TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Sini Siira

Lukuteorian kurssi lukioon

Informaatiotieteiden yksikkö
Matematiikka
Huhtikuu 2015

Tampereen yliopisto
Informaatiotieteiden yksikkö
SIIRA, SINI: Lukuteorian kurssi lukioon
Pro gradu -tutkielma, 59 s.
Matematiikka
Huhtikuu 2015

Tiivistelmä

Tämän Pro gradu -tutkielman tarkoituksena on toimia materiaalina lukuteorian kurssiin, joka pohjautuu nykyiseen kurssiin MAA11: Lukuteoria ja logiikka. Tämä materiaali eroaa kurssin MAA11 materiaaleista siinä, että logiikan osuus on jätetty pois. Sen sijaan lukuteorian aiheisiin paneudutaan syvällisemmin, ja loppupuolella esitellään muutama sovellus. Lukuteorian aiheet, kuten jaollisuus, alkuluvut ja kongruenssi, käydään materiaalissa läpi perusteellisesti. Lisäksi materiaalissa käsitellään lukujärjestelmiä sekä kongruenssien sovelluksia, kuten tarkistusnumeroita ja RSA-salausta. Tässä materiaalissa keskeisiä sisältöjä ovat kokonaislukujen jaollisuus ja jakoyhtälö, Eukleideen algoritmi, alkuluvut, aritmetiikan peruslause, kokonaislukujen kongruenssi, jaollisuustestit sekä Fermat'n pieni lause. Tutkielmassa on haluttu korostaa sitä, miten näitä matemaattisia aiheita voidaan käyttää käytännön sovelluksissa. Materiaalista löytyy soveltavia tehtäviä, mutta perustehtävien määrä on vähäinen. Tämän Pro gradu -tutkielman lähteenä on käytetty Kenneth H. Rosenin kirjaa *Elementary Number Theory and its Applications*, sekä Lukuteoria ja logiikka -kurssikirjaa sarjoista Pyramidi, Matematiikan taito ja Laudatur.

Asiasanat jaollisuus, alkuluvut, kongruenssi

Sisältö

1 Johdanto

Lukuteoria on, kuten nimi kertoo, lukujen tutkimusta. Ennen Pythagorasta tutkittiin vain kokonaislukuja ja rationaalilukuja. Kun Pythagoras ja hänen opetuslapsensa huomasivat, että yksikköneliön lävistäjä ei voi olla rationaaliluku, he järkyttyivät. He tekivät yhdessä päätöksen, että irrationaalilukujen olemassaolo täytyy pitää salaisuutena kuolemanrangaistuksen uhalla. [1, s. 96]

Lukuteorian ongelmat ovat muuttuneet vuosisatojen kuluessa hankalemmiksi. Fermat'n suuri lause todistettiin vasta 1990-luvulla ja Riemannin hypoteesi on edelleen todistamatta. Fermat'n suuren lauseen mukaan yhtälöllä $x^n + y^n = z^n$ ei ole nollasta eroavia kokonaislukuratkaisuja x, y ja z, kun n on kahta suurempi kokonaisluku. Pierre de Fermat esitti suuren lauseensa jo 1700-luvulla, mutta vasta yli 300 vuotta myöhemmin englantilainen Andrew Wiles laati 150 sivun todistuksen, jonka ymmärtää vain muutama matemaatikko maailmassa. [3, s. 51]

Lukuteoria on matematiikan osa-alue, jolla on paljon käytännön sovelluksia modernissa tietoliikenteessä. Koodausteoria sivuaa lukuteoriaa ja monet salausjärjestelmät ovat puhdasta lukuteoriaa.[1, s. 97]

2 Opetussuunnitelma

Tämän Pro gradu -tutkielman tarkoituksena on toimia materiaalina lukuteorian kurssiin, joka pohjautuu nykyiseen kurssiin MAA11: Lukuteoria ja logiikka. Tämä materiaali eroaa kurssin MAA11 materiaaleista siinä, että tästä materiaalista on jätetty pois logiikan osuus. Sen sijaan lukuteorian aiheisiin paneudutaan syvällisemmin, ja loppupuolella esitellään muutama sovellus.

Vuoden 2003 Lukion opetussuunnitelman perusteista on haluttu korostaa seuraavia tavoitteita: opiskelija

- ymmärtää ja osaa käyttää matematiikan kieltä, kuten seuraamaan matemaattisen tiedon esittämistä, lukemaan matemaattista tekstiä, keskustelemaan matematiikasta, ja oppii arvostamaan esityksen täsmällisyyttä ja perustelujen selkeyttä
- oppii näkemään matemaattisen tiedon loogisena rakenteena
- kehittää lausekkeiden käsittely-, päättely- ja ongelmanratkaisutaitojaan
- harjaantuu käsittelemään tietoa matematiikalle ominaisella tavalla, tottuu tekemään otaksumia, tutkimaan niiden oikeellisuutta ja laatimaan perusteluja sekä arvioimaan perustelujen pätevyyttä ja tulosten yleistettävyyttä.

Kurssin Lukuteoria ja logiikka tavoitteista seuraavat ovat myös tämän lukuteorian kurssin tavoitteita: opiskelija

- oppii todistusperiaatteita ja harjoittelee todistamista
- oppii lukuteorian peruskäsitteet ja perehtyy alkulukujen ominaisuuksiin
- osaa tutkia kokonaislukujen jaollisuutta jakoyhtälön ja kokonaislukujen kongruenssin avulla
- osaa määrittää kokonaislukujen suurimman yhteisen tekijän Eukleideen algoritmilla.

Tässä kurssimateriaalissa ei opeteta todistusperiaatteita erikseen, mutta monien lauseiden todistukset ovat materiaalissa mukana. Materiaalissa on myös paljon todistustehtäviä, jotka on tarkoitus tehdä esimerkkien mukaisesti. Lukuteorian aiheet, kuten jaollisuus, alkuluvut ja kongruenssi, käydään materiaalissa läpi perusteellisesti. Lisäksi materiaalissa käsitellään lukujärjestelmiä sekä kongruenssien sovelluksia, kuten tarkistusnumeroita ja RSA-salausta.

Opetussuunnitelman perusteista poimittuja keskeisiä sisältöjä ovat

- kokonaislukujen jaollisuus ja jakoyhtälö

- Eukleideen algoritmi
- alkuluvut
- aritmetiikan peruslause
- kokonaislukujen kongruenssi.

Tässä materiaalissa edellä mainittujen lisäksi keskeisiä sisältöjä ovat jaollisuustestit sekä Fermat'n pieni lause. Tässä materiaalissa on myös haluttu korostaa sitä, miten näitä matemaattisia aiheita voidaan käyttää käytännön sovelluksissa.

