LUKUTEORIAN ALKEET KL 2007 JA 2009

HELI TUOMINEN

Sisältö

Alkusanat

Tässä on muistiinpanot vuosina 2007 ja 2009 luennoimastani kurssista *Lukuteorian alkeet*. Kurssi on suunnattu erityisesti aineenopettajiksi opiskeleville mutta on toki sallittu muillekin. Kurssin laajuus on 4 op (2 ov). Mielenkiintoisia hetkiä lukuteorian parissa.

- Heli -

Versio: 26. helmikuuta 2009.

Käytämme seuraavia standardimerkintöjä:

$$\mathbb{N} = \{1, 2, 3, \dots\} \text{ luonnolliset luvut}$$
$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} \text{ kokonaisluvut}$$

1. Lukujärjestelmät

1.1. **Kymmenjärjestelmä.** Kymmenjärjestelmän luku 1907 voidaan esittää kantaluvun 10 potenssisummana

$$1907 = \underline{1} \cdot 10^3 + \underline{9} \cdot 10^2 + \underline{0} \cdot 10^1 + \underline{7} \cdot 10^0.$$

Numeromerkit tarvitaan kantalukua 10 pienemmille luonnollisille luvuille (1, 2, 3, 4, 5, 6, 7, 8, 9) ja 0:lle. Yleisen säännön mukaan kymmenenpotenssit jätetään pois ja numeron sijainti kertoo, mitä kymmenenpotenssia se esittää.

Huomaa 0:n merkitys: luvussa 1907 ei ole kymmeniä, mutta sitä ei voi merkitä symbolilla 197, sillä

$$197 = \underline{1} \cdot 10^2 + \underline{9} \cdot 10^1 + \underline{7} \cdot 10^0.$$

1.2. **Muita lukujärjestelmiä.** Kantaluvuksi voidaan valita jokin muu ykköstä suurempi luonnollinen luku kuin 10. Seuraavassa luvussa todistamme, että jokainen luonnollinen luku voidaan esittää yksikäsitteisenä potenssisummana valitun kantaluvun avulla. Todistuksessa käytämme *kokonaislukujen jakoyhtälöä*, joka helpottaa myös muunnoksia lukujärjestelmien välillä.

Lause 1.2.1 (Jakoyhtälö)**.** *Olkoot $a, b \in \mathbb{Z}$ ja olkoon $b \neq 0$. Tällöin on yksikäsitteiset luvut $q, r \in \mathbb{Z}$, joille*

$$a = qb + r \quad ja \quad 0 \leq r < |b|.$$

Jakoyhtälön luku a on *jaettava*, b *jakaja*, q *(vaillinainen) osamäärä* ja luku r on *jakojäännös*.

Todistus. Myöhemmin. □

Jos kantaluvuksi valitaan esimerkiksi 8, niin saadaan kahdeksanjärjestelmä, jonka perustana käytetään luvun 8 peräkkäisiä potensseja: $8^0, 8^1, 8^2, 8^3$ jne.

Esimerkki 1.2.2. Kymmenjärjestelmän luku 103 muunnetaan kahdeksanjärjestelmään (soveltamalla jakoyhtälöä kahteen kertaan ja) esittämällä se kahdeksan potenssien summana

$$103 = \begin{cases} 12 \cdot 8 + 7 = (1 \cdot 8 + 4)8 + 7 = \underline{1} \cdot 8^2 + \underline{4} \cdot 8^1 + \underline{7} \cdot 8^0 = 147_8 \\ 1 \cdot 64 + 39 = 1 \cdot 64 + (4 \cdot 8 + 7) = \underline{1} \cdot 8^2 + \underline{4} \cdot 8^1 + \underline{7} \cdot 8^0 = 147_8. \end{cases}$$

Kahdeksanpotenssit jätetään yleensä kirjoittamatta ja kantaluku 8 merkitään luvun oikeaan alakulmaan. Esimerkin 1.2.2:n luku 147_8 luetaan "*yksineljä-seitsemän*" eikä "sataneljäkymmentäseitsemän". Jälkimmäinen lukutapa viittaa kymmenjärjestelmään, jonka kantalukua ei merkitä näkyviin.

Esimerkki 1.2.3. Luku 2007_8 muunnetaan kymmenjärjestelmään seuraavasti

$$2007_8 = 2 \cdot 8^3 + 0 \cdot 8^2 + 0 \cdot 8^1 + 7 \cdot 8^0 = 2 \cdot 512 + 7 = 1031.$$

Huomaa, että kahdeksanpotenssien kertoimina voivat esiintyä luvut $0, 1, 2, 3, 4, 5, 6$ ja 7 (vertaa kymmenjärjestelmä). Yleisesti k-järjestelmässä, missä k on ykköstä suurempi luonnollinen luku, tarvitaan numeromerkit kantalukua k pienemmille luonnollisille luvuille ja nollalle.

Tietokoneissa käytetään luvun 2 potensseihin perustuvia lukujärjestelmiä, erityisesti kaksi- ja kuusitoistajärjestelmiä. Näistä edellistä sanotaan binääri- ja jälkimmäistä heksadesimaalijärjestelmäksi. Heksadesimaalijärjestelmässä luvuille $10, 11, 12, 13, 14$ ja 15 käytetään symboleja A, B, C, D, E ja F.

Esimerkki 1.2.4.

(a) Luku 1234 muunnetaan 16-järjestelmään seuraavasti

$$1234 = 77 \cdot 16 + 2 = (4 \cdot 16 + 13) \cdot 16 + 2 = \underline{4} \cdot 16^2 + \underline{13} \cdot 16^1 + \underline{2} \cdot 16^0 = 4D2_{16}.$$

(b) Luku $10B_{16}$ muunnetaan 10-järjestelmään seuraavasti

$$10B_{16} = 1 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 256 + 11 = 267.$$

Lukujärjestelmissä, joiden kantaluku on kymmenestä eroava, voidaan laskea "tavalliseen tapaan" muuntamatta lukuja 10-järjestelmään.

Esimerkki 1.2.5.

(a) Laske $357_8 + 126_8$. Huomaa, että $7_8 + 6_8 = 15_8$ ja $1_8 + 5_8 + 2_8 = 10_8$. Muistinumerot saadaa kyseisen sarakkeen täysien kahdeksaisten määrästä.

$$\begin{array}{r} 357_8 \\ +\underline{126_8} \\ 505_8 \end{array}$$

(b) Laske $111110_2 + 11001_2$.

$$\begin{array}{r} 111110_2 \\ +\ \underline{11001_2} \\ 1010111_2 \end{array}$$

(c) Laske $1001_2 + 1001_4$. Muunnetaan ensin luku 1001_4 kaksijärjestelmään: $1001_4 = 4^3 + 1 = (2^2)^3 + 1 = 2^6 + 1 = 1000001_2$. Nyt

$$\begin{array}{r} 1000001_2 \\ +\quad 1001_2 \\ \hline 1001010_2 \end{array}$$

eli kysytty summa on 1001010_2.

Esimerkki 1.2.6. Laaditaan kaksi- ja neljäjärjestelmien kertotaulut.

	1	10_2
1	1	10_2
10_2	10_2	100_2

	1	2	3	10_4
1	1	2	3	10_4
2	2	10_4	12_4	20_4
3	3	12_4	21_4	30_4
10_4	10_4	20_4	30_4	100_4.

1.3. **Yksikäsitteisyyslause.** Osoitetaan, että jokaisella luonnollisella luvulla on yksikäsitteinen esitys valitussa lukujärjestelmässä. Todistusta varten palautetaan mieliin induktioperiaate, jonka avulla on kätevä todistaa luonnollisia lukuja koskevia väitteitä.

INDUKTIOPERIAATE A: Olkoon $P(n)$ lukuun $n \in \mathbb{N}$ liittyvä väitelause. Jos $P(1)$ on totta ja jos kaikilla $k \in \mathbb{N}$ siitä, että $P(k)$ on totta seuraa, että $P(k+1)$ on totta, niin $P(n)$ on totta kaikilla $n \in \mathbb{N}$.

Induktioperiaate esitetään usein seuraavissa, edellisen kanssa (loogisesti) ekvivalenteissa muodoissa. (**Mieti, osa harjoitus 1:ssä**)

INDUKTIOPERIAATE B: Jos $Q \subset \mathbb{N}$ on joukko, jolle $1 \in Q$ ja kaikille $k \in \mathbb{N}$ ehdosta $k \in Q$ seuraa, että $k + 1 \in Q$, niin $Q = \mathbb{N}$.

13.1 ==========

INDUKTIOPERIAATE A': Jos $P(1)$ on totta ja jos kaikilla $k \in \mathbb{N}$ siitä, että $P(1), P(2), \ldots, P(k)$ ovat totta seuraa, että $P(k + 1)$ on totta, niin $P(n)$ on totta kaikilla $n \in \mathbb{N}$.

INDUKTIOPERIAATE B': Jos $Q \subset \mathbb{N}$ on joukko, jolle $1 \in Q$ ja kaikille $k \in \mathbb{N}$ ehdosta $1, 2, \ldots, k \in Q$ seuraa, että $k + 1 \in Q$, niin $Q = \mathbb{N}$.

HYVÄN JÄRJESTYKSEN PERIAATE (Well-ordering principle): Jos $C \subset \mathbb{N}$ on epätyhjä joukko, niin C:ssä on pienin alkio.

Lause 1.3.1. *Olkoot $n, k \in \mathbb{N}$, $k > 1$. Tällöin on yksikäsitteiset kokonaisluvut $s \geq 0$ ja $a_0, a_1, \ldots a_s$, joille*

$$n = a_s k^s + a_{s-1} k^{s-1} + \cdots + a_1 k + a_0 \tag{1.3.1}$$

$$0 \leq a_i < k \text{ kaikilla } i = 0, 1, \ldots, s \tag{1.3.2}$$

$$a_s > 0. \tag{1.3.3}$$

Todistus.
Olemassaolo: Todistetaan esityksen olemassaolo induktiolla n:n suhteen: induktioperiaatteen B' joukkona Q ovat ne luonnolliset luvut, jolle väitteen esitys on olemassa.

Jos $n = 1$, niin voidaan valita $s = 0$ ja $a_0 = 1$. Siten $1 \in Q$.

Oletetaan, että $1, 2, \ldots, n-1 \in Q$. Koska $k > 1$, niin on yksikäsitteinen suurin kokonaisluku $s \geq 0$, jolle $k^s \leq n$. Tällöin siis

$$k^s \leq n < k^{s+1}. \tag{1.3.4}$$

Jakoyhtälön (Lause 1.2.1) perusteella on yksikäsitteiset $a_s, r \in \mathbb{Z}$, joille

$$n = a_s k^s + r,$$

missä $0 \leq r < k^s$. Lisäksi on $0 < a_s < k$. (**Harjoitus 1**)

Jos $r = 0$, niin voidaan lopettaa. Oletetaan, että $r > 0$. Koska $r \in \mathbb{N}$ ja $r < n$, niin induktio-oletuksen mukaan on kokonaisluvut $t \geq 0$ ja $b_0, \ldots, b_t$, joille

$$r = b_t k^t + \cdots b_1 k + b_0,$$

$0 \leq b_i < k$ kaikilla $0, 1, \ldots, t$ ja $b_t > 0$. Koska $r < k^s$, niin on $t < s$. Siten

$$n = a_s k^s + 0 \cdot k^{s-1} + \cdots + 0 \cdot k^{t+1} + b_t k^t + \cdots b_1 k + b_0.$$

Siten $n \in Q$. Induktioperiaatteen B' nojalla esityskaava on voimassa kaikilla $n \in \mathbb{N}$.

Yksikäsitteisyys: Olkoon $n \in \mathbb{N}$. Oletetaan, että on kokonaisluvut $s, t \geq 0$, $a_0, a_1, \ldots a_s$, $b_0, b_1, \ldots b_t$ joille $0 \leq a_i < k$, kaikilla $i = 0, 1, \ldots, s$, $0 \leq b_j < k$, kaikilla $j = 0, 1, \ldots, t$, $a_s > 0$, $b_t > 0$ ja

$$n = a_s k^s + \cdots + a_1 k + a_0 = b_t k^t + \cdots + b_1 k + b_0. \tag{1.3.5}$$

Vähentämällä luvun n esitykset yhtälössä (1.3.5) saadaan

$$0 = e_m k^m + \cdots + e_1 k + e_0, \tag{1.3.6}$$

missä $e_i = a_i - b_i$ ja m on suurin kokonaisluku, jolle $a_i \neq b_i$. Tällöin $e_m \neq 0$.

Jos olisi $m = 0$, niin olisi $0 \neq e_m = e_0 = 0$, mikä on ristiriita. On siis oltava $m > 0$. Koska $0 \leq a_i < k$ ja $0 \leq b_i < k$ kaikilla indekseillä i, niin

$$|e_i| = |a_i - b_i| \leq k - 1 \tag{1.3.7}$$

kaikilla $i = 0, 1, \ldots, m$. Nyt käyttämällä tietoa $e_m \in \mathbb{Z} \setminus \{0\}$, kaavaa (1.3.6), kolmioepäyhtälöä, arviota (1.3.7) ja geometrisen summan kaavaa, saadaan

$$\begin{aligned} k^m &\leq |e_m k^m| = |e_{m-1} k^{m-1} + \cdots + e_1 k + e_0| \\ &\leq |e_{m-1}| k^{m-1} + \cdots + |e_1| k + |e_0| \\ &\leq (k-1)(k^{m-1} + \cdots + k + 1) = k^m - 1, \end{aligned}$$

mikä on ristiriita. On siis oltava $s = t$ ja $a_i = b_i$ kaikilla $i = 0, 1, \ldots, s$. Siten luvun n esitys halutulla tavalla on yksikäsitteinen. □

2. Alkulukuteoriaa

Alkuluvut ovat kiinnostaneet matemaatikoita Pythagoraan koulukunnan ajoista lähtien. Monet matematiikan ratkaisemattomista ongelmista liittyvät alkulukuihin. Tässä luvussa osoitamme, että jokainen luonnollinen luku $n > 1$ voidaan esittää alkulukujen tulona täsmälleen yhdellä tavalla tekijöiden järjestystä vailla. Näytämme myös, että alkulukuja on äärettömän monta ja tutkimme alkulukujen esiintymistiheyttä. Ennen näitä tuloksia keskustelemme jaollisuudesta ja etsimme suurinta yhteistä tekijää.

2.1. **Jaollisuus.**

Määritelmä 2.1.1. Olkoot $n, m \in \mathbb{Z}$. Luku n on *jaollinen* luvulla m jos

$$n = km \quad \text{jollain } k \in \mathbb{Z}.$$

Tällöin sanotaan, että m on luvun n *tekijä/jakaja* ja että m *jakaa* luvun n. Jos n on jaollinen luvulla m, niin merkitään $m \mid n$. Jos n ei ole jaollinen luvulla m, niin merkitään $m \nmid n$.

