, \mu_\ell \in \mathbb{Z}[i]$, niin jokainen lukujen $\lambda_1, \dots, \lambda_\ell$ yhteinen tekijä jakaa luvun d. □

Huom. Jos $\text{s.y.t.}(\lambda_1, \lambda_2, \dots, \lambda_\ell)$ koostuu vain yksiköistä, merkitsemme $(\lambda_1, \dots, \lambda_\ell) = 1$.

Lause 6.9 Jos $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}[i]$, $(\lambda_1, \lambda_2) = 1$, ja $\lambda_1 \mid \lambda_2\lambda_3$, niin $\lambda_1 \mid \lambda_3$.

Tod. Nyt $1 = \mu_1\lambda_1 + \mu_2\lambda_2$ jollakin $\mu_1, \mu_2 \in \mathbb{Z}[i]$.
Siis $\lambda_3 = \mu_1\lambda_1\lambda_3 + \mu_2(\lambda_2\lambda_3)$. □

Lause 6.10 $\mathbb{Z}[i]$:ssä jokaisella luvulla on 1-häiritsevän alkutekijähajotelman (1-häiritsevän järjestystä ja liitännäisluvuilla kertomista lukuunottamatta).

Tod. Käyttäen lausetta 6.9 on todistus täsmälleen sama kuin $\mathbb{Z}$:n tapauksessa (myös todetaan ensin, että jos $\lambda_1, \lambda_2, \dots, \lambda_k$ ovat alkulukuja ja $\lambda \mid \lambda_1 \cdots \lambda_k$, niin λ on jonkun luvuista $\lambda_1, \dots, \lambda_k$ liitännäisluku). Yksityiskohdat HT. □

Huom. Johdimme lauseen 6.10 käyttämällä vain sitä, että renkaassa $\mathbb{Z}[i]$ on määritelty normi N, joka on $\mathbb{N}$-arvoinen, multiplikatiivinen, toteuttaa ehdon $N(\lambda)=1 \Leftrightarrow \lambda =$ yksikkö ja jakojäännöslauseen 6.5. Siispä jokaisen ns. Euklidisen lukukunnan kokonaislukujen renkaassa on alkutekijöihinjako 1-häiritsevän!

Esim. 1. Etsitään luvun 5 alkutekijäesitys. Jos $5 = \lambda_1 \lambda_2$ ja $\lambda_1 = a+ib$, $\lambda_2 = c+id$, saamme $N(\lambda_1)N(\lambda_2) = 5 \cdot 5 = 25$. Jos $N(\lambda_1) = 1$, on λ_1 yksikkö, ja λ_2 on 5:n liitännäisluku. Vastaavasti tapaus $N(\lambda_1) = 1$. Jos $N(\lambda_1) = 5 = N(\lambda_2)$ niin $a^2+b^2 = 5$, josta $(a,b) = (\pm 2, \pm 1)$ tai $(b,a) = (\pm 1, \pm 2)$. Kokeilemalla nähdään, että jos $\lambda_1 = 1+2i$, niin $\lambda_2 = 1-2i$. Lauseen 6.4(i) nojalla $1 \pm 2i$ ovat alkulukuja. Siis 5:n alkulukuhajotelma voidaan kirjoittaa

$$5 = (1+2i)(1-2i)$$

(tai $5 = (-1-2i)(-1+2i)$ tai $5 = (-2+i)(-2-i)$ tai $5 = (2-i)(2+i)$)

Huom. Edellä $(1+2i)$ ja $(1-2i)$ ovat eri alkuluvuja siinä mielessä, että ne eivät ole toisiaan liitännäisluvuja.

Esim 2. Onko luku $2-3i$ luvun $7+i$ tekijä?

Ratk. $\frac{7+i}{2-3i} = \frac{(7+i)(2+3i)}{2^2+3^2} = \frac{11}{13} + \frac{23}{13}i \notin \mathbb{Z}[i]$.

Siis $2-3i$ ei ole tekijä.

Esim 3. Määritä kaikki luvun $\lambda = 7+i$ tekijät $\mathbb{Z}[i]$:ssä.