Materiaalista löytyy soveltavia tehtäviä, mutta perustehtävien määrä on vähäinen. Perustehtäviä löytyy lisää Lukuteoria ja logiikka -kurssikirjoista, kuten Pyramidista [1], Matematiikan taidosta [2] ja Laudaturista [3].

3 Jaollisuus

- Voidaanko 57 karkin karkkipussi jakaa tasan a) kahden b) kolmen ihmisen kesken?
- Millä kokonaisluvun a arvoilla jako menee tasan, kun lauseke $a^5 - a$ jaetaan luvulla 5?

3.1 Jaollisuusrelaatio

Määritelmä 3.1: Jaollisuusrelaatio

Olkoot a ja b kokonaislukuja ja $b \neq 0$. Jos on olemassa sellainen kokonaisluku c, että $a = bc$, niin sanotaan, että luku b *jakaa* luvun a ja että b on luvun a *tekijä*. Sanotaan myös, että luku a on *jaollinen* luvulla b. [8, s. 37]

Esimerkki 3.1

Koska $21 = 3 \cdot 7$, niin luku 3 jakaa luvun 21 ja on sen tekijä. Luku 21 on siis jaollinen luvulla 3.

Esimerkki 3.2

Koska ei löydy kokonaislukua k joka toteuttaisi yhtälön $21 = 2k$, niin luku 2 ei ole luvun 21 tekijä, eikä luku 21 ole jaollinen luvulla 2.

Merkintä 3.1

Kun luku b jakaa luvun a, niin $b \mid a$.
Kun luku b ei jaa lukua a, niin $b \nmid a$.

Esimerkki 3.3

- Koska $21 = 3 \cdot 7$, niin $3 \mid 21$ ja $7 \mid 21$.
- Koska luku 21 ei ole jaollinen luvulla 2, niin $2 \nmid 21$.

Esimerkki 3.4

Esimerkkejä jaollisuudesta ovat $10 \mid 2000$, $-20 \mid 100$, $30 \nmid 50$ ja $31 \mid 0$.

3.2 Jaollisuustestit

On muitakin tapoja selvittää, onko luku a jaollinen luvulla b, kuin katsomalla, meneekö jakolasku $a : b$ tasan. Yksi vaihtoehtoinen tapa on käyttää jaollisuustestiä. Jaollisuustestit nopeuttavat suurten lukujen jaollisuuden testaamista.

Lause 3.1: Jaollisuustestit

Kokonaisluku on jaollinen

- luvulla 2, jos ja vain jos sen viimeinen numero on parillinen.
- luvulla 3, jos ja vain jos sen numeroiden summa on jaollinen luvulla 3.
- luvulla 4, jos ja vain jos sen kahden viimeisen numeron muodostama luku on jaollinen luvulla 4.
- luvulla 5, jos ja vain jos sen viimeinen numero on 0 tai 5.
- luvulla 6, jos ja vain jos se on jaollinen luvuilla 2 ja 3.
- luvulla 7, jos luku, josta on poistettu viimeinen numero ja vähennetty viimeinen numero kahdesti, on jaollinen luvulla 7. Tätä voidaan toistaa niin kauan, kunnes luku on niin pieni, että on helppo nähdä onko jäljellä oleva luku jaollinen luvulla 7.
- luvulla 8, jos ja vain jos sen kolmen viimeisen numeron muodostama luku on jaollinen luvulla 8.
- luvulla 9, jos ja vain jos sen numeroiden summa on jaollinen luvulla 9.

Jaollisuustestit todistetaan myöhemmin kappaleessa 7.2.

Esimerkki 3.5

Onko luku 31 265 436 jaollinen luvuilla 2, 3, 4, 5, 6, 7, 8 ja 9?

- On jaollinen luvulla 2, koska viimeinen numero on 6.
- On jaollinen luvulla 3, koska $3+1+2+6+5+4+3+6 = 30$ ja $3 \mid 30$.
- On jaollinen luvulla 4, koska $4 \mid 36$.
- Ei ole jaollinen luvulla 5, koska viimeinen numero on 6.
- On jaollinen luvulla 6, koska on jaollinen luvuilla 2 ja 3.
- Ei ole jaollinen luvulla 7, sillä kun toistetaan jaollisuustestin kaavaa $3126543 - 6 - 6 = 3126531$, $312653 - 1 - 1 = 312651$, $31265 - 1 - 1 = 31263$, $3126 - 3 - 3 = 3120$, $312 - 0 - 0 = 312$, niin lopulta saadaan $31 - 2 - 2 = 27$, ja 27 ei ole jaollinen luvulla 7.
- Ei ole jaollinen luvulla 8, koska $8 \nmid 436$.
- Ei ole jaollinen luvulla 9, koska $9 \nmid 30$.

Esimerkki 3.6

Todista: Kun mistä tahansa kolminumeroisesta luvusta vähennetään luku, joka on alkuperäinen luku käänteisellä numerojärjestyksellä, niin tämä erotus on jaollinen yhdeksällä.

Merkitään alkuperäisen luvun numeroita kirjaimin a, b ja c. Alkuperäinen luku on siis $100a+10b+c$ ja vähennettävä luku on $100c+10b+a$. Nyt erotus

$$\begin{aligned} 100a + 10b + c - (100c + 10b + a) &= 100a - a + 10b - 10b + c - 100c \\ &= 99a - 99c \\ &= 99(a - c) \\ &= 9 \cdot 11(a - c) \\ &= 9t, \end{aligned}$$

missä t on kokonaisluku, koska a ja c ovat kokonaislukuja. Siis erotus on jaollinen yhdeksällä.

3.3 Jaollisuussääntöjä

Lause 3.2: Kokonaislukujen yleisiä jaollisuussääntöjä

Kaikille kokonaisluvuille pätee seuraavat jaollisuussäännöt:

1. $1 \mid a$
2. Jos $a \neq 0$, niin $a \mid a$ ja $a \mid 0$.
3. Jos $a \mid b$ ja $b \mid a$, niin $a = \pm b$.
4. Jos $a \mid b$ ja $b \mid c$, niin $a \mid c$.
5. Jos $a \mid b$, niin $a \mid bk$ kaikilla kokonaisluvuilla k.
6. Jos $a \mid b$ ja $a \mid c$, niin $a \mid (b \pm c)$.
7. Jos $a \mid b$ ja $a \mid c$, niin $a \mid (xb \pm yc)$.

Todistus (vrt. [7, s. 31] ja [3, s. 58]).