Seuraava lause kertoo jaollisuuden ominaisuuksia.

Lause 2.1.2. *Olkoot $n, m, d, a, b \in \mathbb{Z}$. Tällöin*

(1) $n \mid n$ (refleksiivisyys)
(2) *jos* $d \mid n$ *ja* $n \mid m$, *niin* $d \mid m$ (transitiivisuus)
(3) *jos* $d \mid n$ *ja* $d \mid m$, *niin* $d \mid (an + bm)$ (lineaarisuus)
(4) *jos* $d \mid n$, *niin* $ad \mid an$ (tulo)
(5) *jos* $ad \mid an$ *ja* $a \neq 0$, *niin* $d \mid n$ (supistaminen)
(6) $1 \mid n$
(7) $n \mid 0$
(8) *jos* $0 \mid n$, *niin* $n = 0$
(9) *jos* $d \mid n$ *ja* $n \neq 0$, *niin* $|d| \leq |n|$ (vertailu)
(10) *jos* $d \mid n$ *ja* $n \mid d$, *niin* $|d| = |n|$

Todistus. Todistetaan (9), muut kohdat jätetään harjoitustehtäväksi.

Koska $d \mid n$, niin on $k \in \mathbb{Z}$, jolle $n = dk$. Koska $n \neq 0$, niin $k \neq 0$. Lisäksi koska $k \in \mathbb{Z}$, niin $|k| \geq 1$. Siten

$$|n| = |dk| = |d||k| \geq |d|.$$

□

Esimerkki 2.1.3. Luvun 6 tekijät ovat $\pm 1, \pm 2, \pm 3$ ja ± 6.

Esimerkki 2.1.4. Jos luku $k \in \mathbb{Z}$ on jaollinen luvulla 3, niin myös $k^2 + k$ on jaollinen luvulla 3: Koska $3 \mid k$, niin on $l \in \mathbb{Z}$, jolle $k = 3l$. Nyt

$$k^2 + k = k(k + 1) = 3l(3l + 1) = 3m,$$

missä $m = 3l^2 + l \in \mathbb{Z}$. Siten $3 \mid (k^2 + k)$.

15.1 ==========

2.2. **Suurin yhteinen tekijä.**

Määritelmä 2.2.1. Jos luku $d \in \mathbb{Z}$ jakaa kokonaisluvut a ja b, niin d on lukujen a ja b *yhteinen tekijä*. Jos ainakin toinen luvuista a, b on erisuuri kuin nolla, niin lukua

$$\text{syt}(a, b) = \max\{d \in \mathbb{N} : d \mid a \text{ ja } d \mid b\}$$

sanotaan lukujen a ja b *suurimmaksi yhteiseksi tekijäksi* (*the greatest common divisor,* $\gcd(a, b)$).

Huomautus 1. Jos $a, b \in \mathbb{Z}$ ja $a \neq 0$, niin $\text{syt}(a, b)$ on olemassa ja yksikäsitteinen. Miksi?

Perustelu: Merkitään $A = \{d \in \mathbb{N} : d \mid a \text{ ja } d \mid b\}$. Lauseen 2.1.2 (6) perusteella luku 1 on jokaisen kokonaislukuparin yhteinen tekijä, erityisesti $1 \in A$.

Toisaalta, jos $d \in A$, niin Lauseen 2.1.2 (9) nojalla $d \leq |a|$. Vastaavasti, jos $b \neq 0$, niin $d \leq |b|$. Siten jokaisella $d \in A$ pätee

$$d \leq \max\{|a|, |b|\}.$$

Luonnollisten lukujen joukko A on epätyhjä ja ylhäältä rajoitettu, joten siinä on suurin alkio, $\text{syt}(a, b)$.

Huomaa, että jos olisi $a = b = 0$, niin Lauseen 2.1.2 (7) nojalla joukko A yllä olisi $\mathbb{N}$, jossa ei ole suurinta alkiota.

Suurin yhteinen tekijä voidaan määritellä myös kolmelle tai useammalle kokonaisluvulle, joista ainakin yksi on nollasta poikkeava. Tästä lähtien, aina kun kirjoitamme $\text{syt}(a, b)$, niin oletamme, että ainakin toinen luvuista a, b on erisuuri kuin nolla.

Esimerkki 2.2.2.

(a) $\text{syt}(12, 30) = 6$: Luvun 12 positiiviset tekijät ovat $1, 2, 3, 4, 6$ ja luvun 30 $1, 2, 3, 5,$
$6, 10, 15, 30.$

(b) $\text{syt}(n, n + 1) = 1$ kaikilla $n \in \mathbb{N}$: Olkoon $d \in \mathbb{N}$ lukujen n ja $(n + 1)$ jakaja. Lauseen 2.1.2 (3) perusteella d jakaa luvun $n+(-1)(n+1) = -1$. Siten Lauseen 2.1.2 (9) perusteella on oltava $d = 1$. Luvuilla n ja $n+1$ ei siis ole muita positiivisia yhteisiä tekijöitä kuin 1.

Miten kahden kokonaisluvun suurin yhteinen tekijä löydetään? Ensimmäisenä mieleentuleva tapa on molempien lukujen tekijöiden listaaminen ja suurimman yhteisen tekijän etsiminen yhteisten tekijöiden joukosta. Tämä tapa on isoilla luvuilla työläs. Jakoyhtälöön ja seuraavaan lemmaan perustuva *Eukleideen algoritmi* antaa tehokkaamman keinon suurimman yhteisen tekijän löytämiseksi.

Lemma 2.2.3. *Jos* $a, b, q, r \in \mathbb{Z}$ *ja* $a = qb + r$, *niin* $\text{syt}(a, b) = \text{syt}(b, r)$.

Todistus. Lauseen 2.1.2 (3) nojalla jokainen lukujen b ja r yhteinen tekijä jakaa summan $qb + r = a$. Vastaavasti jokainen lukujen a ja b yhteinen tekijä jakaa luvun $a - qb = r$. Pareilla a, b ja b, r on siis samat yhteiset tekijät. Siten on myös $\text{syt}(a, b) = \text{syt}(b, r)$. □

Esimerkki 2.2.4. $\text{syt}(42, 30) = 6$:

$$\begin{aligned} 42 &= 1 \cdot \underline{30} + \boxed{12} \\ \underline{30} &= 2 \cdot \boxed{12} + \underline{\underline{6}} \\ \boxed{12} &= 2 \cdot \underline{\underline{6}}. \end{aligned}$$

2.2.1. *Eukleideen algoritmi.* Olkoot $a, b \in \mathbb{Z}$, $a \neq 0$ tai $b \neq 0$. Merkitään $d = \text{syt}(a, b)$. Jos $a = 0$, niin $d = |b|$ (ja vastaavasti jos $b = 0$, niin $d = |a|$). Voidaan siis olettaa, että $a, b \neq 0$.

20.1 ==========

Koska

$$\text{syt}(a, b) = \text{syt}(-a, b) = \text{syt}(a, -b) = \text{syt}(-a, -b),$$

niin voidaan olettaa, että $a, b \in \mathbb{N}$ ja että $a > b$.

Jakamalla a luvulla b jakoyhtälön (Lause 1.2.1) avulla saadaan luvut $q_1, r_1 \in \mathbb{Z}$, joille

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

Jos $r_1 = 0$, niin $b \mid a$. Tällöin $d = b$ ja voidaan lopettaa.
Jos $r_1 > 0$, niin jaetaan b luvulla r_1. Jakoyhtälö antaa luvut $q_2, r_2 \in \mathbb{Z}$, joille

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

Lemman 2.2.3 nojalla $\text{syt}(a, b) = \text{syt}(b, r_1)$. Siten, jos $r_2 = 0$, niin $d = r_1$; lopetetaan. Jos $r_2 > 0$, jaetaan r_1 luvulla r_2. Jakoyhtälö antaa luvut $q_3, r_3 \in \mathbb{Z}$, joille

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

Jatketaan kuten edellä. Koska jakoyhtälön antamat jakojäännökset r_i ovat ei-negatiisia ja muodostavat aidosti vähenevän jonon,

$$b > r_1 > r_2 > \cdots \geq 0,$$

niin jollain n on oltava $r_n = 0$ (korkeintaan b askelta). Viimeiset kaksi vaihetta ovat

$$\begin{aligned} r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, & 0 < r_{n-1} < r_{n-2}, \\ r_{n-2} &= q_n r_{n-1} + r_n, & r_n = 0. \end{aligned} \tag{2.2.1}$$

Lause 2.2.5 (Eukleideen algoritmi)**.** *Olkoot a, b ja jakojäännökset r_i kuten yllä. Tällöin r_{n-1}, viimeinen positiivinen jakojäännös, on* $\text{syt}(a, b)$.

Todistus. Lemma 2.2.3 sovellettuna ylläoleviin lukujen a, b, r_1, ...,r_{n-3} yhtälöihin kertoo, että

$$d = \text{syt}(a, b) = \text{syt}(b, r_1) = \text{syt}(r_1, r_2) = \cdots = \text{syt}(r_{n-2}, r_{n-1}).$$

Koska yhtälön (2.2.1) perusteella $r_{n-1} \mid r_{n-2}$, niin $\text{syt}(r_{n-2}, r_{n-1}) = r_{n-1}$. Siten $d = r_{n-1}$. □

Eukleideen algoritmin avulla saadaan esitettyä $\text{syt}(a, b)$ lukujen a ja b monikertojen summana (lineaarikombinaationa).

Seuraus 2.2.6 (Bézoutin yhtälö)**.** *Olkoot $a, b \in \mathbb{Z}$, $a \neq 0$. Tällöin on $x, y \in \mathbb{Z}$, joille*

$$\text{syt}(a, b) = xa + yb.$$

Todistus. Jos $a = b$, niin $\text{syt}(a, b) = |a|$. Jos $a > 0$, niin $a = 2a - a = 2a - b$ ($a < 0$ vastaavasti). Voidaan siis olettaa, että $a > b$. Kuten yllä, voidaan lisäksi olettaa, että $a, b \in \mathbb{N}$. (Lukujen a ja b negatiivisuus ei vaikuta suurempaan yhteiseen tekijään, saadussa yhtälössä x ja/tai y kerrotaan tarvittaessa luvulla (-1).)

Jos $b \mid a$, niin $\text{syt}(a, b) = b$ ja $a = kb$ jollain $k \in \mathbb{N}$, $k \geq 2$. Tällöin

$$b = kb - (k-1)b = a - (k-1)b.$$

Jos $b \nmid a$, niin Eukleideen algoritmi "peruuttaen" antaa kertoimet x ja y. □

Esimerkki selventänee asiaa. Ennen sitä kuitenkin vielä toinen seuraus.

Seuraus 2.2.7. *Olkoot $a, b, c \in \mathbb{Z}$ ja $a \neq 0$. Tällöin $c \mid a$ ja $c \mid b$ jos ja vain jos $c \mid \text{syt}(a, b)$.*

Todistus. Harjoitustehtävä (**harjoitus 2**). □

Esimerkki 2.2.8. Lasketaan $\text{syt}(22, 60)$ ja etsitään luvut $x, y \in \mathbb{Z}$, joille $\text{syt}(a, b) = xa + yb$. Eukleideen algoritmilla saadaan

$$\begin{aligned}
60 &= 2 \cdot \underline{22} + \boxed{16} & 16 &= 60 - 2 \cdot 22 \\
\underline{22} &= 1 \cdot \boxed{16} + \underline{\underline{6}} & 6 &= 22 - 16 \\
\boxed{16} &= 2 \cdot \underline{\underline{6}} + 4_* & 4 &= 16 - 2 \cdot 6 \\
\underline{\underline{6}} &= 1 \cdot 4_* + 2_\sharp & 2 &= 6 - 4 \\
4_* &= 2 \cdot 2_\sharp.
\end{aligned}$$

Siten $\text{syt}(22, 60) = 2$. "Peruuttamalla" algoritmissa saadaan

$$\begin{aligned}
2 &= 6 - 4 = 6 - (16 - 2 \cdot 6) = 3 \cdot 6 - 16 = 3(22 - 16) - 16 \\
&= 3 \cdot 22 - 4 \cdot 16 = 3 \cdot 22 - 4(60 - 2 \cdot 22) \\
&= 11 \cdot 22 - 4 \cdot 60.
\end{aligned}$$

Bézoutin yhtälön mukaan lukujen a ja b suurin yhteinen tekijä voidaan siis esittää lukujen a ja b monikertojen summana. Seuraava lause kertoo, että vain luvun $\text{syt}(a, b)$ monikerrat voidaan esittää tällaisena summana.

Lause 2.2.9. *Olkoot $a, b \in \mathbb{Z}$, ($a \neq 0$ tai $b \neq 0$) ja $c \in \mathbb{Z}$. Tällöin*

$$c = ka + lb \quad \textit{jollain } k, l \in \mathbb{Z} \tag{2.2.2}$$

jos ja vain jos $\text{syt}(a, b)$ *jakaa luvun c.*

Todistus. Olkoon $d = \text{syt}(a, b)$. Oletaan ensin, että on $k, l \in \mathbb{Z}$, joille $c = ka+lb$. Koska $d \mid a$ ja $d \mid b$, niin Lauseen 2.1.2 (3) mukaan $d \mid c$.

Jos taas $d \mid c$, niin on $c = md$ jollain $m \in \mathbb{Z}$. Bézoutin yhtälön nojalla on $x, y \in \mathbb{Z}$, joille $d = xa + yb$. Nyt on siis

$$c = md = mxa + myb,$$

missä $mx, my \in \mathbb{Z}$. □

Lauseen 2.2.9 perusteella $\text{syt}(a, b)$ on siis pienin luonnollinen luku, joka voidaan esittää muodossa (2.2.2).

Määritelmä 2.2.10. Jos $a, b \in \mathbb{Z}$ ja $\text{syt}(a, b) = 1$, niin sanotaan, että a ja b ovat *suhteellisia alkulukuja* ja että a ja b ovat *keskenään jaottomia*.

Huomaa, että Lauseen 2.2.9 perusteella luvut $a, b \in \mathbb{Z}$ ovat keskenään jaottomia jos ja vain jos $xa + yb = 1$ jollain $x, y \in \mathbb{Z}$. Huomaa myös, että jos $\text{syt}(a, b) = 1$, niin kaikki kokonaisluvut $c \in \mathbb{Z}$ voidaan esittää summana $c = ka + lb$, $k, l \in \mathbb{Z}$.

Seuraavat jaollisuustulokset pätevät keskenään jaottomille luvuille. Yleisessä tapauksessa Seuraus 2.2.11 ei ole totta (**harjoitus 2**).