Ratk. Etsimme tekijät hieman kömpelöllä tavalla; myöhempien tulosten avulla se olisi helpompaa. Jos $\mu \mid \lambda \Rightarrow N(\mu) \mid N(\lambda)$, eli $N(\mu) \in \{1, 2, 5, 10, 25, 50\} = A$.
Jos $n \in A$, voimme etsiä kokeilemalla kaikkien luvulle $x^2+y^2 = n$. Kokeilun antaa mahdolliset tekijät

$$\mu \in \{\pm 1, \pm i, \pm 1 \pm i, \pm 1 \pm 2i, \pm 2 \pm i, \pm 3 \pm i, \pm 1 \pm 3i, \pm 4 \pm 3i, \pm 3 \pm 4i, \pm 5, \pm 5i, \pm 5 \pm 5i, \pm 7 \pm i, \pm 1 \pm 7i\}.$$

Jos $x+iy$ on $7+i$:n tekijä $\Leftrightarrow \frac{7+i}{x+iy} \in \mathbb{Z}[i]$

$$\Leftrightarrow \frac{(7x+y)+i(x-7y)}{x^2+y^2} \in \mathbb{Z}[i]$$

$$\Leftrightarrow \begin{cases} \frac{7x+y}{x^2+y^2} \in \mathbb{Z} \\ \frac{x-7y}{x^2+y^2} \in \mathbb{Z} \end{cases}$$

Sijoittamalla kaikki edellälöydetyt vaihtoehdot, saamme tehtävän joukoksi

$$\{\pm 1, \pm i, \pm 1 \pm i, \pm(2+i), \pm(1-2i), \pm(3-i), \pm(1+3i), \pm(4-3i), \pm(3+4i), \pm(7+i), \pm(1-7i)\}. \quad \square$$

Otamme tavoitteeksi määrätä kaikki $\mathbb{Z}[i]$:n alkuluvut. Tarvitsemme muutaman apulauseen.

Lause 6.11 Jos $\pi \in \mathbb{Z}[i]$ on alkuluku $\mathbb{Z}[i]$:ssä, niin on olemassa yksikäsittäinen $\mathbb{Z}$:n alkuluku $p \in \mathbb{P}$, jolle $\pi \mid p$.

Tod. Nyt $N(\pi) = \pi\overline{\pi} \in \mathbb{Z}^+$, $N(\pi) \geq 2$. Kirjoittamalla $N(\pi)$ tavallisten alkulukujen tulona, näemme että $\pi \mid p$ jollakin $p \in \mathbb{P}$. Jos p ei olisi 1-käsitteinen, olisi olemassa myös $q \in \mathbb{P}$, $q \neq p$, jolle $\pi \mid q$. Nyt $\exists\, n_1, n_2 \in \mathbb{Z}$ jolle $n_1 q - n_2 p = 1 \Rightarrow \pi \mid 1$, mikä on mahdotonta. $\square$

Ainoa tekniikaltaan hieno, jota tarvitsemme on seuraavan lemman (i)-kohta:

Lemma 6.12 (i) Jos $p \in \mathbb{P}$, $p = 4n+1$ (tai $p = 2$), on olemassa $x \in \mathbb{Z}$ jolle

$$p \mid (x^2+1).$$

(ii) Jos $p \in \mathbb{P}$, $p = 4n+3$, niin $p \neq x^2+y^2$ kaikilla $x, y \in \mathbb{Z}$.

Tod. (i) $\left(\frac{-1}{p}\right) = 1$ kun $p = 4n+1$ (Seuraus 4.6).

(ii) Seuraa suoraan tarkastelemalla vasenta ja oikeata puolta (mod 4). □

Lause 6.13 Olkoon $p \in \mathbb{P}$. Silloin

(i) Jos $p = 2$, p:n alkulukuhajoitelma on
$$2 = (1+i)(1-i),$$
missä $(1-i)$ ja $(1+i)$ ovat toistensa liitännäisalkulukuja ja $\mathbb{Z}[i]$:n alkulukuja.

(ii) Jos $p = 4n+1$, on olemassa $a, b \in \mathbb{Z}$ joille
$$p = (a+ib)(a-ib),$$
missä $a+ib$ ja $a-ib$ ovat $\mathbb{Z}[i]$:n <u>eri</u> alkulukuja.

(iii) Jos $p = 4n-1$, niin p on alkuluku myös $\mathbb{Z}[i]$:ssä.

Tod. (i) Selvästi $2 = (1+i)(1-i)$, tässä $1 \pm i$ ovat alkulukuja sillä $N(1 \pm i) = 2 \in \mathbb{P}$ (Lause 6.4(i)). Lisäksi $1+i = i(1-i)$, joten luvut ovat liitännäisalkulukuja.