1. Koska $a = 1 \cdot a$, niin $1 \mid a$.
2. Väite seuraa suoraan kertolaskuista $a = 1 \cdot a$ ja $0 = 0 \cdot a$.
3. Harjoitustehtävä
4. Koska $a \mid b$ ja $b \mid c$, niin on olemassa sellaiset kokonaisluvut x ja y, joille pätee $ax = b$ ja $by = c$. Nyt siis $c = by = (ax)y = a(xy)$, jolloin pätee $a \mid c$.
5. Koska $a \mid b$, niin on olemassa sellainen kokonaisluku x, jolle pätee $b = ax$. Nyt siis $bk = (ax)k = a(xk)$, joten $a \mid bk$.
6. Koska $a \mid b$ ja $a \mid c$, niin on olemassa sellaiset kokonaisluvut x ja y, joille pätee $b = xa$ ja $c = ya$. Siis $b \pm c = xa \pm ya = (x \pm y)a$.
7. Harjoitustehtävä

□

Esimerkki 3.7

Osoita, että lauseke $n^3 + 3n$ on jaollinen luvulla 2 kaikilla kokonaisluvuilla n.

Jaetaan todistus kahteen osaan sen mukaan, onko n parillinen vai pariton.

Jos n on parillinen, niin se on muotoa $n = 2m$, missä m on kokonaisluku. Nyt $n^3 + 3n = (2m)^3 + 3(2m) = 8m^3 + 6m = 2(4m^3 + 3m)$. Koska $4m^3 + 3m$ on kokonaisluku, niin voidaan todeta, että $n^3 + 3n$ on jaollinen luvulla 2, kun n on parillinen.

Jos n on pariton, on se muotoa $n = 2m + 1$, jolloin

$$\begin{aligned} n^3 + 3n &= (2m+1)^3 + 3 \cdot (2m+1) \\ &= (2m+1)(2m+1)^2 + 6m + 3 \\ &= (2m+1)(4m^2 + 4m + 1) + 6m + 3 \\ &= 8m^3 + 8m^2 + 2m + 4m^2 + 4m + 1 + 6m + 3 \\ &= 8m^3 + 12m^2 + 12m + 4 \\ &= 2(4m^3 + 6m^2 + 6m + 2). \end{aligned}$$

Koska $(4m^3 + 6m^2 + 6m + 2)$ on kokonaisluku, niin lauseke $n^3 + 3n$ on jaollinen luvulla 2, kun n on pariton.

Lauseke $n^3 + 3n$ on jaollinen luvulla 2 kaikilla kokonaisluvuilla n. [3, s. 59]

3.4 Jakoyhtälö

Lause 3.3: Jakoyhtälö

Jos a ja b ovat kokonaislukuja ja $b > 0$, niin on olemassa yksikäsitteiset kokonaisluvut q ja r siten, että yhtälö

$$a = qb + r$$

pätee, kun $0 \leq r < b$. Sanotaan, että q on *osamäärä* ja r on *jakojäännös*, kun luku a jaetaan luvulla b.

Todistus. Vrt. [3, s. 67] ja [7, 32]. Tarkastellaan lukuja $a - bk$, missä k käy läpi kaikki kokonaisluvut. Olkoon $k = q$ pienin kokonaisluku, jolle $a - bk$ on positiivinen, eli kun $k < \frac{a}{b}$. Nimetään $r = a - bq$, jolloin $r \geq 0$. Pitää todistaa, että $r < b$. Tehdään vastaoletus, että $r \geq b$. Nyt $r > r - b = (a - bq) - b =$

$a - b(q+1) \geq 0$, joka on ristiriita, sillä q oli pienin kokonaisluku, jolle $a - bk > 0$. Siis on olemassa $a = qb + r$, missä $0 \leq r < b$.

Osoitetaan vielä, että jos olisi sellaiset kokonaisluvut q, r, q' ja r', että $qd + r = x = q'd + r'$, missä $0 \leq r, r' < d$, niin silloin on oltava $q = q'$ ja $r = r'$. Sovitaan, että $r \leq r'$, jolloin $0 \leq (r' - r) < r' < b$. Samalla

$$\begin{aligned} qb + r &= q'b + r' \\ qb &= q'b + r' - r \\ qb - q'b &= r' - r \\ (q - q')b &= r' - r, \end{aligned}$$

eli $0 \leq (r' - r) = (q - q')b < r' < b$. Koska sekä q että q' ovat kokonaislukuja, niin niiden erotuskin on kokonaisluku. Epäyhtälön $0 \leq (q - q')b < b$ mukaan $q - q' = 0$, joten $q = q'$. Tästä seuraa, että myös $r = r'$. □

Esimerkki 3.8

Jos $a = 100$ ja $b = 7$, niin silloin $q = 14$ ja $r = 2$, sillä $100 = 14 \cdot 7 + 2$. Jos $a = -80$ ja $b = 11$, niin silloin $q = -8$ ja $r = 8$, sillä $-80 = -8 \cdot 11 + 8$.

Esimerkki 3.9

Todista, että $5 \mid (a^5 - a)$, kun a on mikä tahansa kokonaisluku.

Jaetaan polynomi tekijöihin: $a^5 - a = a(a^4 - 1) = a(a^2 - 1)(a^2 + 1) = a(a-1)(a+1)(a^2+1)$. Jakoyhtälön avulla jaetaan kaikki kokonaisluvut ryhmiin sen perusteella, mikä on jakojäännös, kun jaetaan luvulla 5. Eri ryhmät ovat $5q$, $5q+1$, $5q+2$, $5q+3$ ja $5q+4$, missä q on kokonaisluku. Riittää todistaa, että jokin polynomin $a^5 - a$ tekijöistä on jaollinen luvulla 5.

- Kun $a = 5q$, niin tekijä a on jaollinen luvulla 5.
- Kun $a = 5q + 1$, niin tekijä $a - 1 = (5q + 1) - 1 = 5q$ on jaollinen luvulla 5.
- Kun $a = 5q + 2$, niin tekijä $a^2 + 1 = (5q + 2)^2 + 1 = 25q^2 + 20q + 4 + 1 = 5(5q^2 + 4q + 1)$ on jaollinen luvulla 5.
- Kun $a = 5q + 3$, niin tekijä $a^2 + 1 = (5q + 3)^2 + 1 = 25q^2 + 30q + 9 + 1 = 5(5q^2 + 6q + 2)$ on jaollinen luvulla 5.
- Kun $a = 5q + 4$, niin tekijä $a + 1 = (5q + 4) + 1 = 5(q + 1)$ on jaollinen luvulla 5.