Seuraus 2.2.11. *Olkoot $a, b \in \mathbb{Z}$ keskenään jaottomia ja $c \in \mathbb{Z}$. Tällöin*

(1) *Jos $a \mid c$ ja $b \mid c$, niin $ab \mid c$.*
(2) *Jos $a \mid bc$, niin $a \mid c$.*

Todistus. (1): Koska $\text{syt}(a, b) = 1$, niin Bézoutin yhtälön mukaan $xa + yb = 1$ jollain $x, y \in \mathbb{Z}$. Oletuksen nojalla on $k, l \in \mathbb{Z}$, joille $ka = c = lb$. Nyt on

$$c = c(xa + yb) = cxa + cyb = (lb)xa + (ka)yb = ab(lx + ky)$$

ja $lx + ky \in \mathbb{Z}$, joten $ab \mid c$.

(2): Kuten kohdassa (1), saadaan $c = cxa + cyb$ jollain $x, y \in \mathbb{Z}$. Koska $a \mid bc$ ja $a \mid a$, niin Lauseen 2.1.2 (3) nojalla a jakaa summan $cxa + ybc = c$. □

22.1 ==========

2.3. **Lukujen jako alkutekijöihin.**

Määritelmä 2.3.1. Luonnollinen luku $p > 1$ on *alkuluku* (*prime*) jos sen ainoat positiiviset tekijät ovat 1 ja p. Luonnollista lukua $p > 1$, joka ei ole alkuluku, sanotaan *yhdistetyksi luvuksi* (*composite*).

Huomautus 2.

(1) Luku 1 ei ole alkuluku eikä yhdistetty luku.
(2) 2 on ainoa parillinen alkuluku (**Miksi?**) (the only even prime $\rightsquigarrow$ the oddest one)

Muista, että luku $n \in \mathbb{Z}$ on *parillinen*, jos $n = 2k$ jollain $k \in \mathbb{Z}$. Luku n on *pariton*, jos $n = 2k + 1$ jollain $k \in \mathbb{Z}$. Huomaa, että jakoyhtälön perusteella jokainen kokonaisluku $n \in \mathbb{Z}$ on joko muotoa $n = 2k$ tai $n = 2k + 1$, missä $k \in \mathbb{Z}$.

Esimerkki 2.3.2.

(a) 10 esimmäistä alkulukua ovat $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$
(b) Luvulla 24 on (positiiviset) tekijät $1, 2, 3, 4, 6, 8, 12$ ja 24, joten se ei ole alkuluku ($24 = 2^3 \cdot 3$).

Tavoitteena on todistaa seuraava lause:

Lause 2.3.3 (Aritmetiikan peruslause)**.** *Jokainen luonnollinen luku $n \geq 2$ voidaan esittää alkulukujen tulona. Tämä esitys on tekijöiden järjestystä vaille yksikäsitteinen.*

Todistetaan ensin alkulukutekijäesityksen olemassaolo-osa.

Lemma 2.3.4. *Olkoon $n \geq 2$ luonnollinen luku. Tällöin n on alkuluku tai alkulukujen tulo.*

Todistus. Todistetaan väite induktiolla. (Koska väite koskee lukua 2 suurempia luonnollisia lukuja, niin induktiotodistuksen ensimmäisessä vaiheessa tarkastetaan, että väite on totta luvulle $n = 2$.)

(1) Koska 2 on alkuluku, niin väite on totta kun $n = 2$.
(2) Olkoon $k \in \mathbb{N}$, $k \geq 2$. Oletetaan, väite on totta luvuille $2, \ldots, k$. Pitää näyttää, että väite on totta luvulle $k + 1$. Jos $k + 1$ on alkuluku, niin väite on totta. Jos $k+1$ ei ole alkuluku, niin sillä on positiivinen tekijä $d \in \mathbb{N}$, $d \neq 1$, $d \neq (k + 1)$. Siten on

$$k + 1 = md \quad \text{jollain } m \in \mathbb{N}.$$

Lauseen 2.1.2 (9) ja tietojen $d \neq 1$, $d \neq (k + 1)$ perusteella on $m < k + 1$ ja $d < k + 1$. Koska $m, d \in \mathbb{N}$, niin $m \leq k$ ja $d \leq k$. Induktio-oletuksen nojalla m ja d voidaan esittää alkulukujen tulona (tai ne ovat alkulukuja). Siten myös $k + 1$ on alkulukujen tulo.

Induktioperiaatteen nojalla väite on totta kaikille $n \in \mathbb{N}$, $n \geq 2$. □

Onko alkulukuesityksen yksikäsitteisyys selvä asia? Tarkastellaan esimerkkejä.

Esimerkki 2.3.5. Esitetään luku 120 alkulukujen tulona:

$$120 = 10 \cdot 12 = (2 \cdot 5) \cdot (3 \cdot 4) = (2 \cdot 5) \cdot (3 \cdot 2 \cdot 2) = 2^3 \cdot 3 \cdot 5.$$

Jako voitaisiin tehdä myös seuraavasti

$$120 = 3 \cdot 40 = 3 \cdot 5 \cdot 8 = 2^3 \cdot 3 \cdot 5 \text{ tai}$$
$$120 = 6 \cdot 20 = 2 \cdot 3 \cdot 4 \cdot 5 = 2 \cdot 3 \cdot 2 \cdot 2 \cdot 5 = 2^3 \cdot 3 \cdot 5.$$

Huomaa, että tekijät esiintyvät tavallisesti suuruusjärjestyksessä. Vastaavasti voidaan jakaa mitä tahansa luonnollista lukua kunnes kaikki tekijät ovat alkulukuja (muista Lemma 2.3.4). Voiko kaksi eri jakotapaa johtaa eri tulokseen? Voi, jos tutkitaan vastaavaa esitystä luonnollisten lukujen $\mathbb{N}$ aidossa osajoukossa.

Esimerkki 2.3.6. Olkoon

$$\mathbb{P} = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\} = \{n \in \mathbb{Z} : n \text{ on parillinen}\}.$$

Yhteen-, vähennys- ja kertolasku ovat joukon $\mathbb{P}$ sisäisiä laskutoimituksia. Joukossa $\mathbb{P}$ voidaan määritellään käsitteet tekijä, jaollisuus ja alkuluku samaan tapaan kuin kokonaislukujen joukossa, esim. luku $m \in \mathbb{P}$ jakaa luvun $n \in \mathbb{P}$, jos on $k \in \mathbb{P}$ siten, että $n = km$.

Joukon $\mathbb{P}$ alkulukuja ovat esimerkiksi $2, 6, 10, 14, 18, 26$ ja 30. Nyt

$$180 = 6 \cdot 30 = 10 \cdot 18,$$

missä kaikki tekijät ovat joukon $\mathbb{P}$ alkulukuja.

Lemma 2.3.7 (Eukleideen lemma)**.** *Olkoon p alkuluku ja olkoot $a, b \in \mathbb{Z}$. Jos $p \mid (ab)$, niin $p \mid a$ tai $p \mid b$. Yleisemmin, jos $p \mid (a_1 \cdots a_n)$, missä $a_i \in \mathbb{Z}$ kaikilla $i = 1, \dots, n$, niin $p \mid a_i$ jollain i.*

Todistus. Jos $p \mid a$, niin OK. Jos $p \nmid a$, niin $\text{syt}(a, p) = 1$. (**Miksi?**)

Seurauksen 2.2.11 (2) perusteella $p \mid b$. Yleinen tapaus todistetaan induktiolla (harjoitus). □

Lauseen 2.3.3 todistus, tapa 1. Olkoon $n \in \mathbb{N}$, $n \geq 2$. Lemman 2.3.4 perusteella n on alkuluku tai alkulukujen tulo. Näytetään, että n voidaan esittää yksikäsitteisellä tavalla tulona

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

missä $p_1, \dots p_k$ ovat alkulukuja, $p_i \neq p_j$ kun $i \neq j$ ja $e_i \in \mathbb{N}$ kaikilla $i = 1, \dots k$. Todistetaan esityksen yksikäsitteisyys induktiolla luvun n suhteen.

(1) Koska luku $n = 2$ on alkuluku eikä sitä voi esittää tulona muista alkuluvuista, niin väite on totta kun $n = 2$.

(2) Oletetaan, että esitys on yksikäsitteinen luonnollisilla luvuilla $2, 3, \ldots, n-1$. Pitää näyttää, että tällöin myös luvulla n on yksikäsitteinen esitys. Jos n on alkuluku, niin OK.

Voidaan siis olettaa, että n on yhdistetty luku. Oletetaan, että on alkuluvut p_i, q_j ja luvut $e_i, f_j \in \mathbb{N}$, $i = 1, \ldots, k$, $j = 1, \ldots, s$, joille $p_i \neq p_j$ ja $q_i \neq q_j$ kun $i \neq j$ ja

$$n = p_1^{e_1} \cdots p_k^{e_k} = q_1^{f_1} \cdots q_s^{f_s}. \tag{2.3.1}$$

Koska $p_1 \mid n$, niin Eukleideen lemman perusteella se jakaa jonkin luvuista q_j, $j \in \{1, \ldots, s\}$.

Numeroimalla luvut q_j tarvittaessa uudelleen voidaan olettaa, että $p_1 \mid q_1$. Koska p_1 ja q_1 ovat alkulukuja, niin on $p_1 = q_1$. Jakamalla (2.3.1) p_1:llä saadaan

$$\tfrac{n}{p_1} = p_1^{e_1 - 1} \cdots p_k^{e_k} = q_1^{f_1 - 1} \cdots q_s^{f_s}.$$

Koska $p_1 \geq 2$ alkulukuna, niin on $n/p_1 \leq n - 1$. Induktio-oletuksen mukaan luvulla n/p_1 on (järjestystä vailla) yksikäsitteinen esitys alkulukujen tulona. Järjestämällä tarvittaessa luvut p_i ja q_j suuruusjärjestykseen saadaan, että $k = s$, $p_i = q_i$ ja $e_i = f_i$ kaikilla $i = 1, \ldots, k$.

Siten myös esitys (2.3.1) on yksikäsitteinen. Väite seuraa induktioperiaatteesta. □

Huomautus 3. Äskeisessä todistuksessa käytimme epäyhtälöä:

$$\tfrac{n}{p} \leq \tfrac{n}{2} \leq n - 1,$$

missä p on alkuluku ja $n \in \mathbb{N}$, $n \geq 2$. Todistus on helppo harjoitustehtävä.

27.1. ==========

Määritelmä 2.3.8. Aritmetiikan peruslauseen antamaa luvun $n \in \mathbb{N}$, $n \geq 2$, esitystä

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

missä $p_1 < \cdots < p_k$ ovat alkulukuja ja $e_1, \ldots e_k \in \mathbb{N}$, sanotaan luvun n *alkutekijäesitykseksi*. Luvut p_i, $i = 1, \ldots, k$, ovat luvun n *alku(luku)tekijöitä*.

Huomautus 4. Alkutekijäesityksen yksikäsitteisyys on syy siihen, että lukua 1 ei kutsuta alkuluvuksi.

Alkutekijäesityksen löytäminen isoille luvuille voi olla hankalaa. Seuraava tulos helpottaa tekijöiden löytämistä.

Lemma 2.3.9. *Olkoon $n \in \mathbb{N}$, $n \geq 2$. Luku n on yhdistetty luku jos ja vain jos on alkuluku $p \leq \sqrt{n}$ joka jakaa luvun n.*

Todistus. Jos on sellainen alkuluku p, että $p \mid n$ ja $1 < p \leq \sqrt{n} < n$, niin n on yhdistetty luku.

Oletetaan, että $n \in \mathbb{N}$, $n \geq 2$, on yhdistetty luku. Olkoon p luvun n pienin alkutekijä. Tällöin on $k \in \mathbb{N}$, $k \geq p$, jolle $n = kp$. Nyt

$$n = kp \geq p^2,$$

joten on $p \leq \sqrt{n}$. □

Esimerkki 2.3.10. Etsitään luvun $n = 132$ alkutekijäesitys. Koska n on parillinen, niin se ei ole alkuluku. Koska

$$11^2 = 121 < 132 < 144 = 12^2,$$

niin on $11 < \sqrt{n} < 12$. Siten luvulla 132 on lukua 12 pienempi alkutekijä (mahdolliset tekijät 2, 3, 5, 7, 11). Nyt

$$132 = \begin{cases} 12 \cdot 11 = 2^2 \cdot 3 \cdot 11 \\ 2 \cdot 66 = 2^2 \cdot 33 = 2^2 \cdot 3 \cdot 11. \end{cases}$$

Lauseen 2.3.3 todistus, tapa 2. Olkoon

$$E = \{n \in \mathbb{N} : n \geq 2 \text{ ja } n \text{ voidaan esittää useammalla kuin yhdellä tavalla alkulukujen tulona.}\}$$

Näytetään, että $E = \emptyset$. Jos E on epätyhjä, niin joukossa E on pienin luku n. Olkoon

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_s$$

luvun n kaksi eri esitystä alkulukujen tulona. Jos $p_i \mid q_j$ jollain indeksiparilla i, j, niin on $p_i = q_j$. Tällöin olisi $n/p_i < n$ ja $n/p_i \in E$, mikä on mahdotonta sillä n on joukon E pienin luku. Siten luvut p_i ja q_j ovat eri alkulukuja. (Järjestämällä tarvittaessa uudelleen,) voidaan olettaa, että tekijät p_i ja q_j ovat suuruusjärjestyksessä. Lemman 2.3.9 nojalla $p_1^2 \leq n$ ja $q_1^2 \leq n$. Koska lisäksi $p_1 \neq q_1$ ja $p_1, q_1 \in \mathbb{N}$, niin on $p_1 q_1 < n$.

Luvut p_1 ja q_1 jakavat luvun n, joten Lauseen 2.1.2 (3) nojalla ne jakavat myös luvun

$$m = n - p_1 q_1.$$

Toisaalta, koska $0 < m < n$ ja n on joukon E pienin luku, niin $m \notin E$. Siten m:llä on yksikäsitteinen alkutekijäesitys ja p_1 ja q_1 ovat luvun m alkutekijöitä.

Koska p_1 ja q_1 jakavat luvun m, niin Seurauksen 2.2.11 (1) nojalla $p_1 q_1 \mid m$. Siten Lauseen 2.1.2 (3) perusteella $p_1 q_1$ jakaa erotuksen $m - p_1 q_1 = n$. Lisäksi, koska $p_1 \mid n$, niin Lauseen 2.1.2 (5) nojalla $q_1 \mid (n/p_1)$. Nyt

$$n/p_1 = p_2 \cdots p_k < n$$

on luonnollinen luku, joten sillä on yksikäsitteinen alkutekijäesitys. Siten on oltava $q_1 = p_i$ jollain $i = 2, \ldots, k$. Tämä on ristiriita, sillä luvut p_i ja q_j ovat eri alkulukuja. Siis joukko E on tyhjä. □

Alkutekijäesityksen avulla voidaan helposti todistaa esimerkikisi luvun $\sqrt{2}$ irrationaalisuus. Muista, että luku x on rationaaliluku jos $x = n/m$ jollain $n, m \in \mathbb{Z}$, $m \neq 0$.