(ii) Lemman 6.12 on olemassa $x \in \mathbb{Z}$ jolle $p \mid (x^2+1)$ eli $p \mid (x+i)(x-i)$. Jos p olisi $\mathbb{Z}[i]$:n alkuluku, tulisi olla
$$p \mid (x+i) \text{ tai } p \mid (x-i).$$
Tämä on mahdotonta, sillä $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$.

Siis $p = \pi\mu$, missä $\pi \in \mathbb{Z}[i]$ on alkuluku ja $\mu \in \mathbb{Z}[i]$ ei ole yksikkö. Erityisesti

$$N(p) = p^2 = N(\pi)N(\mu), \quad 1 < N(\pi), N(\mu).$$

Ainoa mahdollisuus on, että $N(\pi) = p$, eli $\pi\overline{\pi} = p \Rightarrow \mu = \overline{\pi}$. Selvästi π ja $\overline{\pi}$ ovat yhtäaikaisesti alkulukuja, joten kirjoittamalla $\pi = a+ib$ saadaan alkuosa väitteestä. Tulee vielä osoittaa, etteivät π ja $\overline{\pi}$ ole liitännäisiä. Suora tarkastus osoittaa, että jos $\pi = \varepsilon\overline{\pi}$, missä ε yksikkö (eli $\varepsilon \in \{\pm 1, \pm i\}$), niin joko $\pi \in \mathbb{Z}$, $\pi \in i\mathbb{Z}$ tai $\pi = a \pm ia$, $a \in \mathbb{Z}$, ja mikään näistä vaihtoehdoista ei tule kysymykseen.

(iii) Jos p ei olisi $\mathbb{Z}[i]$:n alkuluku, päättelisimme, että $p = a^2+b^2$ kuten (ii)-kohdassa. Tämä on mahdotonta Lemman 6.12 (ii) nojalla. □

Seuraus 6.14. *$\mathbb{Z}[i]$:n alkuluvut ovat luvut* ① $1+i$, ② $p = 4n-1 \in \mathbb{P}$ *ja* ③ $a \pm ib$, *missä* $p = a^2+b^2 = 4n+1 \in \mathbb{P}$, *sekä kaikki e.m. lukujen liitännäisluvut.*

Tod. Jos $\pi \in \mathbb{Z}[i]$ on alkuluku, jakaa se Lauseen 6.11 nojalla jonkin tavallisen alkuluvun $p \in \mathbb{P}$. Väite seuraa nyt Lauseesta 6.13. □

Seuraus 6.15 *Tavallinen alkuluku $p \in \mathbb{P}$ voidaan lausua, kahden neliön summana $p = a^2+b^2$ $(a, b \in \mathbb{Z})$ jos ja vain jos $p = 2$ tai p on muotoa $4n+1$. Esitys on 1-käsitteinen lukujen a ja b etumerkkejä ja järjestystä vaille.*

Tod. Muotoa $p = 4n-1 \in \mathbb{P}$ olevat luvut eivät ole 2:n neliön summia Lemman 6.12 (ii) nojal. Ja. Luvut $p=2$ tai $p = 4n+1 \in \mathbb{P}$ puolestaan ovat, mihin seuraa suoraan lauseesta 6.13. Olkoon $p = (a+ib)(a-ib) = \pi\bar{\pi}$ kuten lauseessa 6.13. Jos $p = (a'+ib')(a-ib') = \pi'\bar{\pi}'$ on toinen esitys, ovat π' (ja $\bar{\pi}'$) alkulukuja. Lauseen 6.4 (i) nojalla, sillä taas päätellemme, että $N(\pi') = N(\bar{\pi}') = p$. Siis $\pi\bar{\pi} = \pi'\bar{\pi}'$, ja alkuluvunhajoitelmien 1-käsitteisyyden nojalla π' on joko π:n tai $\bar{\pi}$:n liitännäisluku, mistä jälkimmäinen väite seuraa. □

Esim. $5 = 2^2+1^2$, 7 ei ole kahden neliön summa, 107 ei ole myöskään, mutta 113 on (esim. $113 = 7^2+8^2$).

Selvitämme nyt mikähän kaikki luvut voidaan kunna kahden (kokonaisluvun neliöiden summana. Tätä varten on hyödyllistä ensin huomata, että

Lemma 6.16 $n \in \mathbb{N}$ voidaan kunna kahden neliön summana täsmälleen kun

$$n = \lambda\bar{\lambda} = N(\lambda)$$

jollakin $\lambda \in \mathbb{Z}[i]$.