Siis luku $a^5 - a$ on jaollinen luvulla 5 kaikilla kokonaisluvuilla a. [3, s. 67]

3.5 Tehtäviä

1. *Täydellinen luku* on sellainen positiivinen kokonaisluku, joka on itseään pienempien positiivisten tekijöidensä summa. [1, s. 104]
   (a) Tutki, onko luku 28 täydellinen.
   (b) Tutki, onko luku 100 täydellinen.
2. Osoita, että luku 6 on pienin täydellinen luku. [1, s. 104]
3. Jos a, b ja c ovat peräkkäisiä kokonaislukuja, mitkä seuraavista väitteistä on totta? [3, s. 64]
   (a) Ainakin yksi luvuista on jaollinen kahdella.
   (b) Yksi luvuista on jaollinen kolmella.
   (c) Yksi luvuista on jaollinen neljällä.
4. Määritä ne luvut a, joille $a \mid (a + 6)$. [2, s. 55]

5. Todista oikeaksi tai vääräksi: [2, s. 55]

   (a) Jos luku on jaollinen luvulla 3, niin se on jaollinen luvulla 9.

   (b) Jos luku on jaollinen luvulla 9, niin se on jaollinen luvulla 3.

6. Kirjoita jakoyhtälö luvuille

   (a) 58 ja 7

   (b) 84 ja 6

   (c) 150 ja 11.

7. Liisalla on 12 kirjekuorta ja 12 korttia. Kirjekuoret on numeroitu 1-12 ja kortit 110-121. Voiko Liisa sijoittaa kortin kuoren sisään siten, että kunkin kuoren numero on kortin numeron tekijä? [3, s. 64]

8. Kuusinumeroinen luku $33XY2Y$ on jaollinen luvulla 275. Määritä X ja Y. [3, s. 64]

9. Todista: Jos $a \mid b$ ja $b \mid a$, niin $a = \pm b$.

10. Todista: Jos $a \mid b$ ja $a \mid c$, niin $a \mid (xb \pm yc)$.

11. Todista oikeaksi tai vääräksi: [2, s. 55]

    (a) Jos $k \mid (ab)$, niin $k \mid a$.

    (b) Jos $a \mid (b + c)$, niin $a \mid b$ ja $a \mid c$.

    Vertaa lauseen 3.2 kohtiin 5. ja 6.

12. Osoita, että lauseke $n(n + 1)$ on parillinen kaikilla kokonaisluvuilla n. [3, s. 63]

13. Osoita, että $3 \mid (n^3 + 8n)$ kaikilla kokonaisluvuilla n. [1, s. 104]

14. Osoita, että jos n on pariton, niin $n^2 - 9$ on jaollinen luvulla 8. [1, s. 104]

4 Lukujärjestelmät

- Voiko luku 1000 tarkoittaa kahdeksaa?
- Jos saisit luoda numerojärjestelmän uudelleen, olisiko se samanlainen kuin nykyinen numerojärjestelmämme?

4.1 Kymmenjärjestelmä

Lukujen merkitsemistä helpottaa eri lukujärjestelmät. Biologisista syistä yleisesti käytetyin lukujärjestelmä on kymmenjärjestelmä. Kymmenjärjestelmä on paikkajärjestelmä, jonka kantaluku on 10, ja paikkajärjestelmällä tarkoitetaan sitä, että luvun paikka ilmaisee ykkösiä, kymmeniä, satoja jne. Kymmenjärjestelmää kutsutaan myös arabialaiseksi desimaalijärjestelmäksi.

Esimerkki 4.1

Kirjoita luku $3105,89$ kymmenpotensseja käyttäen.

$$\begin{aligned} 3105,89 &= 3000 + 100 + 5 + 0,8 + 0,09 \\ &= 3 \cdot 1000 + 1 \cdot 100 + 0 \cdot 10 + 5 \cdot 1 + 8 \cdot 0,1 + 9 \cdot 0,01 \\ &= 3 \cdot 10^3 + 1 \cdot 10^2 + 0 \cdot 10^1 + 5 \cdot 10^0 + 8 \cdot 10^{-1} + 9 \cdot 10^{-2} \end{aligned}$$

4.2 Muut lukujärjestelmät

Lause 4.1

Olkoon x kokonaisluku ja $x > 1$. Jokainen positiivinen kokonaisluku n voidaan kirjoittaa yksikäsitteisesti muodossa $n = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$, missä k on positiivinen kokonaisluku, a_j on kokonaisluku, joka on välillä $0 \leq a_j < x$, kun $j = 0, 1, \ldots, k$ ja $a_k \neq 0$.

Todistus (vrt. [7, s. 40-42]). Lähdetään tarkastelemaan lukua n jakoyhtälön kautta, kun jakajana on x. Nyt siis $n = q_0 x + a_0$ ja $0 \leq a_0 < x$. Jos $a_0 \neq 0$, niin teemme saman luvulle q_0, sitten luvulle q_1 jne. kunnes saavutetaan $q_k = 0$.

Siis

$$\begin{aligned} q_0 &= q_1 x + a_1 && (0 \leq a_1 < x) \\ q_1 &= q_2 x + a_2 && (0 \leq a_2 < x) \\ &\vdots \\ q_{k-2} &= q_{k-1} x + a_{k-1} && (0 \leq a_{k-1} < x) \\ q_{k-1} &= 0 \cdot x + a_k && (0 \leq a_k < x). \end{aligned}$$

Osamäärä q_k on lopulta 0, sillä $n > q_0 > q_1 > \cdots > q_k \geq 0$.

Nyt sijoitetaan ensimmäiseen jakoyhtälöön $n = q_0 x + a_0$ toinen, sitten kolmas jne. Saadaan

$$\begin{aligned} n &= (q_1 x + a_1)x + a_0 = q_1 x^2 + a_1 x + a_0 \\ n &= q_2 x^3 + a_2 x^2 + a_1 x + a_0 \\ &\vdots \\ n &= q_{k-1} x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0 \\ n &= a_k x^k + a_{k-1} b^{k-1} + \ldots + a_1 x + a_0. \end{aligned}$$

Nyt siis $0 \leq a_j < x$ kaikilla $j = 0, 1, \ldots, k$ ja $a_k \neq 0$.

Jakoyhtälön yksikäsitteisyyden nojalla myös tämä lukujen esitystapa on yksikäsitteinen. □

Kantaluku voi olla mikä tahansa lukua 1 suurempi kokonaisluku. Muita yleisimmin käytettyjä lukujärjestelmiä ovat 8-järjestelmä eli oktaalijärjestelmä (0-7), kuvankäsittelyssä käytetty 16-järjestelmä eli heksadesimaalijärjestelmä (0-15), jossa lukuja 10-15 merkitään kirjaimin A-F, sekä tietotekniikassa käytetty binäärijärjestelmä, jossa käytetään ainoastaan lukuja 0 ja 1.

Merkintä 4.1

Muussa kuin kymmenjärjestelmässä esitetty luku esitetään muodossa x_n, missä n on lukujärjestelmän kantaluku.