Seuraus 2.3.11. *Olkoot $n, a \in \mathbb{N}$. Jos $\sqrt[n]{a}$ on rationaaliluku, niin $\sqrt[n]{a}$ on luonnollinen luku, erityisesti $a = r^n$ jollain $r \in \mathbb{N}$.*

Todistus. Koska $\sqrt[n]{a}$ on positiivinen rationaaliluku, niin on $r, s \in \mathbb{N}$ joille

$$\sqrt[n]{a} = \frac{r}{s}.$$

Voidaan olettaa, että $\text{syt}(r, s) = 1$ (jos ei, niin supistetaan). Näytetään, että $s = 1$. Jos olisi $s > 1$, niin olisi alkuluku p, jolle $p \mid s$. Lauseen 2.1.2 (3) nojalla p jakaisi tulon $as^n = r^n$. Siten Eukleideen lemman perusteella $p \mid r$. Tämä on mahdotonta, sillä $\text{syt}(r, s) = 1$ ja p on alkuluku. On siis $s = 1$ ja siten $\sqrt[n]{a} = r$. □

2.4. **Alkulukujen esiintymistiheydestä.** Tässä luvussa tutkimme, kuinka paljon alkulukuja on ja kuinka ne sijoittuvat luonnollisten lukujen joukkoon.

Lause 2.4.1 (Eukleideen lause)**.** *Alkulukuja on äärettömän monta.*

Todistus. Näytetään, että minkä tahansa äärellisen alkulukujoukon ulkopuolella on alkuluku.

Olkoot $p_1, \ldots, p_n$ alkulukuja. Näytetään, että on alkuluku, joka ei ole mikään luvuista $p_1, \ldots, p_n$. Olkoon

$$N = p_1 \cdots p_n + 1.$$

Nyt $N \in \mathbb{N}$ ja $N > 2$, joten se on Lemman 2.3.4 mukaan joko alkuluku tai alkulukujen tulo. Jos N on alkuluku, niin olemme löytäneet alkuluvun, joka on kaikkia lukuja $p_1, p_2, \ldots, p_n$ aidosti suurempi.

Jos N ei ole alkuluku, niin sillä on alkulukutekijä q. Jos $q = p_i$ jollain i, niin Lauseen 2.1.2 (3) perusteella q jakaisi luvun $N - p_1 \cdots p_n = 1$, mikä on mahdotonta. Siten $q \neq p_i$ kaikilla $i = 1, \ldots, n$. □

Huomautus 5. Jos valitaan luvuiksi p_i n ensimmäistä alkulukua, niin y.o. todistus antaa suurinta lukua p_n isomman alkuluvun.

Huomautus 6. Luku $N = p_1 \cdots p_n + 1$ **ei** välttämättä ole alkuluku. Esimerkiksi jos $p_1 = 3$ ja $p_2 = 5$, niin

$$N = 3 \cdot 5 + 1 = 16 = 2^4.$$

Luvun N alkutekijä 2 on joukkoon $\{p_1, p_2\}$ kuulumaton alkuluku.

29.1. ==========

Huomaa, että jos luku 2 ei ole alkulukujen $p_1, p_2, \ldots p_n$ joukossa, niin tulo $p_1 \cdots p_n$ on pariton (**Harjoitus 3**). Tällöin $N = p_1 \cdots p_n + 1$ on parillinen eikä siten ole alkuluku.

Esimerkki 2.4.2. Lauseen 2.4.1 todistusmenetelmä toimii muissakin tilanteissa. Näytetään seuraavaksi, että muotoa

$$4n + 3, \quad n \in \mathbb{N},$$

olevia alkulukuja on äärettömän monta. Olkoot $p_1, \ldots, p_k$ muotoa $4n+3$ olevia alkulukuja. Määritellään

$$N = 4p_1 \cdots p_k + 3.$$

Luku N on muotoa $4n + 3$. Se ei ole jaollinen millään luvuista p_i, $i = 1, \ldots, k$, eikä luvuilla $2, 3$. (**Miksi?**)

Lauseen 2.3.3 nojalla $N = q_1 \cdots q_s$, missä luvut q_i ovat alkulukuja. Näytetään, että jokin luvun N alkutekijöistä q_i on muotoa $4n + 3$.

Jakoyhtälön perusteella kaikilla $i = 1, \ldots s$ on $n_i, r_i \in \mathbb{Z}$, joille

$$q_i = 4n_i + r_i \text{ ja } 0 \leq r_i \leq 3.$$

Koska N ei ole jaollinen luvulla 2, niin r_i ei voi olla 0 eikä 2. Jos olisi $r_i = 1$ kaikilla $i = 1, \ldots s$, niin N olisi muotoa $4n + 1$ olevien lukujen tulona myös muotoa $4n + 1$ (Harjoitus).

Siten on oltava $q_i = 4n_i + 3$ jollain $i = 1, \ldots s$. Koska luvut $p_1, \ldots p_k$ eivät ole luvun N tekijöitä, niin q_i ei ole mikään luvuista p_i.

Huomaa, että todistus ei toimi, jos yritetään näyttää, että muotoa $4n + 1$ olevia alkulukuja on äärettömän monta. Nimittäin, jos määritellään

$$N = 4p_1 \cdots p_k + 1$$

ja käytetään jakoyhtälöä luvun N alkutekijöihin, niin ei voida päätellä, että jokin tekijöistä olisi muotoa $4n+1$. Esimerkiksi luku $77 = 7 \cdot 11 = 4 \cdot 19 + 1$ on muotoa $4n + 1$, mutta sen alkutekijät $7 = 4 + 3$ ja $11 = 2 \cdot 4 + 3$ ovat muotoa $4n + 3$.

Seuraava tulos on kuitenkin totta (ja todistus vaikea).

Lause 2.4.3 (Dirichlet 1837)**.** *Jos $a, b \in \mathbb{Z}$, $a > 0$ ja $\operatorname{syt}(a, b) = 1$, niin muotoa*

$$p = an + b, \quad n \in \mathbb{N}$$

olevia alkulukuja on äärettömän monta.

Todistus. Ei todisteta. □

Olkoot n ensimmäistä alkulukua $p_1, p_2, \ldots, p_n$. Seuraava tulos antaa karkean ylärajan luvulle p_n.

Seuraus 2.4.4. *Olkoon $n \in \mathbb{N}$. Tällöin $p_n \leq 2^{2^{n-1}}$.*

Todistus. Todistetaan induktiolla luvun n suhteen.
(1) Kun $n = 1$, niin $p_1 = 2 = 2^{2^0}$.
(2) Oletetaan, että arvio on totta luvuille $p_1, \ldots, p_n$. Kuten Lauseen 2.4.1 todistuksessa, huomataan, että luvulla

$$p_1 \cdots p_n + 1$$

on alkutekijä p ja että $p \neq p_i$ kaikilla $i = 1, \ldots, n$. Koska alkuluku p ei ole n:n ensimmäisen alkuluvun joukossa, niin $p_{n+1} \leq p$. Induktio-oletusta ja geometrisen sarjan osasummaa käyttämällä saadaan

$$\begin{aligned} p_{n+1} &\leq p \leq p_1 \cdots p_n + 1 \leq 2^{2^0} \cdot 2^{2^1} \cdots 2^{2^{n-1}} + 1 \\ &= 2^{1+2+4+\cdots+2^{n-1}} + 1 = 2^{2^n-1} + 1 \\ &= \frac{1}{2} \cdot 2^{2^n} + 1 \leq 2^{2^n}. \end{aligned}$$

Siten väite on totta kaikille $n \in \mathbb{N}$. □

Seuraavaksi tarkastelemme luonnollisten lukujen joukossa esiintyviä reikiä alkulujen välillä ja alkulukujen esiintymistiheyttä. Huomataan, että alkulukujen välissä on sekä pieniä, että suuria aukkoja.

Lause 2.4.5. *Kaikille $n \in \mathbb{N}$, $n \geq 2$, on $n-1$ peräkkäistä luonnollista lukua, joista mikään ei ole alkuluku.*

Todistus. Olkoon $n \in \mathbb{N}$, $n \geq 2$. Peräkkäisiä lukuja

$$n! + 2, n! + 3, \ldots, n! + n$$

on $n-1$ kappaletta. Nyt

$$n! + 2 = 2 \cdot 3 \cdots n + 2 = 2(3 \cdots n + 1)$$

on jaollinen luvulla 2,

$$n! + 3 = 2 \cdot 3 \cdots n + 3 = 3(2 \cdot 4 \cdots n + 1)$$

on jaollinen luvulla 3, ja yleisesti

$$n! + i = 2 \cdot 3 \cdots n + i = i(2 \cdots (i-1)(i+1) \cdots n + 1)$$

on jaollinen luvulla i, $i = 2, 3 \ldots, n$. Siten mikään luvuista $n!+2, n!+3, \ldots, n!+n$ ei ole alkuluku. □

Määritelmä 2.4.6. Jos p ja $p+2$ ovat alkulukuja, niin paria $p, p+2$ sanotaan *alkulukukaksosiksi (twin primes)*. Jos p ja $p+4$ ovat alkulukuja, niin paria $p, p+4$ sanotaan *alkulukuserkuksiksi (cousin primes)*.

Esimerkkejä alkulukukaksosista ovat $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$ ja $(29,31)$. Se, onko alkulukukaksosia äärettömän monta, on yksi lukuteorian ratkaisemattomista ongelmista (twin prime conjecture). Suurin löydetty alkulukukaksospari on $2003663613 \cdot 2^{19500} \pm 1$, (tammikuu 2007). Sellaisia alkulukuja p, että luvulla $p+2$ on korkeintaan kaksi alkutekijää, on äärettömän monta.

Lause 2.4.7. *Olkoon p_n n. alkuluku ja k_n, k_n+2 n. alkulukukaksospari. Tällöin lukujen $\frac{1}{p_n}$ muodostaman sarja hajaantuu eli*

$$\sum_{n=1}^{\infty} \frac{1}{p_n} = \infty$$

ja lukujen $\frac{1}{k_n} + \frac{1}{k_n+2}$ *muodostaman sarja suppenee eli*

$$\sum_{n=1}^{\infty} \frac{1}{k_n} + \frac{1}{k_n+2} < \infty.$$

Todistus. Ei todisteta tällä kurssilla. Ensimmäisen väitteen todistus ei ole vaikea, katso esim. [1, Theorem 1.13]. Jälkimmäisen väitteen summaa sanotaan Brunin vakioksi. □

3.2 ==========

Määritellään funktio $\pi : [0, \infty) \to \mathbb{N} \cup \{0\}$,

$$\pi(x) = \sharp\{p : p \text{ on alkuluku, } p \leq x\},$$

missä $\sharp$ tarkoittaa lukumäärää. Annetulle luvulle x, $\pi(x)$ kertoo siis välillä $[0, x]$ olevien alkulukujen lukumäärän (prime counting function). Tällä funktiolla ei ole mitään tekemistä vakion π kanssa.

Esimerkiksi $\pi(1) = 0$, $\pi(2) = 1$, $\pi(7) = 4$ (alkuluvut $2, 3, 5$ ja 7 ovat pienempiä tai yhtäsuuria kuin luku 7) ja $\pi(7, 5) = 4$.

Huomautus 7. Jos p_n on n. alkuluku, niin $\pi(p_n) = n$. Toisaalta $p_{\pi(n)} = n$ jos ja vain jos n on alkuluku.

Jos jaetaan $\pi(x)$ eli alkulukujen määrä välillä $[0, x]$ välin pituudella x, niin saadaan alkulukujen esiintymistiheys tällä välillä.

Esimerkki 2.4.8.

$$\left|\begin{array}{ccccccc} x & 2 & 7 & 25 & 100 & 500 & 5000 \\ \pi(x) & 1 & 4 & 9 & 25 & 95 & 669 \\ \frac{\pi(x)}{x} & 0,5 & \sim 0,57 & 0,36 & 0,25 & 0,19 & \sim 0,13 \end{array}\right|.$$

Huomaa, että

$$\pi(101)/101 = 26/101 \sim 0,257 > 0,25 = \pi(100)/100.$$

Koska alkulukuja on äärettömän monta, niin $\pi(x) \to \infty$ kun $x \to \infty$. Alkulukujen tiheys $\pi(x)/x$ lähestyy nollaa kun x lähestyy ääretöntä. Seuraava lause kertoo, että tiheyden lasku on hidasta; $\pi(x)/x$ lähestyy nollaa yhtä hitaasti kuin $1/\log(x)$.

Lause 2.4.9 (Alkulukulause (prime number theorem))**.**

$$\lim_{x\to\infty} \frac{\frac{\pi(x)}{x}}{\frac{1}{\log(x)}} = \lim_{x\to\infty} \frac{\pi(x)}{x} \log(x) = 1.$$

Todistus. Vaikea. □

2.4.1. *Eratostheneen seula.* Lukua $x > 0$ pienemmät alkuluvut löydetään Eratostheneen seulan avulla seuraavasti:

(1) Kirjoitetaan luonnolliset luvut, jotka ovat pienempiä tai yhtäsuuria kuin x.
(2) Poistetaan ensimmäisen alkuluvun eli luvun 2 monikerrat.
(3) Poistetaan toisen alkuluvun eli luvun 3 monikerrat.
(4) Poistetaan kolmannen alkuluvun eli luvun 5 monikerrat.
(5) Jatketaan ... jäljelle jääneet luvut ovat lukua x pienemmät alkuluvut.

Huomaa, että Lemman 2.3.9 nojalla riittää käydä läpi lukua $\sqrt{x}$ pienemmät alkuluvut.

Esimerkki 2.4.10. Etsitään alkuluvut p, joille $p \leq 37$. Riittää käydä läpi alkuluvut $p \leq 7$, sillä $6^2 = 36 < 37 < 49 = 7^2$.

	2	3	$\boxed{4}$	5	$\boxed{\bar{6}}$	7	$\boxed{8}$	$\bar{9}$	$\boxed{10}$
11	$\boxed{\bar{12}}$	13	$\boxed{14}$	$\bar{15}_*$	$\boxed{16}$	17	$\boxed{\bar{18}}$	19	$\boxed{20_*}$
$\bar{21}$	$\boxed{22}$	23	$\boxed{\bar{24}}$	25_*	$\boxed{26}$	$\bar{27}$	$\boxed{28}$	29	$\boxed{\bar{30}_*}$
31	$\boxed{32}$	$\bar{33}$	$\boxed{34}$	35_*	$\boxed{\bar{36}}$	37			

Seuraavaksi tutustutaan alkulukuja koskeviin ratkaisemattomiin ongelmiin.