Tod. Jos $\lambda = x+iy$, niin $n = \lambda\bar{\lambda} \Leftrightarrow n = x^2+y^2$. □

Lause 6.17. Olkoon $n \in \mathbb{N}$. Tällöin

$$n = x^2 + y^2$$

jollakin $x, y \in \mathbb{Z}$ jos ja vain jos jokainen muotoa $4k-1$ oleva n:n alkutekijä esiintyy parillisena potenssina n:n alkulukuhajotelmassa.

Tod. Olkoon $n = 2^e p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_\ell^{\beta_\ell}$, missä p_j:t ovat muotoa $4k+1$ olevia ja q_j:t muotoa $4k-1$ olevia tavallisia alkulukuja. Valitaan jokaiselle $j \le k$ luku $\lambda_j \in \mathbb{Z}[i]$ jolle $N(\lambda_j) = \lambda_j \overline{\lambda_j} = p_j$ (Seuraus 6.15, Lemma 6.16). Jos jokainen β_j on parillinen, saamme

$$N(\lambda) = n,$$

missä $$\lambda = (1+i)^e \left(\prod_{j=1}^{k} \lambda_j^{\alpha_j} \right) \prod_{s=1}^{\ell} q_s^{\beta_s/2},$$

eli n voidaan esittää kahden neliön summana. Oletetaan sitten, että vaikkapa β_1 on pariton (ja tietysti $q_j \neq q_1$ kun $j \ge 2$)[x]. $N_{\mathbb{Z}[i]}$:n q_1 on $\mathbb{Z}[i]$:n alkuluku (Lause 6.13). Olkoon $n = x^2 + y^2 = (x+iy)(x-iy)$, ja olkoon q_1^r korkein q_1:n potenssi, joka jakaa luvun $x+iy$. Sillon konjugoimalla näemme, että q_1^r on myös korkein q_1:n potenssi, joka jakaa luvun $x-iy$. Yhteensä q_1^{2r} on korkein q_1:n potenssi joka jakaa luvun n[x], mikä on vastoin n:n alkulukuhajotelmaa

$$n = (1+i)^e (1-i)^e \lambda_1^{\alpha_1} \overline{\lambda_1}^{\alpha_1} \cdots \lambda_k^{\alpha_k} \overline{\lambda_k}^{\alpha_k} q_1^{\beta_1} \cdots q_\ell^{\beta_\ell}.$$

Siis oletus $n = x^2 + y^2$ oli väärä, ja tässä tapauksessa n ei ole kahden neliön summa. □

---

x) Huomaa, että luvut $1 \pm i$, $\lambda_j, \overline{\lambda_j}$, $q_2, \ldots, q_\ell$ eivät ole q_1:n konjugaatteja.

Viimeinen tuloksemme kahden neliön summana esittämisestä laskee eri esitysten lukumäärän:

Lause 6.18. Olkoon $n \geq 1$,

$$n = 2^{e_0} \prod_{j=1}^{k} p_j^{\alpha_j} \prod_{s=1}^{\ell} q_s^{\beta_s},$$

missä $p_j \in \mathbb{P}$ ovat eri alkulukuja muotoa $4k+1$ ja $q_s \in \mathbb{P}$ ovat eri alkulukuja muotoa $4k-1$. Merkitään symbolilla $r_2(n)$ luvun n eri esitysten lukumäärää kahden neliön summana. Silloin $r_2(n) = 0$ jos jokin eksponenteista β_s on pariton. Muussa tapauksessa, jos kaikki β_s:t ovat parillisia, niin

$$r_2(n) = 4 \prod_{j=1}^{k} (1+\alpha_j).$$

Tod. Lauseen 6.17 nojalla voimme olettaa että kaikki β_s:t ovat parillisia. Meidän on etsittävä lukujen $\lambda \in \mathbb{Z}[i]$ lukumäärä, joille

$$(1) \qquad \lambda\bar{\lambda} = n = (1-i)^{e_0}(1+i)^{e_0} \prod_{j=1}^{k} \lambda_j^{\alpha_j} \prod_{j=1}^{k} \bar{\lambda}_j^{\alpha_j} \prod_{s=1}^{\ell} q_s^{\beta_s},$$