Esimerkki 4.2

- Kymmenjärjestelmän luku 2 vastaa binääriä 10, joten $2 = 10_2$.
- Kymmenjärjestelmän luku 10 vastaa oktaalia 12, joten $10 = 12_8$.

Historiaa 1: Lukujärjestelmät

Kymmenjärjestelmä ei ole ainut historian saatossa käytetty lukujärjestelmä. Alkeellisinta laskemista suoritettiin kahden ryhmissä. Silloin, kun ihminen hankki elantonsa keräilemällä ja metsästämällä, ei suurille luvuille ollut tarvetta, ja jo kahden ylittävä määrä nähtiin suurena. Australian koillisosassa asuvat heimot sekä Afrikan pygmiheimot nimeävät numeroita kahden ryhmissä.

Viisijärjestelmään perustuvat laskutavat ovat yleisempiä, sillä sormien käyttö laskemisessa on luontevaa. Grönlannin inuiittien kielessä yhdistyy viisi- ja 20-järjestelmä, sillä lukusanat tulevat ihmisen raajoista. Lukujen nimiä ovat esimerkiksi 6="toinen käsi", 7="toinen käsi kaksi", 11= "ensimmäinen jalka", 17 ="toinen jalka kaksi"ja 20="mies". Myös esimerkiksi tukkimiehen kirjanpito perustuu viiden sarjoihin ryhmittelelmiseen.

Myös lukua 12 on käytetty esimerkiksi mitta- ja painojärjestelmien kantalukuna. Briteissä oli vuoteen 1971 asti käytössä rahayksikkö, jonka perusyksikkö punta oli 20 shillinkiä ja shillinki 12 penniä. Tässä rahajärjestelmässä oli siis mukana kantaluvut 12, 20 ja 240. Kelttien parissa käytettiin kaksikymmenjärjestelmää, jonka vaikutus näkyy edelleen ranskankielessä. Ranskankielinen sana luvulle 80 on quatre-vingt, eli neljä-kaksikymmentä ja luvulle 90 quatre-vingt-dix, eli neljä-kaksikymmentä-kymmenen. Myös esimerkiksi mayat ja azteekit käyttivät kehittynyttä 20-järjestelmää.

Kymmenjärjestelmä on kuitenkin ollut jo pitkään käytetyin lukujärjestelmä. Sitä on käytetty Egyptissä, Kreikassa, Intiassa ja Kiinassa muinaisista ajoista lähtien, ja se levisi jo ennen ajanlaskun alkua. Kymmenjärjestelmä perustuu sormien lukumäärään ja on kantalukua 5 luonnollisempi, sillä ihminen on harjaantunut käyttämään molempia käsiään. [5, s. 3-5]

Muuntaminen toisesta lukujärjestelmästä kymmenjärjestelmään sujuu kätevästi lauseen 4.1 avulla.

Esimerkki 4.3

Mitä seuraavat luvut ovat kymmenjärjestelmässä: a) 1010101_2 b) 125_8

a)

$$\begin{aligned} 1010101_2 &= 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\ &= 1 \cdot 64 + 0 + 1 \cdot 16 + 0 + 1 \cdot 4 + 0 + 1 \cdot 1 \\ &= 64 + 16 + 4 + 1 \\ &= 85 \end{aligned}$$

b)

$$\begin{aligned} 125_8 &= 1 \cdot 8^2 + 2 \cdot 8^1 + 5 \cdot 8^0 \\ &= 1 \cdot 64 + 2 \cdot 8 + 5 \cdot 1 \\ &= 64 + 16 + 5 \\ &= 85 \end{aligned}$$

Esimerkki 4.4

Mitä seuraavat luvut ovat kymmenjärjestelmässä: a) $F03B_{16}$ b) $1001,101_2$?

a)

$$\begin{aligned} F03B_{16} &= 15 \cdot 16^3 + 0 \cdot 16^2 + 3 \cdot 16^1 + 11 \cdot 16^0 \\ &= 15 \cdot 4096 + 0 + 3 \cdot 16 + 11 \cdot 1 \\ &= 61440 + 48 + 11 \\ &= 61499 \end{aligned}$$

b)

$$\begin{aligned} 1001,101_2 &= 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 + 1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3} \\ &= 1 \cdot 8 + 0 + 0 + 1 \cdot 1 + 1 \cdot \frac{1}{2^1} + 0 + 1 \cdot \frac{1}{2^3} \\ &= 8 + 1 + 0,5 + 0,125 \\ &= 9,625 \end{aligned}$$

Kun halutaan muuntaa kymmenjärjestelmän luku toiseen järjestelmään, muutetaan jakolaskun avulla muoto samanlaiseksi kuin lauseessa 4.1.

Esimerkki 4.5

Esitä luku 161 oktaali- ja binäärijärjestelmässä.

Oktaalijärjestelmässä 161 on

$$161 = 20 \cdot 8 + 1 = (2 \cdot 8 + 4) \cdot 8 + 1 = 2 \cdot 8^2 + 4 \cdot 8^1 + 1 \cdot 8^0 = 241_8$$

ja vastaavasti binäärijärjestelmässä se on

$$\begin{aligned} 161 &= 2 \cdot 80 + 1 = 2 \cdot 2 \cdot 40 + 1 = 2 \cdot 2 \cdot 2 \cdot 20 + 1 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 10 + 1 \\ &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 + 1 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot (2 \cdot 2 + 1) + 1 \\ &= 2^5(2^2 + 1) + 1 = 2^7 + 2^5 + 1 = 10100001_2. \end{aligned}$$

Toinen tapa muuntaa lukuja kymmenjärjestelmästä toiseen on toistamalla jakoyhtälöä, jolloin kysytty lukujärjestelmän luku saadaan jakojäännöksistä, kun jakojäännökset luetaan alhaalta ylös.

Esimerkki 4.6

Esitä luku 161 oktaali- ja binäärijärjestelmässä.

Oktaalijärjestelmään muuntaessa jaetaan luvulla 8, jolloin

$$\begin{aligned} 161 &= 8 \cdot 20 + 1 \\ 20 &= 8 \cdot 2 + 4 \\ 2 &= 8 \cdot 0 + 2. \end{aligned}$$

Nyt jakojäännökset alhaalta ylös antavat oktaalin, joten $161 = 241_8$.

Vastaavasti binääriksi muuntaessa

$$\begin{aligned} 161 &= 2 \cdot 80 + 1 \\ 80 &= 2 \cdot 40 + 0 \\ 40 &= 2 \cdot 20 + 0 \\ 20 &= 2 \cdot 10 + 0 \\ 10 &= 2 \cdot 5 + 0 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \\ 1 &= 2 \cdot 0 + 1, \end{aligned}$$

ja saadaan $161 = 10100001_2$.