2.4.2. *Goldbachin konjektuuri.* Jokainen parillinen kokonaisluku $n \geq 4$ on kahden alkuluvun summa.

- Goldbachin kirje Eulerille 1742.
- $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7$, ...
- Konjektuurin ratkaisusta oli luvattu miljoonan dollarin palkinto 2000-2002, ratkaisua ei kuitenkaan pystytty todistamaan.
- Totta luvuille $n < 12 \cdot 10^{17}$ (2008).

2.4.3. $n^2 + 1$ *konjektuuri.* Muotoa $n^2 + 1$, $n \in \mathbb{N}$, olevia alkulukuja on äärettömän monta.

- $2 = 1^2 + 1$ mutta jos $n > 1$ on pariton, niin $n^2 + 1$ on parillinen eikä siten ole alkuluku.
- Esimerkiksi $2^2 + 1 = 5$, $4^2 + 1 = 17$, $6^2 + 1 = 37$ ja $10^2 + 1 = 101$ ovat alkulukuja mutta $12^2 + 1 = 145 = 5 \cdot 29$ ei ole.

2.4.4. *Fermat'n numerot.* Muotoa

$$F_n = 2^{2^n} + 1, n = 0, 1, 2, \ldots$$

olevia lukuja sanotaan *Fermat'n numeroiksi* ja vastaavaa muotoa olevia alkulukuja *Fermat'n alkuluvuiksi*.

- Fermat'n konjektuuri oli, että F_n on alkuluku kaikilla n. Näin ei kuitenkaan ole. Viisi ensimmäistä lukua $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ ja $F_4 = 65537$ ovat alkulukuja.

- Euler (1732): $F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$.
- Alkutekijäesitys on löydetty luvuille $F_5, \ldots, F_{11}$.
- F_n ei ole alkuluku jos $5 \leq n \leq 32$ (2003).
- $F_m = F_0 \cdot F_1 \cdot F_{m-1} + 2$
- Onko Fermat'n alkulukuja äärettömän monta, entä yhdistettyjä Fermat'n lukuja?

Olipa Fermat'n alkulukuja äärettömän monta tai ei, niin Fermatin lukujen alkutekijöitä on äärettömän monta. Nimittäin,

Lemma 2.4.11. *Jos $n \neq m$, niin* $\operatorname{syt}(F_n, F_m) = 1$.

Todistus. Olkoot $n, k \in \mathbb{N}$ ja olkoon $d = \operatorname{syt}(F_n, F_{n+k})$. Näytetään kohta, että $F_n \mid (F_{n+k} - 2)$. Koska tällöin $d \mid F_n$ ja $F_n \mid (F_{n+k} - 2)$, niin jaollisuuslauseen 2.1.2 nojalla $d \mid (F_{n+k} - 2)$. Koska $d \mid F_{n+k}$, niin d jakaa erotuksen $F_{n+k} - (F_{n+k} - 2) = 2$. On siis oltava $d = 1$ tai $d = 2$. Kaikki Fermat'n luvut ovat parittomia, joten on $d = 1$.

Näytetään nyt, että $F_n \mid (F_{n+k} - 2)$. Merkitsemällä $x = 2^{2^n}$ saadaan

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1,$$

joten $F_n \mid (F_{n+k} - 2)$. □

Huomautus 8. Yllä todistetun tuloksen perusteella mikä tahansa ääretön joukko Fermat'n numeroita antaa äärettömän monta alkulukua. Tämä antaa uuden todistuksen Lauseelle 2.4.1.

Monet pienet alkuluvut ovat muotoa $2^n \pm 1$, esimerkiksi $3, 5, 7, 31$. Potenssin 2^n esiintyminen kaavassa ei ole sattumaa, sillä

Lause 2.4.12. *Olkoot $a, n \in \mathbb{N}$, $a, n \geq 2$, lukuja, joille $a^n - 1$ on alkuluku. Tällöin $a = 2$ ja n on alkuluku.*

Todistus. Näytetään ensin, että $a = 2$. Geometrisen sarjan $(n-1)$. osasumma S_{n-1} suhdeluvulla a on

$$S_{n-1} = \frac{1 - a^n}{1 - a}, \tag{2.4.1}$$

joten $(a-1) \mid a^n - 1$. Koska $a^n - 1$ on alkuluku ja $a \geq 2$, niin on oltava $a = 2$.

Näytetään seuraavaksi, että n on alkuluku. Jos olisi $n = km$ joillain $m, k \in \mathbb{N}$, $m, k > 1$, niin geometrisen sarjan osasumman (2.4.1) avulla saataisiin

$$2^n - 1 = 2^{m^k} - 1 = \big(2^m - 1\big)\big(1 + 2^m + (2^m)^2 + \cdots + (2^m)^{k-1}\big).$$

Luku $2^n - 1$ olisi siis jaollinen luvulla $2^m - 1$. Tämä on mahdotonta, sillä $2^n - 1$ on alkuluku. Luvun n on siis oltava alkuluku. □

Lause 2.4.13. *Olkoot $a, m \in \mathbb{N}$, $a \geq 2$, lukuja, joille $a^m + 1$ on alkuluku. Tällöin a on parillinen ja $m = 2^n$ jollain $n \in \mathbb{N} \cup \{0\}$.*

Todistus. Jos a olisi pariton, niin a^m olisi pariton (**Harjoitus 3**) ja siten a^m+1 olisi parillinen. Koska 2 on ainoa parillinen alkuluku ja $a^m + 1 \geq 3^1 + 1 = 4$, niin luvun a on oltava parillinen.

Jos luvulla m olisi pariton tekijä $k > 1$, niin olisi $m = 2^n k$ jollain kokonaisluvulla $n \geq 0$. Tällöin, kuten Lemman 2.4.11 todistuksessa saadaan

$$\frac{a^m + 1}{a^{2^n} + 1} = \frac{a^{2^n k} + 1}{a^{2^n} + 1} = a^{2^n(k-1)} - a^{2^n(k-2)} + \cdots + 1,$$

eli $(a^{2^n} + 1) \mid (a^m + 1)$. Koska $a^m + 1$ on alkuluku, niin tämä on mahdotonta. Siis luvulla m ei ole parittomia tekijöitä. □

2.4.5. *Mersennen alkuluvut.* Muotoa $2^p - 1$ olevia alkulukuja sanotaan *Mersennen alkuluvuiksi*.

- Lauseen 2.4.12 perusteella $M_p = 2^p - 1$ voi olla alkuluku vain jos p on alkuluku.
- Konjektuuri: Mersennen alkulukuja on äärettömän monta.
- $M_2 = 2^2-1 = 3$, $M_3 = 2^3-1 = 7$, $M_5 = 2^5-1 = 31$, $M_7 = 2^7-1 = 127$ ovat alkulukuja, mutta $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ ei ole
- Muotoa $2^p - 1$ olevien lukujen alkulukutestaukseen on tehokkaita testejä. Siksi suurimmat tunnetut alkuluvut ovat Mersennen alkulukuja.
- $\text{syt}(M_n, M_k) = 1$ kun $n \neq k$.
- Mersennen alkuluvut liittyvät täydellisiin lukuihin.

Määritelmä 2.4.14. Luku $n \in \mathbb{N}$ on *täydellinen (perfect)*, jos se on itseään aidosti pienempien positiivisten tekijöidensä summa. Siis jos $1 = m_1 < m_2 < \cdots < m_k < m_{k+1} = n$ ovat luvun n positiiviset tekijät ja

$$n = 1 + m_2 + \cdots + m_k,$$

niin n on täydellinen.

Esimerkki 2.4.15. Täydellisiä lukuja ovat esimerkiksi

$$\begin{aligned} 6 &= 1 + 2 + 3, \\ 28 &= 1 + 2 + 4 + 7 + 14 \quad \text{ja} \\ 496 &= 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248. \end{aligned}$$

Täydellisten alkulukujen käsite lienee peräisin Pythagoraan koulukunnalta.

Eukleides todisti, että jokaista Mersennen alkulukua kohti on täydellinen luku. Tästä seuraa, että jos Mersennen alkulukuja on äärettömän monta, niin on myös täydellisiä lukuja. Saadaanko näin kaikki täydelliset luvut? Seuraavan lauseen jälkimmäinen kohta on Eulerin tulos (1849).

Lause 2.4.16.

(1) *Jos* $2^p - 1$ *on alkuluku, niin luku* $n = 2^{p-1}(2^p - 1)$ *on täydellinen.*
(2) *Jos luku* n *on parillinen ja täydellinen, niin on Mersennen alkuluku* $2^p - 1$*, jolle* $n = 2^{p-1}(2^p - 1)$.

Todistus. Ei todisteta. □

Onko parittomia täydellisiä lukuja? Vastausta ei tiedetä. Jos on, niin ne ovat suurempia kuin 10^{300}.

3. Kokonaislukujen jaollisuus

Tässä luvussa tarkastellaan jaollisuussääntöjä. Aloitetaan kurssin alussa luvatulla jakoyhtälön eli Lauseen 1.2.1 todistuksella.

Jakoyhtälö: Olkoot $a, b \in \mathbb{Z}$ ja $b \neq 0$. Tällöin on yksikäsitteiset $q, r \in \mathbb{Z}$, joille

$$a = qb + r \quad \text{ja} \quad 0 \leq r < |b|.$$

Todistus.
Olemassaolo: Tutkitaan muotoa $a - qb$, $q \in \mathbb{Z}$, olevia ei-negatiivia kokonaislukuja ja etsitään niistä pienin. Näytetään ensin, että joukko

$$S = \{y \geq 0 : y = a - qb \text{ jollain } q \in \mathbb{Z}\} \subset \mathbb{N} \cup \{0\}.$$

ei ole tyhjä.
Jos $a \geq 0$, niin $a = a - 0 \cdot b \in S$.
Jos $a < 0$ ja $b \geq 1$, niin

$$a - b \cdot a = a(1 - b) \geq 0$$

ja siten $(a - b \cdot a) \in S$.
Jos $a < 0$ ja $b < 1$, niin koska $b \neq 0$ ja $b < 1$, niin on $b \leq -1$ ja siten $(1+b) \leq 0$. Nyt

$$a + b \cdot a = a(1 + b) \geq 0$$

ja siten $(a + b \cdot a) \in S$.

Hyvän järjestyksen periaatteen nojalla joukossa S on pienin luku; olkoon se r. Joukon S määritelmän mukaan on $a = qb + r$ jollain $q \in \mathbb{Z}$.

Halutun esityksen olemassaoloon pitää näyttää vielä, että $r < |b|$. Jos $b > 0$ ja jos olisi $r \geq b$, niin luku

$$a - (q + 1)b = a - qb - b = r - b \geq 0$$

kuuluisi joukkoon S. Toisaalta $r - b < r$, mikä on mahdotonta, sillä r on joukon S pienin luku. Vastaavasti, jos $b < 0$ ja jos olisi $r \geq -b$, niin olisi

$$a - (q - 1)b = a - qb + b = r + b \geq 0$$

ja $r + b < r$. Luku $a - (q - 1)$ olisi siis lukua r pienempi joukon S luku. On siis oltava $r \leq |b|$.

10.2 ==========
Yksikäsitteisyys: Oletetaan, että on $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, $0 \leq r_1, r_2 < |b|$, joille

$$a = q_1 b + r_1 = q_2 b + r_2.$$

Tällöin $(q_1 - q_2)b = r_2 - r_1$ eli $b \mid (r_2 - r_1)$. Jos $q_1 \neq q_2$, niin $|q_1 - q_2| \geq 1$ ja siten $|r_2 - r_1| \geq |b|$. Tämä on mahdotonta, sillä $0 \leq r_1, r_2 \leq |b| - 1$. On siis $q_1 = q_2$ ja siten myös $r_1 = r_2$.

Jakoyhtälön esitys luvulle a on siis olemassa ja yksikäsitteinen. □

3.1. **Jaollisuus kymmenjärjestelmässä.** Muista, että Lauseen 1.3.1 mukaan jokaiselle $n \in \mathbb{N}$ on yksikäsitteiset kokonaisluvut $s \geq 0$ ja $a_0, a_1, \ldots, a_s$, joille

$$n = a_s 10^s + a_{s-1} 10^{s-1} + \cdots + a_1 10 + a_0 = a_s a_{a-1} \ldots a_0, \tag{3.1.1}$$

$0 \leq a_i \leq 9$ kaikilla $i = 0, 1, \ldots, s$ ja $a_s > 0$. Tässä luvussa luvut $a_0, \ldots, a_s$ viittaavat esitykseen (3.1.1).

Jaollisuus luvuilla $2, 5$ ja 10 on helposti pääteltävissä. Koska täysiä kymmeniä sisältävät luvut ovat aina jaollisia luvuilla 2, 5 ja 10, niin jaollisuuden voi päätellä kahdesta viimeisestä numerosta Lauseen 2.1.2 avulla.

Lause 3.1.1 (1. jaollisuuslause)**.** *Olkoon $n \in \mathbb{N}$. Luku n on jaollinen*

(1) *luvulla* 2 *(eli parillinen) jos ja vain jos a_0 on jaollinen luvulla* 2 *eli jos ja vain jos $a_0 \in \{0, 2, 4, 6, 8\}$,*
(2) *luvulla* 5 *jos ja vain jos $a_0 = 0$ tai $a_0 = 5$,*
(3) *luvulla* 10 *jos ja vain jos $a_0 = 0$.*

Todistus. Seuraa helposti Lauseesta 2.1.2. □

Esimerkki 3.1.2.

(1) Luku $78445 = 78440 + 5$ on jaollinen luvulla 5 mutta ei luvulla 2 eikä luvulla 10.
(2) Luku $100008 = 100000 + 8$ on jaollinen luvulla 2 mutta ei luvulla 5 eikä luvulla 10.

Lohkaisuperiaate

Samaan tapaan voidaan johtaa muitakin jaollisuussääntöjä. Tutkittaessa luvun $n \in \mathbb{N}$ jaollisuutta luvulla t, esitetään n summana, jonka ensimmäinen yhteenlaskettava on jaollinen luvulla t:

$$n = l + k, \quad \text{missä } l, k \in \mathbb{N} \text{ ja } t \mid l. \tag{3.1.2}$$

Lukua l sanotaan *lohkaisutermiksi* ja lukua k *kriittiseksi termiksi*. Jaollisuuslauseesta 2.1.2 seuraa, että n on jaollinen luvulla t jos ja vain jos $t \mid k$.