missä kirjoitimme $p_j = \lambda_j\bar{\lambda}_j$ sopivalla $\mathbb{Z}[i]$:n alkuluvulla λ_j. Luvut q_s ovat $\mathbb{Z}[i]$:n alkulukuja. Luvun λ alkutekijöiden tulee kuulua lukuihin $\lambda_j, \bar{\lambda}_j, (1+i), q_s$ $(1 \leq j \leq k,\ 1 \leq s \leq \ell)$ — huomaa (lause 6.13), että λ_j ja $\bar{\lambda}_j$ ovat eri alkulukuja, mutta $1+i$ ja $1-i$ ovat toistensa konjugaatteja. Voimme siis kirjoittaa

$$\lambda = i^{\nu}(1+i)^{\mu} \prod_{j=1}^{k} \lambda_j^{k_j} \prod_{j=1}^{k} \bar{\lambda}_j^{k_j'} \prod_{s=1}^{\ell} q_s^{\gamma_s},$$

missä $\nu \in \{0,1,2,3\}$ (i^{ν} on mo. yksikkö), $\mu \geq 0$, $k_j \geq 0$, $k_j' \geq 0$ ja $\gamma_s \geq 0$.

Eri eksponenttien arvoilla saamme eri lukuja λ (miksi?). Kertomalla $\lambda\bar{\lambda}$ saamme yhtälön

$$n = \lambda\bar{\lambda} = i^{\nu} i^{-\nu} (1+i)^{\mu} (1-i)^{\mu} \prod_{j=1}^{k} \lambda_j^{\ell_j} \prod_{j=1}^{k} \bar{\lambda}_j^{\ell_k} \prod_{j=1}^{k} \bar{\lambda}_j^{\ell'_j} \prod_{j=1}^{k} \lambda_j^{\ell'_j} \prod_{s=1}^{\ell} q_s^{2\varkappa_s}$$

$$= 2^{\mu} \prod_{j=1}^{k} p_j^{\ell_j + \ell'_j} \prod_{s=1}^{\ell} q_s^{2\varkappa_s}$$

Saamme yhtälöt

(1) $2\varkappa_s = B_s \quad \forall s \in \{1, \dots, \ell\}$

(2) $\ell_j + \ell'_j = d_j \quad \forall j \in \{1, \dots, k\}$

Jäljellä jäävä yhtälö voidaan kirjoittaa $2^{\mu} = 2^{e_0}$, josta saamme $\mu = e_0$. Samoin (1) määrää luvut $\varkappa_s$ täysin. Puolestaan j. yhtälöllä (2) on $d_j + 1$ positiivista ratkaisua. Luku ν voidaan valita vapaasti neljästä vaihtoehdosta. Yhteensä ratkaisujen lukumäärä siis

$$4 \prod_{j=1}^{k} (1 + d_j) \quad \square$$

Esim. Jos $n = 500$ kirjoitamme

$$500 = 2^2 5^3$$

Ratkaisuja on $4 \cdot (3+1) = 16$ kpl. Löytääksemme ne oletamme, että $5 = (2+i)(2-i)$. Siispä eri ratkaisut yhtälölle $\lambda\bar{\lambda} = 500$ ovat (vrt. ed. tehtävä)

$$i^{\nu} (1+i)^2 (2+i)^a (2-i)^{3-a} \qquad (0 \le \nu \le 3,\ 0 \le a \le 3)$$

eli luvut $2(2+i)^a (2-i)^{3-a}$ sekä näiden liitännäisluvut. Laskun antaa esitykset

$$500 = (\pm 4)^2 + (\pm 22)^2 = (\pm 22)^2 + (\pm 4)^2 = (\pm 10)^2 + (\pm 20)^2 = (\pm 20)^2 + (\pm 10)^2 .$$

Kvadraattisista lukukunnista

Edellä $\mathbb{Q}(i)$ saatiin liittämällä i kuntaan $\mathbb{Q}$. Yleisemmin voidaan tarkastella kuntaa $\mathbb{Q}(\sqrt{D})$, missä $D \in \mathbb{Z}$ ($|D|$:llä ei epätriviaaleja neliötekijöitä). Käy ilmi, että kunnan $\mathbb{Q}(\sqrt{D})$ kokonaisluvuiksi on luonnollista määritellä luvut

$$a + bw \quad (a, b \in \mathbb{Z}),$$

missä $w = \begin{cases} \sqrt{D}, & \text{jos } D \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{D}}{2}, & \text{jos } D \equiv 1 \pmod 4. \end{cases}$

Yksi tärkeimmistä kysymyksistä on: onko $\mathbb{O}(\sqrt{D})$:n kokonaislukujen alkutekijöihin jako yksikäsitteinen? Tapauksessa $\mathbb{Q}(i)$ vastaus oli myönteinen (lause 6.10). Aina tämä ei ole voimassa:

Esim. $\mathbb{Q}(\sqrt{-5})$:ssä $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

(HT: osoita että $2, 3, 1 \pm \sqrt{-5}$ ovat alkuelukuja $\mathbb{Q}(\sqrt{D})$:ssä).