Joidenkin lukujärjestelmien välillä on helppo tehdä muunnoksia. Esimerkiksi binäärien ja heksadesimaalien välillä vaihtaminen on sujuvaa, sillä yksi heksadesimaali vastaa neljän binäärin ketjua. Pitkän binäärin jakaminen neljän binäärin ketjuihin helpottaa binäärin muuttamista heksadesimaaliksi.

Esimerkki 4.7

Binäärin 1010111001_2 muuttaminen heksadesimaaliksi aloitetaan jakamalla binääri neljän ketjuiksi, oikealta aloittaen. Saadaan ketjut 1001, 1011, ja viimeisestä muodostetaan neljän ketju lisäämällä eteen kaksi nollaa, jolloin saadaan 0010. Nyt $1001 = 2^3+1 = 9$, $1011 = 2^3+2+1 = 11$ ja $0010 = 2$, joten vastaus on heksadesimaalina $2B9_{16}$.

4.3 Tehtäviä

15. Muunna kymmenjärjestelmään a) 1000101_8 b) 2443_5
16. Muunna kymmenjärjestelmään a) 1000101_2 b) $ABBA_{16}$
17. Esitä kymmenjärjestelmän luku 100 a) binäärinä b) heksadesimaalina.
18. Esitä luku 11011011_2 oktaalina.
19. Esitä luku 31321_4 binäärinä.
20. Missä lukujärjestelmässä 52 on kymmenjärjestelmän luku 57?
21. Missä lukujärjestelmässä 21120 on kymmenjärjestelmän luku 600?
22. Esitä heksadesimaaliluvut 1-F neljän numeron binäärinketjuina.
23. Esitä luku $FA14C_{16}$ binäärinä.
24. Keksi lukujärjestelmäpari, joiden välillä on helppo vaihtaa.
25. Suorita laskutoimitukset binäärijärjestelmässä a) $10100_2 + 11011_2$ b) $10101_2 \cdot 11001_2$.

5 Alkuluvut

- Kuinka monta eri tapaa on kirjoittaa kertolasku, jonka tulo on 30? Entä 31?
- Kuinka monta tekijää on luvuilla 30 ja 31?

5.1 Alkuluku ja yhdistetty luku

Määritelmä 5.1: Alkuluku

Olkoon p positiivinen kokonaisluku ja suurempi kuin 1. Lukua p kutsutaan *alkuluvuksi*, jos p on jaollinen ainoastaan itsellään ja luvulla 1, ja niiden vastaluvuilla. [8, s. 68]

Esimerkki 5.1

Luvut 2, 3, 5, 7, 23, 41 ja 107 ovat alkulukuja.

Luku 1 ei ole alkuluku. Tämä perustuu sopimukseen, sillä jos se olisi alkuluku, minkään luvun alkutekijähajotelma ei olisi enää yksikäsitteinen. Ykkösellä kertominenhan ei muuta mitään, joten hajotelmaan voisi lisätä mielivaltaisen paljon ykkösiä [1, s. 105]. Alkutekijähajotelmasta lisää ks. määritelmä 5.3.

Määritelmä 5.2: Yhdistetty luku

Positiivista kokonaislukua, joka on suurempi kuin 1 mutta ei ole alkuluku, kutsutaan *yhdistetyksi luvuksi*. [8, s. 68]

Esimerkki 5.2

Luvut $91 = 7 \cdot 13$ ja $66 = 2 \cdot 3 \cdot 11$ ovat yhdistettyjä lukuja.

Lause 5.1

Jos p on alkuluku ja $p \mid ab$, niin $p \mid a$ tai $p \mid b$.

Todistus sivuutetaan (ks. [1, s. 132]).

Lause 5.2: Aritmetiikan peruslause

Jokainen positiivinen kokonaisluku, joka on suurempi kuin 1, voidaan esittää järjestystä vaille yksikäsitteisesti alkulukujen tulona.

Todistus (vrt. [7, s. 97-98]). Tehdään vastaoletus, että on olemassa kokonaisluku, joka on suurempi kuin 1, mutta jolla ei ole alkulukutekijää. Olkoon n pienin tällainen luku. Jos n olisi alkuluku, niin sillä olisi alkulukutekijä n. Siis luku n on yhdistetty luku ja n voidaan esittää muodossa $n = ab$, missä $1 < a, b < n$. Koska n oli pienin luku, jolla ei ole alkulukutekijää, niin luvulla a on oltava alkulukutekijä. Mutta lauseen 3.2 kohdan 4. mukaan luvun a tekijä on myös luvun n tekijä, mikä on ristiriita. Vastaoletus kumotaan, joten jokainen positiivinen kokonaisluku voidaan kirjoittaa alkulukujen tulona.

Todistetaan seuraavaksi, että luvun esitysmuoto alkulukujen tulona on yksikäsitteinen. Tehdään vastaoletus, että luku n voidaan esittää kahdella eri tavalla alkulukujen tulona. Nämä alkulukujen tulot ovat $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ ja $q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$. Nyt siis $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$. Sievennetään yhtälöstä yhteiset tekijä, jolloin saadaan $p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m} = q_1^{b_1} q_2^{b_2} \cdots q_n^{b_n}$. Nyt kaikki alkuluvut ovat toistaan eroavia, eli $p_1 \neq q_i$ kaikilla $i = 1, 2, \ldots, n$. Kuitenkin $p_1 \mid q_1^{b_1} q_2^{b_2} \cdots q_n^{b_n}$, jolloin $p_1 \mid q_i^{b_i}$ jollakin $i = 1, 2, \ldots, n$. Koska p_1 on alkuluku, niin $p_1 \mid q_i$. Mutta koska myös q_i on alkuluku, niin tulisi olla $p_1 = q_i$, mikä on ristiriita. Siis alkulukujen tulo on yksikäsitteinen. □

Määritelmä 5.3: Alkutekijähajotelma

Esitystapaa, jossa luku esitetään yksikäsitteissä muodossa alkulukujen tulona, kutsutaan *alkutekijähajotelmaksi*. [7, s. 97]

Esimerkki 5.3

Esimerkkejä alkutekijähajotelmasta:
$4 = 2 \cdot 2 = 2^2$, $40 = 2 \cdot 2 \cdot 2 \cdot 5 = 2^3 \cdot 5$ ja $287 = 7 \cdot 41$.

5.2 Alkulukujen määrä

Lause 5.3: Alkulukujen äärettömyys

Alkulukuja on äärettömän monta.