Lohkaisuperiaate (3.1.2) on käyttökelpoinen, jos jaollisuus voidaan selvittää sen avulla helpommin kuin jaettaessa lukua n luvulla t. Jos kriittinen termi on helposti määrättävissä ja se on pieni lukuun n verrattuna, niin lohkaisuperiaatetta kannattaa käyttää. Sopivan lohkaisutermin valinta ja olemassaolo riippuvat luvuista n ja t.

Jos jakaja t on jokin kymmenen potenssien $10, 100, 1000, \ldots$ tekijä, niin lohkaisutermiksi valitaan luvun n vastaavia kymmenen potensseja sisältävä osa.

Esimerkiksi, koska $4 \mid 100$, niin neljällä jaollisuutta tutkittaessa lohkaisutermiksi valitaan luvun n täysiä satoja sisältävä osa $a_s a_{s-1} \dots a_2 00$.

Lause 3.1.3 (2. jaollisuuslause)**.** *Olkoon $n \in \mathbb{N}$. Luku n on jaollinen luvulla 4 jos ja vain jos luku $a_1 a_0$ on jaollinen luvulla 4.*

Esimerkki 3.1.4.

(1) Luvut 123$\underline{44}$ ja 21$\underline{12}$ ovat 4:llä jaollisia.
(2) Luvut 110$\underline{13}$ ja 20$\underline{07}$ eivät ole 4:llä jaollisia.

Lukujen 100 ja 1000 tekijöille saadaan vastaavasti esimerkiksi jaollisuuslauseet:

Lause 3.1.5 (3. jaollisuuslause)**.** *Olkoon $n \in \mathbb{N}$. Luku n on jaollinen luvulla 50 jos ja vain jos $a_1 = 0$ ja $a_0 = 0$ tai $a_1 a_0 = 50$. Luku n on jaollinen luvulla 25 jos ja vain jos $a_1 = 0$ ja $a_0 = 0$ tai $a_1 a_0 \in \{25, 50, 75\}$.*

Lause 3.1.6 (4. jaollisuuslause)**.** *Olkoon $n \in \mathbb{N}$. Luku n on jaollinen luvulla 8 jos ja vain jos luku $a_2 a_1 a_0$ on jaollinen luvulla 8.*

Tarkasteltaessa jaollisuutta luvuilla 3 ja 9 sopiva lohkaisutermi saadaan lukujen $9 = 10 - 1$, $99 = 100 - 1$, $999 = 1000 - 1, \dots$ avulla, sillä nämä luvut ovat jaollisia luvuilla 3 ja 9. Esimerkiksi luvussa

$$\begin{aligned} 2481 &= 2(999 + 1) + 4(99 + 1) + 8(9 + 1) + 1 \\ &= (2 \cdot 999 + 4 \cdot 99 + 8 \cdot 9) + (2 + 4 + 8 + 1) \end{aligned}$$

lohkaisutermi on luvuilla 3 ja 9 jaollisten lukujen summana jaollinen sekä luvulla 3 että luvulla 9, joten kriittinen termi 15 ratkaisee alkuperäisen luvun jaollisuuden. Koska $3 \mid 15$ ja $9 \nmid 15$, niin 2481 on jaollinen luvulla 3 mutta ei luvulla 9.

Huomaa, että yllä kriittinen termi on lohkaisutermin valinnan seurauksena *alkuperäisen luvun numeroiden summa*. Yleisesti, jos

$$n = a_s a_{s-1} \dots a_0 = a_s(10^s - 1 + 1) + \dots + a_1(9 + 1) + a_0,$$

niin lukua

$$a_s + a_{s-1} + \dots + a_0 \tag{3.1.3}$$

sanotaan luvun n *numerosummaksi*. Jos lohkaisutermiksi valitaan luvuilla 3 ja 9 jaollinen summa

$$a_s(10^s - 1) + \dots + a_1 9,$$

niin numerosumma (3.1.3) on kriittinen termi.

Lause 3.1.7 (5. jaollisuuslause)**.** *Olkoon $n \in \mathbb{N}$. Luku n on jaollinen luvulla 3 (9) jos ja vain jos numerosumma* (3.1.3) *on jaollinen luvulla 3 (9).*

Esimerkki 3.1.8.

(1) Luvun 4005 numerosumma on $4+5=9$, joten 4005 on jaollinen luvuilla 3 ja 9 (Lause 3.1.7).
(2) Luvun 12345 numerosumma $1+2+3+4+5=15$ on jaollinen luvulla 3, mutta ei luvulla 9. Siten $3 \mid 12345$ ja $9 \nmid 12345$ (Lause 3.1.7).
(3) Luvut 10550 ja 2300 ovat jaollisia sekä luvulla 50 että luvulla 25. Luku 1205 ei ole jaollinen luvulla 25 eikä luvulla 50 (Lause 3.1.5).
(4) Luvut $4\underline{032}$ ja $1\underline{160}$ ovat jaollisia luvulla 8, mutta $8 \nmid 2111$ (Lause 3.1.6).
(5) Onko lukujen 14105 ja 25055 summa jaollinen luvulla 8? Lauseen 3.1.6 riittää tarkastella summan kolmea viimeistä numeroa eli lukua $105 + 55 = 160$. Koska $160 = 20 \cdot 8$, niin tutkittava summa on jaollinen luvulla 8.

Tutkitaan seuraavaksi jaollisuutta luvulla 11. Lohkaisutermin määrittämistä varten haetaan luvulla 11 jaollisia lukuja, jotka ovat mahdollisimman lähellä kymmenen potensseja $10, 100, 1000, \ldots$

Luvut $11 = 10 + 1$, $99 = 100 - 1$ ja $1001 = 1000 - 1$ ovat jaollisia luvulla 11 ja yleisesti luvut

$$\begin{array}{l} 10^m + 1, \text{ kun } m \text{ on pariton} \\ 10^m - 1, \text{ kun } m \text{ on parillinen} \end{array} \tag{3.1.4}$$

ovat jaollisia luvulla 11. Jaollisuus seuraa kaavasta

$$a^m - b^m = (a-b)(a^{m-1} + a^{m-2}b + \cdots + ab^{m-2} + b^{m-1}), \tag{3.1.5}$$

missä $a, b \in \mathbb{Z}$ ja $m \in \mathbb{N}$ (**Todistus harjoitus**). Luku $a - b$ on siis luvun $a^m - b^m$ tekijä. Valitsemalla kaavassa (3.1.5) $a = 10$ ja $b = -1$, nähdään, että luku

$$10^m - (-1)^m$$

on jaollinen luvulla 11. Koska $(-1)^m = -1$ parittomilla m ja $(-1)^m = 1$ parillisilla m, niin (3.1.4) on totta.

Korvataan luvun n summaesityksessä (3.1.1) 10^m summalla

$$(10^m - (-1)^m) + (-1)^m$$

kaikilla $m = 1, \ldots s$. Lohkaisutermiksi valitaan varmasti luvulla 11 jaollinen osa

$$a_s(10^s - (-1)^s) + \cdots + a_2 99 + a_1 11.$$

Kriittiseksi termiksi jää tällöin

$$a_0 - a_1 + a_2 - \cdots + (-1)^s a_s, \tag{3.1.6}$$

eli alkuperäisen luvun numerot laskettuna yhteen vaihtuvin etumerkein. Summaa (3.1.6) sanotaan luvun n *vuorottelevaksi numerosummaksi*.

12.2 ==========

Esimerkki 3.1.9. Onko luku 6479 jaollinen luvulla 11? Nyt

$$\begin{aligned} 6479 &= 6 \cdot (1001 - 1) + 4 \cdot (99 + 1) + 7 \cdot (11 - 1) + 9 \\ &= (6 \cdot 1001 + 4 \cdot 99 + 7 \cdot 11) + (-6 + 4 - 7 + 9) \end{aligned}$$

ja koska vuorotteleva numerosumma (kriittinen termi) $-6 + 4 - 7 + 9 = 0$ on jaollinen luvulla 11, niin $11 \mid 6479$.

Lause 3.1.10 (6. jaollisuuslause)**.** *Olkoon $n \in \mathbb{N}$. Luku $n \in \mathbb{N}$ on jaollinen luvulla* 11 *jos ja vain jos luku* 11 *jakaa luvun n vuorottelevan numerosumman.*

Esimerkki 3.1.11.

(1) $11 \nmid 641045$ sillä vuorotteleva numerosumma $5-4+0-1+4-6 = -2$ ei ole jaollinen luvulla 11.
(2) $11 \mid 2020909$ sillä vuorotteleva numerosumma $9-0+9-0+2-0+2 = 22$ on jaollinen luvulla 11.

Jaollisuussäännöt eivät aina ole yksinkertaisia. Esimerkiksi luvulla 7 jaollisuudelle ei ole yhtä helppoa sääntöä kuin edellä esitetyt jaollisuuslauseet. Tarkastellaan asiaa esimerkin avulla.

Esimerkki 3.1.12. Onko luku 485 jaollinen luvulla 7?

Lohkaisutermin muodostamista varten kirjoitetaan $10 = 7+3$ ja $100 = 98+2$, missä 7 ja 98 ovat lukuja 10 ja 100 lähimmät luvulla 7 jaolliset luvut. Nyt

$$\begin{aligned} 485 &= 4(98 + 2) + 8(7 + 3) + 5 \\ &= (4 \cdot 98 + 8 \cdot 7) + (2 \cdot 4 + 3 \cdot 8 + 5), \end{aligned}$$

missä kriittinen termi on $2 \cdot 4 + 3 \cdot 8 + 5 = 37$. Koska $7 \nmid 37$, niin 485 ei ole jaollinen luvulla 7.

Yleisesti, jos

$$n = a_2a_1a_0 = a_2 10^2 + a_1 10 + a_0$$

on korkeintaan *kolminumeroinen* luku, niin

$$n = (a_2 98 + a_1 7) + (a_2 2 + a_1 3 + a_0).$$

Kriittistä termiä $a_2 2 + a_1 3 + a_0$ sanotaan 1. *jaksotermiksi*. Korkeintaan kolminumeroinen luku on siis jaollinen luvulla 7 täsmälleen silloin, kun 1. jaksotermi on jaollinen luvulla 7.

Oletetaan seuraavaksi, että $n \in \mathbb{N}$ on korkeintaan kuusinumeroinen. Seitsemällä jaollisen luvun $1001 = 7 \cdot 143$ avulla voidaan lohkaista luvusta n täysiä tuhansia sisältävä, luvulla 7 jaollinen osa. Jäljelle jäävää korkeintaan kolminumeroista lukua käsitellään kuten edellä.

Esimerkki 3.1.13. Onko 648532 jaollinen luvulla 7? Nyt

$$\begin{aligned} 648532 &= 648(1001 - 1) + 5(98 + 2) + 3(7 + 3) + 2 \\ &= \underbrace{(648 \cdot 1001 + 5 \cdot 98 + 3 \cdot 7)}_{\text{1. lohkaisu}} - 648 + \underbrace{(2 \cdot 5 + 3 \cdot 3 + 2)}_{\text{1. jaksotermi}} \end{aligned}$$

ja luvulle -648 (**huomaa etumerkki**) saadaan

$$\begin{aligned} -648 &= -[6(98+2)+4(7+3)+8] \\ &= \underset{\text{2. lohkaisu}}{-(6\cdot 98+4\cdot 7)} \underset{\text{2. jaksotermi}}{-(2\cdot 6+3\cdot 4+8)}\,. \end{aligned}$$

Luvun 648532 kriittinen termi on 1. ja 2. jaksotermin summa

$$(2\cdot 5+3\cdot 3+2)-(2\cdot 6+3\cdot 4+8)=21-32=-11,$$

joka ei ole jaollinen luvulla 7. Siten $7 \nmid 648532$.

Huomautus 9. Numeroryhmää -648 vastaava kriittisen termin osa, 2. jaksotermi, muodostettiin merkkiä vaille samalla tavalla kuin 1. jaksotermi.

Yleisesti: Tutkittaessa luvun $n \in \mathbb{N}$ jaollisuutta luvulla 7, luku n jaetaan oikealta alkaen kolmen numeron ryhmiin $a_2a_1a_0$, $a_5a_4a_3$, ..., (viimeisessä ryhmässä on 1-3 numeroa). Kunkin ryhmän jaksotermi saadaan laskemalla yhteen 2·(vasemmanpuoleinen numero), 3·(keskimmäinen numero) ja oikeanpuolimmainen numero. Tähän summaan liitetään etumerkki $(-1)^{i+1}$, missä i on ryhmän **järjestysnumero oikealta**. Kriittinen termi saadaan laskemalla nämä etumerkilliset jaksotermit yhteen. (Tarkka perustelu induktiolla)

Esimerkki 3.1.14. Luvun 63 104 333 kriittinen termi on

$$(2\cdot 3+3\cdot 3+3)-(2\cdot 1+3\cdot 0+4)+(3\cdot 6+3).=18-6+21=33$$

Koska $7 \nmid 33$, niin $7 \nmid 63104333$.

Samaan tapaan voidaan johtaa jaollisuussääntöjä muissa lukujärjestelmissä, katso esimerkiksi [5]. Kuten kymmenjärjestelmässäkin, on helpointa löytää jaollisuussäännöt kantaluvun k potenssien tekijöille.

4. Kongruenssi

Kongruenssi mahdollistaa jaollisuuteen liittyvien asioiden käsittelyn tavalla, joka muistuttaa yhtälöiden käsittelyä. Kiinnitetylle $n \in \mathbb{N}$, kokonaisluvut korvataan luvulla n jaettaessa jäävällä jakojäännöksellään.

4.1. Kongruenssin määritelmä.

Määritelmä 4.1.1. Olkoon $n \in \mathbb{N}$ ja olkoot $a, b \in \mathbb{Z}$. Luku a on *kongruentti luvun b kanssa modulo n*,

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

jos $n \mid (a-b)$. Jos $n \nmid (a-b)$, niin merkitään $a \not\equiv b \pmod{n}$. Lukua n sanotaan *moduliksi*.

Huomautus 10. Kongruenssin määritelmästä seuraa, että

(1) $a \equiv b \pmod{n} \iff a-b=kn$ jollain $k \in \mathbb{Z} \iff a=b+kn$ jollain $k \in \mathbb{Z}$,

(2) $a \equiv b \pmod{n} \iff$ Luvuilla a ja b on jakajan n suhteen samat jakojäännökset jakoyhtälössä eli on $k, l, r \in \mathbb{Z}$, $0 \leq r < n$, joille $a = kn + r$ ja $b = ln + r$ (**Harjoitus 6**),
(3) jos $a \equiv r \pmod{n}$ ja $0 \leq r < n$, niin luku r on a:n jakojäännös jaettaessa n:llä, *jakojäännös modulo n*.
(4) $a \equiv 0 \pmod{n} \iff n \mid a$.

Esimerkki 4.1.2.