Kunnassa $\mathbb{O}(\sqrt{D})$ voidaan määritellä normi. Jos lauseen 6.5 vastine pätee kunnan $\mathbb{O}(\sqrt{D})$ kokonaisluvuille, sanomme että kunta on Euklidinen. Antamme todistus lauseille 6.7-6.10 toimii silloin ilman muutoksia ja saamme tuloksen:

- Euklidisessa lukukunnassa alkutekijöihinjako on yksikäsitteinen.

Milloin $\mathbb{Q}(\sqrt{D})$ on Euklidinen?

- jos $D<0$ on $\mathbb{Q}[\sqrt{D}]$ Euklidinen jos ja vain jos $D \in \{-1,-2,-3,-7,-11\}$ (helppo)
- jos $D>0$ on $\mathbb{Q}[\sqrt{D}]$ Euklidinen jos ja vain jos

$D \in \{2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73\}$

(vaikea, 1950-luvulta).

Myös eräillä muilla D:n arvoilla on alkuteki. jöihin jako 1-häviteinen, esim. negatiivisilla D kun $D \in \{-19,-43,-67,-163\}$.

Avoin kysymys: Onko olemassa ∞ monta $D>0$ joille $\mathbb{Q}[\sqrt{D}]$:ssä alkutekijöihin jako on 1-häviteinen?

Alkutekijöihin jaon 1-häviteisyysongelma ratkaise siirtymällä ideaalien teoriaan (Kummer, Dedekind, ...) Edellisiä kysymyksiä voi tosin tarkastella yleisemmässä lukurenkaassa $\mathbb{Q}[x_0]$, missä x_0 on mv. algebrallinen luku. Tällä kurssilla emme kuitenkaan laajenna tarkastelujamme $\mathbb{Q}[i]$:n ulkopuolelle.

Lagrangen lause: luvun esitys 4:n neliön summana

Todistamme kurssimme päätteeksi kuuluisan tuloksen, jonka mukaan jokainen positiivinen kokonaisluku on 4:n neliön summa (Fermat?, ensimmäinen julkaistu todistus Lagrangelta. Sovellamme todistuksessa

'äärettömän laskeutumisen menetelmää', jota Fermat sovelsi vaikeissa tilanteissa.

Esim. $11 = 9+1+1+0$, $152 = 100+36+16+0$, $7 = 4+1+1+1$.
Tapaus 7 osoittaa, että 3 neliötä riitä yleisesti.

Lause 6.19 Jokaisella $n \in \mathbb{N}$ on olemassa $x,y,z,w \in \mathbb{Z}$ joille
$$n = x^2+y^2+z^2+w^2$$

Tod. Sovellamme yllättävää identiteettiä

(1) $$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)$$
$$= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 + (x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2$$
$$+ (x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2 + (x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2$$

Tämän nojalla, jos luvut n_1 ja n_2 ovat kumpikin 4:n neliön summia, niin myös n_1n_2 on.
Siispä riittää todistaa, että jokainen alkuluku $p \in \mathbb{P}$, $p \geq 3$ on lausuttavissa 4:n neliön summana (huomaa, että $2 = 1^2+1^2+0^2+0^2$).
Osoitamme ensin, että jokin p:n moniherta on tätä muotoa.

Lemma 6.20 Jos $p \geq 3$, $p \in \mathbb{P}$, on olemassa $x,y \in \mathbb{Z}$ joille $1+x^2+y^2 = mp$, missä $m < p$.