Todistus (vrt. [7, s. 67]). Tehdään vastaoletus, että alkulukuja on äärellinen määrä. Merkitään alkulukuja symboleilla p_1, p_2,..., p_n. Tarkastellaan lukua $k = p_1 p_2 \cdots p_n + 1$. Lauseen 5.2 nojalla k on alkulukujen tulo, eli joku alkuluvuista p_1, p_2,..., p_n on siis sellainen, että $p_i \mid k$. Koska myös $p_i \mid p_1 p_2 \cdots p_n$, niin pätee $p_i \mid (k - p_1 p_2 \cdots p_n) = 1$. Tämä on ristiriita, sillä $p_i > 1$. □

5.3 Alkulukujen etsiminen

On monia erilaisia menetelmiä, joilla voi tutkia, onko jokin luku alkuluku. Osa menetelmistä antaa varmasti oikean vastauksen, osa vain suurella todennäköisyydellä. Täysin varma algoritmi olisi tietysti paras vaihtoehto, mutta sellaiset ovat usein hitaita [1, s. 109]. Alkulukutesti ja Erastotheneen seula ovat kaksi tapaa, joilla voi etsiä suhteellisen pieniä alkulukuja.

Lause 5.4: Alkulukutesti

Luku $n \geq 2$ on alkuluku, jos ja vain jos se ei ole jaollinen millään sellaisella alkuluvulla, joka on enintään $\sqrt{n}$.

Todistus (vrt. [3, s. 57]). Oletetaan, että kokonaisluvuille n, x ja y pätee $n = xy$. Pitää osoittaa, että luvun n tekijöistä $x \leq \sqrt{n}$ tai $y \leq \sqrt{n}$.

Tehdään vastaväite, että $x > \sqrt{n}$ ja $y > \sqrt{n}$. Vastaväitteestä seuraa, että $x \cdot y > \sqrt{n} \cdot \sqrt{n} = n$. Tulos $xy > n$ on ristiriidassa alkuperäisen oletuksen kanssa, joten joko $x \leq \sqrt{n}$ tai $y \leq \sqrt{n}$. □

Esimerkki 5.4

Onko luku 181 alkuluku?

Käytetään alkulukutestiä. Koska $\sqrt{181} \approx 13,5$, riittää tutkia, onko 181 jaollinen luvuilla 2, 3, 5, 7, 11, 13. Koska luku 181 ei ole jaollinen millään näistä, niin se on alkuluku.

Erastotheneen seula on tehokas menetelmä alkulukujen taulukointiin, tai useampien alkulukujen etsimiseen samalla vaivalla. Jos halutaan löytää kaikki alkuluvut joukosta $\{1, 2, ..., n\}$, tehdään niistä lista. Sen jälkeen aloitetaan

pienimmästä alkuluvusta (eli luvusta 2), ja yliviivataan kaikki ne kahta suuremmat luvut, jotka ovat sillä jaollisia. Kun ollaan päästy listan loppuun, etsitään seuraava alkuluku (luvun 2 jälkeen 3) ja käydään läpi sen monikerrat. Käydään järjestyksessä läpi kaikki alkuluvut pienimmästä alkuluvusta lukuun $\sqrt{n}$ asti. Tämän jälkeen kaikki yliviivaamatta jääneet luvut ovat alkulukuja. [1, s. 109]

5.4 Goldbachin otaksuma

Goldbach esitti Eulerille vuonna 1742 otaksuman, jonka mukaan jokainen neljää suurempi parillinen luku voidaan esittää kahden alkuluvun summana. Esimerkiksi $4 = 2+2$, $14 = 3+11$ ja $20 = 7+13$. Vielä tänäkään päivänä, yli 250 vuotta myöhemmin, otaksumaa ei ole onnistuttu todistamaan oikeaksi tai vääräksi. Se kuitenkin pätee kaikille luvuille $n < 4 \cdot 10^{17}$ [6], joten vaikuttaa siltä, että se olisi myös yleisesti tosi. [2, s. 59] On kuitenkin myös hyvin mahdollista, että otaksuma ei pidäkään paikkaansa.

5.5 Tehtäviä

26. Kuinka monta parillista alkulukua on olemassa? [2, s. 55]

27. Todista oikeaksi tai vääräksi: Kahden alkuluvun

    (a) summa

    (b) tulo

    on alkuluku. [2, s. 55]

28. Hajota luku a) 63, b)129, c) 154 alkutekijöihin.

29. Hajota luku a) 1 155, b) 1386, c) 11 800 alkutekijöihin.

30. Testaa alkulukutestillä, onko luku a) 41, b) 51, c) 143 alkuluku.

31. Määritä Erasthotheneen seulalla kaikki lukujen 50 ja 100 välissä olevat alkuluvut. Vrt. [2, s. 60]

32. Esitä Goldbachin otaksuman mukaisesti kahden alkuluvun summana a) 22, b) 30, c) 100. Vrt. [2, s. 60]

33. Alkulukua p vastaa *Mersennen luku* $M_p = 2^p - 1$. [2, s. 61]

    (a) Monet Mersennen luvut ovat alkulukuja. Totea tämä luvuista M_2, M_3, M_5 ja M_7.

    (b) Kaikki Mersennen luvut eivät kuitenkaan ole alkulukuja. Totea tämä luvusta M_{11}.

    (c) Osoita, ettei alkuluku ole välttämättä Mersennen luku.

34. Ratkaise a ja b yhtälöstä $2^a 3^b = 1296$. [3, s. 64]

35. Lukion oppilaista muodostetun kuuden pelaajan lentopallojoukkueen ikien tulo on 23 970 816. Mikä on pelaajien ikien summa? [3, s. 64]

36. Todista: Jos $a \geq 3$ on alkuluku, niin $a + 1$ on yhdistetty luku. [2, s. 55]

6 Suurin yhteinen tekijä syt ja pienin yhteinen jaettava pyj

- Suorakulmion muotoisen huoneen lattia halutaan päällystää neliön muotoisilla laatoilla. Huoneen leveys on 3,6 m ja pituus 2,4 m. Mikä on suurin mahdollinen laatan sivupituus, että koko huone saadaan päällystettyä kokonaisilla laatoilla, kun sivun pituuden on oltava kokonaisluku?
- Kaksi junaa lähtee Helsingistä klo 12.00. Toinen lähtee Helsingistä 50 minuutin välein, toinen 90 minuutin välein. Monelta junat seuraavan kerran lähtevät samaan aikaan Helsingistä?

6.1 Suurin yhteinen tekijä

Määritelmä 6.1: Suurin yhteinen tekijä

Olkoot a ja b kokonaislukuja ja ainakin toinen nollasta eroava. Positiivista kokonaislukua d kutsutaan lukujen a ja b *suurimmaksi yhteiseksi tekijäksi*, jos seuraavat ehdot ovat voimassa [8, s. 90]:

1. $d \mid a$ ja $d \mid b$
2. Jos $x \mid a$ ja $x \mid b$, niin silloin $x \mid d$.

Merkintä 6.1

Suurin yhteinen tekijä merkitään $\text{syt}(a, b) = d$.