(1) $19 \equiv 7 \pmod{12}$, $1 \equiv -1 \pmod{2}$, $8 \equiv 1 \pmod{7}$,
(2) $n \in \mathbb{Z}$ on parillinen jos ja vain jos $n \equiv 0 \pmod{2}$,
(3) $n \in \mathbb{Z}$ on pariton jos ja vain jos $n \equiv -1 \pmod{2}$,
(4) $a \equiv b \pmod{1}$ kaikilla $a, b \in \mathbb{Z}$,
(5) jos $a \equiv b \pmod{n}$ ja $d \in \mathbb{N}$ on luvun n tekijä, niin $a \equiv b \pmod{d}$ (**Harjoitus 6**)
(6) kello; minuutit modulo 60 ja tunnit modulo 12 tai 24, esimerkiksi $40 + 35 \equiv 15 \pmod{60}$ ja $10 + 5 \equiv 3 \pmod{12}$

Lause 4.1.3. *Kongruenssi on joukon $\mathbb{Z}$ ekvivalenssirelaatio. Siis jos $n \in \mathbb{N}$ ja $a, b, c, d \in \mathbb{Z}$, niin*

(1) $a \equiv a \pmod{n}$ *(refleksiivisyys),*
(2) *jos* $a \equiv b \pmod{n}$, *niin* $b \equiv a \pmod{n}$ *(symmetrisyys),*
(3) *jos* $a \equiv b \pmod{n}$ *ja* $b \equiv c \pmod{n}$, *niin* $a \equiv c \pmod{n}$ *(transitiivisuus).*

Todistus. Kohdat 1-3 seuraavat jaollisuuden ominaisuuksista (jaollisuuslause 2.1.2):

(1) $n \mid 0$,
(2) jos $n \mid (a - b)$, niin $n \mid (b - a)$,
(3) jos $n \mid (a - b)$ ja $n \mid (b - c)$, niin n jakaa luvun $(a - b) + (b - c) = a - c$.

□

Seuraava lause kertoo, kuinka **saman modulin** kongruensseja voidaan laskea yhteen ja kertoa.

Lause 4.1.4 (Laskusäännöt)**.** *Olkoon $n \in \mathbb{N}$ ja olkoot $a, b, c, d, x, z \in \mathbb{Z}$. Tällöin*

(1) *jos* $a \equiv b \pmod{n}$ *ja* $c \equiv d \pmod{n}$, *niin* $ax + cy \equiv bx + dy \pmod{n}$,
(2) *jos* $a \equiv b \pmod{n}$ *ja* $c \equiv d \pmod{n}$, *niin* $ac \equiv bd \pmod{n}$,
(3) *jos* $a \equiv b \pmod{n}$, *niin* $a^m \equiv b^m \pmod{n}$ *kaikilla* $m \in \mathbb{N}$.

Todistus. Jaollisuuslauseen 2.1.2 perusteella saadaan:

(1) Koska $n \mid (a - b)$ ja $n \mid (c - d)$, niin n jakaa luvun

$$x(a - b) + y(c - d) = (ax + cy) - (bx + dy)$$

(2) ja luvun

$$(a-b)c+(c-d)bac-bc+bc-bd=ac-bd.$$

(3) Induktiolla: jos $m=1$, niin OK. Oletetaan, että $a^m \equiv b^m \pmod{n}$. Valitsemalla kohdassa (2) $c=a$ ja $d=b$, saadaan

$$a^m a \equiv b^m b \pmod{n} \text{ eli } a^{m+1} \equiv b^{m+1} \pmod{n}.$$

Induktioperiaatteen nojalla väite on totta kaikilla $m \in \mathbb{N}$.

□

Kongruensseja **ei** yleensä voi jakaa. Esimerkiksi $14 \equiv 8 \pmod 6$, mutta $7 \not\equiv 4 \pmod 6$. Lukua 2 ei siis voi supistaa pois.

Huomautus 11. Lauseesta 4.1.4 seuraa, että

(1) (induktiolla)

$$\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod{n} \quad \text{ja} \quad a_1 a_2 \cdots a_k \equiv b_1 b_2 \cdots b_k \pmod{n}$$

jos $a_i \equiv b_i \pmod{n}$ kaikilla $i = 1, \ldots, k$.

(2) jaettaessa samalla luvulla summan jakojäännös on jakojäännöksien summa ja tulon jakojäännös on jakojäännöksien tulo.

(3) kongruenssin molemmille puolille voi lisätä minkä tahansa kokonaisluvun. Siis jos $a, b, a_0 \in \mathbb{Z}$ ja $n \in \mathbb{N}$, niin $a \equiv b \pmod{n}$ jos ja vain jos $a + a_0 \equiv b + a_0 \pmod{n}$. (Muista refleksiivisyys Lause 4.1.3 (1)).

17.2 ==========

Esimerkki 4.1.5. Koska $2 \equiv 5 \pmod 3$, niin Lauseen 4.1.4 perusteella $2^{100} \equiv 5^{100} \pmod 3$. Edelleen, Lauseista 4.1.3 ja 4.1.4 seuraa, että

$$2^{100} + 5 \equiv 5^{100} + 2 \pmod 3.$$

Seuraava tulos kertoo, miten kongruensseja voi/saa jakaa.

Lause 4.1.6 (Supistussääntö)**.** *Olkoon $n \in \mathbb{N}$ ja olkoot $a, b, c \in \mathbb{Z}$ lukuja, joille $ac \equiv bc \pmod n$. Jos $\text{syt}(n, c) = 1$, niin $a \equiv b \pmod n$. Yleisemmin, jos $d = \text{syt}(n, c)$, niin*

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

Todistus. Todistetaan tapaus $d = 1$. Pitää siis näyttää, että $n \mid (a-b)$. Oletuksen mukaan $ac \equiv bc \pmod n$, joten $n \mid c(a-b)$. Koska $\text{syt}(n, c) = 1$, niin Seurauksen 2.2.11 perusteella $n \mid (a-b)$. On siis $a \equiv b \pmod n$. □

Lauseen 4.1.3 perusteella kongruenssi on ekvivalenssirelaatio joukossa $\mathbb{Z}$. Ekvivalenssirelaatio jakaa joukon $\mathbb{Z}$ erillisiin ekvivalenssiluokkiin, joita kongruenssin tapauksessa kutsutaan kongruenssiluokiksi.

Määritelmä 4.1.7. Olkoon $n \in \mathbb{N}$ ja olkoon $a \in \mathbb{Z}$. Joukko

$$[a] = [a]_n = \big\{b \in \mathbb{Z} : a \equiv b \pmod{n}\big\}$$

on luvun a *määräämä kongruenssiluokka modulo* n.

Luokka $[a]_n$ koostuu siis muotoa $a + kn$, $k \in \mathbb{Z}$, olevista kokonaisluvuista, esimerkiksi

$$[\,4\,]_3 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}.$$

Lemma 4.1.8. *Olkoon $n \in \mathbb{N}$ ja olkkot $a, b \in \mathbb{Z}$. Tällöin*

(1) $a \in [a]_n$,
(2) $a \equiv b \pmod{n}$ *jos ja vain jos* $[a]_n = [\,b\,]_n$,
(3) *joko* $[a]_n = [\,b\,]_n$ *tai* $[a]_n \cap [\,b\,]_n = \emptyset$.

Todistus.

(1) Lause 4.1.3 (1).
(2) Kongruenssiluokan määritelmä ja Lause 4.1.3 (2)-(3).
(3) Riittää näyttää, että jos $[a]_n \cap [\,b\,]_n \neq \emptyset$, niin $[a]_n = [\,b\,]_n$. Oletetaan, että on $c \in [a]_n \cap [\,b\,]_n$ eli $a \equiv c \pmod{n}$ ja $b \equiv c \pmod{n}$. Lauseen 4.1.3 (2)-(3) perusteella on $a \equiv b \pmod{n}$. Väite seuraa kohdasta (2).

□

Seuraava lause kertoo, että jokainen kongruenssiluokka vastaa yhtä luvulla n jaettaessa jäävää jakojäännöstä $0, 1, \ldots, n-1$.

Lause 4.1.9. *Olkoon $n \in \mathbb{N}$. Kongruenssiluokat $[\,0\,]_n, [\,1\,]_n, \ldots, [n-1]_n$ ovat erillisiä ja niiden yhdiste on $\mathbb{Z}$. Toisin sanoen, jokainen kokonaisluku on kongruentti modulo n täsmälleen yhden kokonaisluvun $0, 1, \ldots n-1$ kanssa.*

Todistus. Huomataan ensin, että mitkään kaksi luvuista $0, 1, \ldots, n-1$ eivät ole kongruentteja keskenään (**Harjoitus 6**). Siten Lemman 4.1.8 nojalla kongruenssiluokat $[\,0\,]_n, [\,1\,]_n, \ldots, [n-1]_n$ ovat erillisiä.

Jos $k \in \mathbb{Z}$, niin jakoyhtälön nojalla on luvut $q, r \in \mathbb{Z}$, joille $k = qn + r$ ja $0 \leq r \leq n-1$. Siten $k \equiv r \pmod{n}$ ja $k \in [r]_n$.

Koska toisaalta jokainen kongruenssiluokka $[\,i\,]_n$, $i = 0, 1, \ldots, n-1$, on joukon $\mathbb{Z}$ osajoukko, niin

$$\mathbb{Z} = \bigcup_{i=0}^{n-1} [\,i\,]_n.$$

□

Usein merkitään

$$\mathbb{Z}_n = \big\{[\,i\,]_n : i = 0, 1 \ldots, n-1\big\} = \big\{[\,i\,]_n : i \in \mathbb{Z}\big\}$$

ja kutsutaan joukkoa $\mathbb{Z}_n$ *kokonaisluvuiksi modulo* n.

Esimerkki 4.1.10. Koska kaikki kokonaisluvut ovat kongruentteja keskenään modulo 1, niin kongruenssiluokkia modulo 1 on vain yksi; $\mathbb{Z}_1 = [0]_1 = \mathbb{Z}$.

Kongruenssiluokkia modulo 2 on kaksi ja $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$. Luokista $[0]_2$ ja $[1]_2$ edellinen koostuu parillisista ja jälkimmäinen parittomista luvuista.

Kongruenssiluokilla voidaan laskea yhteen-, vähennys- ja kertolaskuja.

Määritelmä 4.1.11. Olkoon $n \in \mathbb{N}$ ja olkoot $a, b \in \mathbb{Z}$. Määritellään laskutoimitukset joukossa $\mathbb{Z}_n$ seuraavasti

$$\begin{aligned} [a]_n + [\,b\,]_n &= [a+b]_n, \\ [a]_n - [\,b\,]_n &= [a-b]_n, \\ [a]_n [\,b\,]_n &= [ab]_n. \end{aligned} \tag{4.1.1}$$

Jotta laskutoimitukset olisivat hyvin määriteltyjä, kohdan (4.1.1) kaavojen oikeat puolet saavat riippua vain eksivalenssiluokista $[a]_n$ ja $[\,b\,]_n$, eivät eksivalenssiluokkien edustajista a ja b.

Näytetään, että yhteenlasku on hyvin määritelty: Pitää näyttää, että jos on $a^*, b^* \in \mathbb{Z}$, joille $[a]_n = [a^*]_n$ ja $[\,b\,]_n = [b^*]_n$, niin $[a+b]_n = [a^*+b^*]_n$. Lemman 4.1.8 (2) nojalla on $a \equiv a^* \pmod{n}$ ja $b \equiv b^* \pmod{n}$, joten Lauseen 4.1.4 (1) perusteella on $a + b \equiv a^* + b^* \pmod{n}$. Lemma 4.1.8 (2) toiseen suuntaan kertoo, että $[a+b]_n = [a^*+b^*]_n$.

Esimerkki 4.1.12. Esimerkkejä kongruessiluokkien yhteen- ja kertolaskusta:

$$\begin{aligned} [\,1\,]_3 + [\,2\,]_3 &= [1+2]_3 = [\,3\,]_3 = [\,0\,]_3 \\ [\,2\,]_5 [\,4\,]_5 &= [\,2 \cdot 4\,]_5 = [\,8\,]_5 = [\,3\,]_5 \end{aligned}$$

19.2. ==========

Esimerkki 4.1.13. Olkoon $n \in \mathbb{N}$, olkoot $a, b \in \mathbb{Z}$ ja olkoon P kokonaislukukertoiminen polynomi,

$$P(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_k x^k, \quad c_0, c_1, \ldots, c_k \in \mathbb{Z}.$$

Jos $a \equiv b \pmod{n}$, niin $P(a) \equiv P(b) \pmod{n}$.

Perustelu: Koska $a \equiv b \pmod{n}$, niin Lauseen 4.1.4 (ja Huomatuksen 11) perusteella $a^i \equiv b^i \pmod{n}$ kaikilla $i \in \mathbb{N}$. Edelleen, Lauseesta 4.1.4 seuraa, että $c_i a^i \equiv c_i b^i \pmod{n}$ kaikilla i ja että $\sum_{i=0}^{k} c_i a^i \equiv \sum_{i=0}^{k} c_i b^i \pmod{n}$. Siten $P(a) \equiv P(b) \pmod{n}$.

Jos kokonaislukukertoimisella polynomilla P on juuri $a \in \mathbb{Z}$, niin $P(a) \equiv 0 \pmod{n}$ kaikilla $n \in \mathbb{N}$. Edellisestä esimerkin avulla voidaan joskus päätetellä, että polynomilla ei ole kokonaislukujuuria: jos yhtälöllä $P(x) \equiv 0 \pmod{n}$ ei ole ratkaisua, niin polynomilla P ei ole juuria.

4.2. **Jaollisuussääntöjä kongruenssien avulla.** Edellisessä luvussa johdettuja jaollisuussääntöjä voidaan todistaa kätevästi myös kongruenssien avulla. Onko luku $n \in \mathbb{N}$,

$$n = a_s 10^s + a_{s-1} 10^{s-1} + \cdots + a_1 10 + a_0,$$

jaollinen luvulla $t \in \mathbb{N}$?

Esimerkki 4.2.1. Kolmella jaollisuus perustellaan seuraavasti: Koska $10 \equiv 1 \pmod 3$, niin Lauseen 4.1.4 (3) perusteella $10^k \equiv 1 \pmod 3$ kaikilla $k \in \mathbb{N}$. Koska Lauseen 4.1.4 ja Huomautuksen 11 perusteella on

$$a_s 10^s + \cdots + a_1 10 + a_0 \equiv a_s + \cdots + a_1 + a_0 \pmod 3,$$

niin n on jaollinen luvulla 3 jos ja vain jos sen numerosumma on jaollinen luvulla 3. Vastaava perustelu toimii luvulla 9 jaollisuudelle.