Tod. Tarkastellaan lukuja $0^2, 1^2, \dots, \left(\frac{p-1}{2}\right)^2$.
Ne ovat kerrenään epäkongruentteja,
ja niitä on $\frac{1}{2}(p+1)$ kpl. Samo pätee luvuille

$$-1-0^2, -1-1^2, -1-2^2, \dots, -1-\left(\frac{p-1}{2}\right)^2.$$

Yhteensä lukuja $(p+1)$ kpl. Kyyhkyslakka periaatteen nojalla (sijoita ensin ensimmäisen joukon luvut, sitten toisen) joku ensimmäisen joukon luvuista, olkoon se x^2, on kongruentti jonkin jälkimmäisen joukon luvun kanssa, olkoon se $-1-y^2$. Siis

$$x^2 \equiv -1-y^2 \quad \text{eli} \quad p \mid (x^2+y^2+1).$$

Lisäksi $m = \dfrac{x^2+y^2+1}{p} \le \dfrac{2\left(\frac{p-1}{2}\right)^2+1}{p} < p$. ∎

Olkoon nyt $m \ge 1$ <u>pienin luku</u>, jolle pätee

$$(2)\quad mp = x_1^2+x_2^2+x_3^2+x_4^2$$

joillakin $x_1, \dots, x_4$. Edellisen kommen perusteella m on hyvin määritelty ja $m < p$. Halvamme osoittaa, että $m = 1$. Tehdään vastaoletus ja johdetaan ristiriita.

(To) <u>Jos m on parillinen</u>, silloin joko

(i) x_1, x_2, x_3, x_4 ovat kaikki parillisia
(ii) — " — — " — — " — parittomia
(iii) kaksi luvuista, esim. x_1 ja x_2 ovat parillisia, x_3 ja x_4 parittomia.

Tapaus (i) on mahdoton, koska silloin

$$\frac{1}{4}mp = \left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2 + \left(\frac{x_4}{2}\right)^2.$$

Tapauksissa (ii) ja (iii) luvut x_1+x_2, x_1-x_2, x_3+x_4 ja x_3-x_4 ovat parittomia, jolloin

$$\frac{1}{2}mp = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2,$$

mikä on taas vastoin luvun m valintaa. Siispä m on pariton!

(2$_0$) Jos m on pariton, silloin $m \geq 3$.

Jos kaikki luvut esityksessä (2) olisivat jaollisia m:llä, seuraisi $m \mid p$, mikä on mahdotonta koska $1 < m < p$. Voimme siis valita *itseisesti pienimmät jäännökset* y_1, y_2, y_3, y_4 ja luvut $b_1, \dots, b_4$ niin että

$$\begin{cases} y_i = x_i - b_i m & (1 \leq i \leq 4), \\ |y_i| < \frac{1}{2}m \quad \text{ja jokin } y_i \neq 0. \end{cases}$$

↖ m pariton!

Silloin $0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\left(\frac{1}{2}m\right)^2 < m^2$.

Lisäksi (huomaa, että $y_i \equiv x_i \pmod m$)

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod m$$

Siispä

$$(3) \quad \begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= mp \quad (1 < m < p) \\ y_1^2 + y_2^2 + y_3^2 + y_4^2 &= mm_1 \quad (1 < m_1 < m) \end{aligned}$$

Kertomalla yhtälöt puolittain ja soveltamalla lemmaa (1) saamme

$$\begin{aligned} m^2 m_1 p &= (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &= z_1^2 + z_2^2 + z_3^2 + z_4^2, \end{aligned}$$

missä

$$\begin{cases} z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ \quad \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod m \\ z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\ \quad \equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 = 0 \pmod m \\ z_3 = x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \\ \quad \equiv x_1x_3 - x_3x_1 + x_4x_2 - x_2x_4 = 0 \pmod m \\ z_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \\ \quad \equiv x_1x_4 - x_4x_1 + x_2x_3 - x_3x_2 = 0 \pmod m \end{cases}$$

Siispä luvut $t_i = z_i/m$ ovat kokonaislukuja $(i=1,\dots,4)$ ja

$$t_1^2 + t_2^2 + t_3^2 + t_4^2 = m_1 p ,$$

missä $1 \le m_1 < m$, mikä on mahdotonta. □

Huom. Hilbert osoitti n. 1910 analyyttisen menetelmän: jos $k \ge 1$ on kiinnitetty, niin on olemassa luku $r = r(k)$ jolle jokainen $n \ge 1$ on laskettavissa muodossa

$$n = x_1^k + \dots + x_r^k \qquad (x_1, \dots, x_r \in \mathbb{N} \cup \{0\}).$$

Tämä ratkaisi kuuluisan ns. Waringin ongelman.

FIN