Esimerkki 4.2.2. Neljällä jaollisuus: Koska $10^k \equiv 0 \pmod 4$ kaikilla $k \in \mathbb{N}$, $k \geq 2$, niin Lauseen 4.1.4 ja Huomautuksen 11 perusteella on

$$a_s 10^s + \cdots + a_2 10^2 + a_1 a_0 \equiv (a_s + \cdots + a_2) \cdot 0 + (a_1 a_0) \pmod 4,$$

eli $n \equiv a_1 a_0 \pmod 4$. Siten $4 \mid n$ jos ja vain jos 4 jakaa luvun $a_1 a_0$.

Toisaalta koska $10 \equiv 2 \pmod 4$, niin

$$a_s 10^s + \cdots + a_1 10 + a_0 \equiv (a_s + \cdots + a_2) \cdot 0 + (a_1 2 + a_0) \pmod 4,$$

eli $n \equiv 2a_1 + a_0 \pmod 4$. Siten $n \mid 4$ jos ja vain jos 4 jakaa luvun $2a_1 + a_0$. Näin saatiin toinen sääntö luvulla 4 jaollisuudelle.

4.3. **Lineaarinen kongruenssi.** Olkoon $n \in \mathbb{N}$ ja olkoot $a, b \in \mathbb{Z}$. Kongruenssia

$$ax \equiv b \pmod n \tag{4.3.1}$$

sanotaan (yhden muuttujan) *lineaariseksi kongruenssiyhtälöksi*. Lukua $\boxed{x \in \mathbb{Z}}$ joka toteuttaa yhtälön (4.3.1) sanotaan kongruenssiyhtälön *ratkaisuksi*.

Esimerkki 4.3.1. Tarkastellaan lineaarista kongruenssiyhtälöä

(1) $2x \equiv 6 \pmod{12}$.
Etsitään siis kokonaislukuja x, joille $12 \mid (2x - 6)$. Ainakin luvut $x = 3$ ja $x = 9$ ovat ratkaisuja. Onko muita?
Esimerkiksi $x = 15$ on ratkaisu, mutta koska $15 \equiv 3 \pmod{12}$, niin se on kongruenssimielessä sama ratkaisu kuin 3.

(2) $2x \equiv 3 \pmod 4$.
Etsitään kokonaislukuja x, joille $4 \mid (2x - 3)$.
Koska $2x - 3 = 2x - 3 - 1 + 1 = 2x - 4 + 1 = 2(x - 2) + 1$ on pariton kaikilla $x \in \mathbb{Z}$, niin kongruenssiyhtälöllä ei ole ratkaisua.

Huomautus 12.

(1) Jos $c \in \mathbb{Z}$, niin **joko kongruenssiluokan** $[\,c\,]_n$ **kaikki luvut** ovat lineaarisen kongruenssiyhtälön (4.3.1) ratkaisuja **tai mikään luvuista** $x \in [\,c\,]_n$ **ei** ole ratkaisu.
(2) Koska jokaisen luvun $x \in \mathbb{Z}$ jakojäännökselle r modulo n pätee $x \equiv r \pmod{n}$, niin yhtälöön (4.3.1) ratkaisua haettaessa riittää kohdan (1) perusteella tutkia luvut $0, 1, \ldots, n-1$.

Esimerkin 4.3.1(1) ratkaisuja ovat siis $[\,3\,]_{12}$ ja $[\,9\,]_{12}$. Se, että yhtälöllä (2) ei ole ratkaisuja, voitaisiin perustella myös tarkistamalla, että mikään luvuista $0, 1, 2, 3$ ei ole yhtälön ratkaisu.

Milloin lineaarisella kongruenssiyhtälöllä on ratkaisu? Tarkastellaan asiaa esimerkin avulla.

Esimerkki 4.3.2. Etsi yhtälön $18x \equiv 8 \pmod{22}$ ratkaisut. Jakojäännöksien $0, 1, \ldots, 21$ testaaminen on iso urakka. Haetaan lukuja $x \in \mathbb{Z}$, jolle $18x - 8 = 22y$ jollain $y \in \mathbb{Z}$ eli etsitään lineaarisen yhtälön

$$18x - 22y = 8$$

kokonaislukuratkaisuja. Bézoutin yhtälön nojalla on $k, l \in \mathbb{Z}$, joille

$$18k - 22l = \operatorname{syt}(18, 22) = 2. \tag{4.3.2}$$

Luvut $k, l \in \mathbb{Z}$ saadaan Eukleideen algoritmista tai keksimällä; tässä $k = 5$ ja $l = 4$ kelpaavat. Kertomalla yhtälö (4.3.2) puolittain luvulla 4 saadaan

$$18 \cdot 5 \cdot 4 - 22 \cdot 4 \cdot 4 = 8,$$

joten $18 \cdot 20 \equiv 8 \pmod{22}$. Siten $x \equiv 20 \pmod{22}$ on alkuperäisen kongruenssiyhtälön ratkaisu. Kokeilemalla huomataan, että myös $x \equiv 9 \pmod{22}$ on ratkaisu ($18 \cdot 9 - 8 = 162 - 8 = 154 = 7 \cdot 22$).

24.2 ==========

Yleisesti saadaan

Lause 4.3.3 (Lineaarisen kongruenssin lause)**.** *Olkoon $n \in \mathbb{N}$, olkoot $a, b \in \mathbb{Z}$ ja $d = \operatorname{syt}(a, n)$.*

(1) *Jos $d \nmid b$, niin lineaarisella kongruenssilla $ax \equiv b \pmod{n}$ ei ole ratkaisua $x \in \mathbb{Z}$.*
(2) *Jos $d \mid b$, niin lineaarisella kongruenssilla $ax \equiv b \pmod{n}$ on d ratkaisua (kongruenssiluokkaa modulo n). Ratkaisut saadaan seuraavasti: haetaan $k_0, l_0 \in \mathbb{Z}$, joille $ak_0 + nl_0 = d$. Tällöin*

$$x_0 = \frac{b}{d}\, k_0 \tag{4.3.3}$$

on yhtälön $ax \equiv b \pmod{n}$ ratkaisu. Kaikki ratkaisut saadaan kaavalla

$$x \equiv x_0 + i\,\frac{n}{d} \pmod{n}, \quad i = 0, 1, \ldots, d-1.$$

Todistus. Todistetaan väite (1). Jos $x \in \mathbb{Z}$ olisi yhtälön $ax \equiv b \pmod{n}$ ratkaisu, niin olisi $ax - b = ny$ jollain $y \in \mathbb{Z}$. Koska $d \mid a$ ja $d \mid n$, niin d jakaisi luvun $ax - ny = b$. Tämä on mahdotonta, sillä $d \nmid b$. Siis kongruenssiyhtälöllä $ax \equiv b \pmod{n}$ ei ole ratkaisua.

Kohdasta (2) todistetaan vain, että (4.3.3) on ratkaisu. Todistuksen loppu on harjoitustehtävä. Bézoutin yhtälön nojalla on $k_0, l_0 \in \mathbb{Z}$, joille

$$ak_0 + nl_0 = d.$$

Kertomalla tämä yhtälö puolittain luvulla $b/d \in \mathbb{Z}$ saadaan

$$a\,\frac{b}{d}\,k_0 + n\,\frac{b}{d}\,l_0 = b,$$

missä $\frac{k_0 b}{d}, \frac{l_0 b}{d} \in \mathbb{Z}$. Siten $x_0 \equiv \frac{k_0 b}{d} \pmod{n}$ on ratkaisu. □

Seuraus 4.3.4. *Jos $n \in \mathbb{N}$, $a \in \mathbb{Z}$ ja $\operatorname{syt}(a, n)=1$, niin lineaarisella kongruenssilla $ax \equiv b \pmod{n}$ on ratkaisu kaikilla $b \in \mathbb{Z}$. Ratkaisu on yksikäsitteinen kongruenssiluokkana.*

Todistus. Lause 4.3.3. □

Esimerkki 4.3.5. Ratkaise yhtälö

(1) $10x \equiv 6 \pmod{12}$
Koska $\operatorname{syt}(10, 12) = 2$ ja $2 \mid 6$, niin Lauseen 4.3.3 nojalla yhtälöllä on kaksi ratkaisua. Nyt

$$10 \cdot (-1) + 12 \cdot 1 = 2,$$

joten $x_0 = \frac{6}{2} \cdot (-1) = -3 \equiv 9 \pmod{12}$ on ratkaisu.
Toinen ratkaisu on $x_1 \equiv x_0 + \frac{12}{2} \pmod{n}$ eli $x_1 \equiv 3 \pmod{12}$. Ratkaisut ovat siis kongruenssiluokat $[\,3\,]_{12}$ ja $[\,9\,]_{12}$.

(2) $7x \equiv 3 \pmod{12}$.
Koska $7 \cdot 9 = 63 \equiv 3 \pmod{12}$, niin kongruenssiluokka $[\,9\,]_{12}$ on ratkaisu. Koska $\operatorname{syt}(7, 12) = 1$, niin Lauseen 4.3.3 nojalla tämä on ainoa ratkaisu.

(3) $4x \equiv 5 \pmod{12}$.
Koska $\operatorname{syt}(4, 12) = 4$ ja $4 \nmid 5$, niin ratkaisua ei ole.

Tarkastellaan lopuksi lineaaristen kongruenssiyhtälöiden muodostamia yhtälöryhmiä. Aloitetaan esimerkillä.

Esimerkki 4.3.6. Onko lukua $x \in \mathbb{Z}$, jolle lineaariset kongruenssiyhtälöt

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

ovat totta? Huomaa, että jos $x_0 \in \mathbb{Z}$ on yhtälöryhmän ratkaisu, niin myös luku

$$x_0 + 3 \cdot 5 \cdot 7t$$

on ratkaisu kaikilla $t \in \mathbb{Z}$. Kaikki kongruenssiluokan $[x_0]_{105}$ luvut ovat siis ratkaisuja. Se, että muita ratkaisuja ei ole, seuraa Lauseesta 4.3.8.

Esimerkki 4.3.7. Onko lukua $x \in \mathbb{Z}$, jolle lineaariset kongruenssiyhtälöt

$$x \equiv 3 \pmod 9 \quad \text{ja} \quad x \equiv 2 \pmod 6$$

ovat totta?

Jos $x \equiv 3 \pmod 9$, niin $3 \mid (x-3)$ ja siten 3 jakaa luvun $x - 3 + 3 = x$. Jos $x \equiv 2 \pmod 6$, niin $3 \mid (x-2)$. Jos $3 \mid x$, niin 3 jakaisi luvun $x - (x-2) = 2$, mikä ei ole totta. Siis $3 \nmid x$, eikä yhtälöillä ole yhteistä ratkaisua.

Lause 4.3.8 (Kiinalainen jäännöslause)**.** *Olkoot $n_1, \ldots, n_k \in \mathbb{N}$ lukuja, joille* $\text{syt}(n_i, n_j) = 1$ *aina, kun $i \neq j$. Olkoot $b_1, \ldots, b_k \in \mathbb{Z}$. Tällöin kongruenssiyhtälöryhmällä*

$$x \equiv b_1 \pmod{n_1}, \quad x \equiv b_2 \pmod{n_2} \quad \textit{ja} \quad x \equiv b_k \pmod{n_k}$$

on yksikäsitteinen ratkaisu kongruenssiluokkana modulo n, $n = n_1 \cdots n_k$.

Todistus. Olkoon

$$c_i = \frac{n}{n_i}, \quad i = 1, 2, \ldots, k.$$

Koska $\text{syt}(n_i, n_j) = 1$ aina, kun $i \neq j$, niin $\text{syt}(c_i, n_i) = 1$ kaikilla $i = 1, 2, \ldots, k$. Seurauksen 4.3.4 perusteella yhtälöllä

$$c_i x \equiv 1 \pmod{n_i}$$

on yksikäsitteinen ratkaisu kongruenssiluokkana modulo n_i. Olkoon se $[d_i]_{n_i}$

Näytetään, että luku

$$x_0 = b_1 c_1 d_1 + b_2 c_2 d_2 + \cdots + b_k c_k d_k$$

on yhtälöryhmän ratkaisu.

Jos $i \neq j$, niin $n_i \mid c_j$ ja siten $b_j c_j d_j \equiv 0 \pmod{n_i}$. Luvun x_0 määritelmän mukaan on siis $x_0 \equiv b_i c_i d_i \pmod{n_i}$. Koska $c_i d_i \equiv 1 \pmod{n_i}$, niin on

$$x_0 \equiv b_i \pmod{n_i}$$

eli x_0 on kaikkien ryhmän kongruenssiyhtälöiden ratkaisu. Jaollisuuslauseen avulla nähdään helposti, että kongruenssiluokka $[x_0]_n$ on yhtälöryhmän ratkaisu.

Näytetään seuraavaksi, että muita ratkaisuja ei ole. Olkoon $x \in \mathbb{Z}$ yhtälöryhmän ratkaisu. Koska tällöin on $x \equiv b_i \pmod{n_i}$ ja $x_0 \equiv b_i \pmod{n_i}$, niin Lauseen 4.1.3 perusteella $x_0 \equiv x \pmod{n_i}$ ja siten $n_i \mid (x - x_0)$ kaikilla $i = 1, 2, \ldots, k$. Koska $\text{syt}(n_i, n_j) = 1$, niin Seurauksen 2.2.11 perusteella luku $n = n_1 \cdots n_k$ jakaa luvun $x - x_0$ eli $x \equiv x_0 \pmod{n}$. Siis ainoa ratkaisu on $[x_0]_n$. □

Esimerkki 4.3.9. Luku $x = 23$ toteuttaa Esimerkin 4.3.6 lineaariset kongruenssiyhtälöt. Kiinalaisen jäännöslauseen perusteella kongruenssiluokka $[23]_{105}$ on yhtälöryhmän yksikäsitteinen ratkaisu.

Viitteet

[1] Apostol, T.M.: *Introduction to analytic number theory* - Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[2] Hardy, G.H. ja Wright, E.M.: *An Introduction to the Theory of Numbers* - Oxford University Press, London

[3] Jones, G.A. ja Jones, J.M.: *Elementary number theory* - Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 1998.

[4] Järvenpää, M.: *Lukuteorian alkeet* - luennot 2005, Jyväskylän yliopisto.

[5] Nevanlinna, V.: *Lukuteorian alkeet* - Luentomoniste 8, Jyväskylän yliopisto, 2004

[6] Redmond, D.: *Number theory. An introduction* - Monographs and Textbooks in Pure and Applied Mathematics, 201. Marcel Dekker, Inc., New York, 1996.

[7] Silverman, J.H.: *A Friendly Introduction to Number Theory* - Pearson Prentice Hall, 2006.

Matematiikan ja tilastotieteen laitos, PL 35, 40014 Jyväskylän yliopisto
E-mail address: heli.m.tuominen@jyu.fi