Esimerkki 6.1

Lukujen 105 ja 350 yhteiset tekijät ovat ± 1, ± 5, ± 7 ja ± 35, joten $\text{syt}(105, 350) = 35$.Muita esimerkkejä ovat $\text{syt}(6, 12) = 6$, $\text{syt}(40, 100) = 20$, $\text{syt}(7, 25) = 1$ ja $\text{syt}(-34, 17) = 17$.

6.2 Pienin yhteinen jaettava

Määritelmä 6.2: Pienin yhteinen jaettava

Olkoot a ja b positiivisia kokonaislukuja. Niiden *pienin yhteinen jaettava* on pienin positiivinen kokonaisluku, joka on jaollinen sekä luvulla a että b. [7, s. 100]

Merkintä 6.2

Pienin yhteinen jaettava merkitään $\text{pyj}(a, b) = e$.

Esimerkki 6.2

Nämä ovat lukujen pienimpiä yhteisiä jaettavia: $\text{pyj}(10, 15) = 30$, $\text{pyj}(10, 14) = 70$, $\text{pyj}(3, 21) = 21$ ja $\text{pyj}(7, 13) = 91$.

Suurimman yhteisen tekijän ja pienimmän yhteisen jaettavan voi selvittää alkutekijähajotelman avulla. Luvut a ja b kirjoitetaan alkulukujen tuloksi $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ ja $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, missä $p_1, p_2, ..., p_n$ ovat alkutekijähajotelmissa esiintyvät alkuluvut. Jos joku alkuluku p_i esiintyy vain luvun a alkutekijähajotelmassa mutta ei luvun b, niin silloin vastaava b_i on 0 ja vastaavasti a_i on 0 jos p_i esiintyy vain luvun b alkutekijähajotelmassa. Lukujen a ja b suurin yhteinen tekijä on kaikkien yhteisten alkutekijöiden tulo. Pienin yhteinen jaettava on kaikkien eri alkulukujen tulo ja jos luvuissa a ja b esiintyy sama alkuluku, valitaan suurempi a_i tai b_i.

Siis suurin yhteinen tekijä ja pienin yhteinen jaettava ovat

$$\text{syt}(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)},$$

$$\text{pyj}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)},$$

missä $\min(x, y)$ tarkoittaa pienempää luvuista x ja y ja $\max(x, y)$ suurempaa.

Esimerkki 6.3

Määritetään lukujen 240 ja 555 suurin yhteinen tekijä ja pienin yhteinen jaettava.

Jaetaan luvut alkutekijöihin:

$$240 = 24 \cdot 10 = 3 \cdot 8 \cdot 2 \cdot 5 = 2^4 \cdot 3 \cdot 5$$
$$740 = 74 \cdot 10 = 2 \cdot 37 \cdot 2 \cdot 5 = 2^2 \cdot 5 \cdot 37.$$

Koska suurin yhteinen tekijä on yhteisten tekijöiden tulo, niin

$$\operatorname{syt}(240, 740) = 2^{\min(4,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,1)} \cdot 37^{\min(0,1)} = 2^2 \cdot 3^0 \cdot 5^1 \cdot 37^0 = 20.$$

Pienin yhteinen jaettava on kaikkien eri alkulukujen tulo, joten

$$\operatorname{pyj}(240, 740) = 2^{\max(4,2)} \cdot 3^{\max(1,0)} \cdot 5^{\max(1,1)} \cdot 37^{\max(0,1)} = 2^4 \cdot 3^1 \cdot 5^1 \cdot 37^1 = 8880.$$

Lause 6.1: Syt:n ja pyj:n tulo

Kahden luvun tulo on yhtä kuin niiden syt:n ja pyj:n tulo

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

Todistus Ks. [2, s.70]. Olkoon $d = \operatorname{syt}(a, b)$. Tällöin $a = dm$ ja $b = dn$ ja $\operatorname{syt}(m, n) = 1$. Jos $\operatorname{syt}(m, n) = s > 1$, niin silloin luvuilla a ja b olisi yhteinen tekijä $ds > d$. Koska $\operatorname{pyj}(a, b) = dmn$, niin $ab = dmdn = d(dmn) = \operatorname{syt}(a, b) \operatorname{pyj}(a, b)$. □

Esimerkki 6.4

Lukujen 240 ja 740 tulo on 177600. Niiden suurimman yhteisen tekijän ja pienimmän yhteisen jaettavan laskimme esimerkissä 6.3 ja niiden tulo on $\operatorname{syt}(240, 740) \cdot \operatorname{pyj}(240, 740) = 20 \cdot 8880 = 177600$.

6.3 Eukleideen algoritmi

Kun tutkittavat luvut ovat suuria, on alkutekijöihin jako työlästä. Silloin suurimman yhteisen tekijän hakemiseen kannattaa käyttää Eukleideen algoritmia. [3, s. 79]

Lause 6.2: Eukleideen algoritmi

Olkoot a ja b positiivisia kokonaislukuja ja olkoon $a \geq b$. *Eukleideen algoritmissa* toistetaan jakoyhtälöä peräkkäin, korvaamalla jaettava jakajalla ja jakaja jakojäännöksellä, kunnes jako menee tasan:

$$\begin{aligned} a &= q_0 b + r_1 && (0 \leq r_1 < b) \\ b &= q_1 r_1 + r_2 && (0 \leq r_2 < r_1) \\ r_1 &= q_2 r_2 + r_3 && (0 \leq r_3 < r_2) \\ &\vdots \\ r_{k-2} &= q_{k-1} r_{k-1} + r_k && (0 \leq r_k < r_{k-1}) \\ r_{k-1} &= q_k r_k. \end{aligned}$$

Viimeinen nollasta eroava jakojäännös on lukujen a ja b suurin yhteinen tekijä, eli $\text{syt}(a, b) = r_k$.

Todistus Vrt. [7, s. 81 ja 87-88]. Kun algoritmia suoritetaan, jää jakojäännökseksi lopulta 0. Algoritmi voidaan suorittaa enintään a kertaa, sillä kokonaislukuja $a \geq b > r_1 > r_2 > \ldots \geq 0$ voi olla enintään a kappaletta.

Todistetaan, että jakoyhtälössä $a = q_0 b + r_1$ pätee $\text{syt}(a, b) = \text{syt}(b, r_1)$. Nyt, koska $\text{syt}(a, b) = \text{syt}(q_0 b + r_1, b)$, voidaan todistaa, että $\text{syt}(q_0 b + r_1, b) = \text{syt}(b, r_1)$. Riittää todistaa, että luvuilla $q_0 b + r_1$ ja b on täsmälleen samat yhteiset tekijät kuin luvuilla b ja r_1.

Olkoon x lukujen b ja r_1 yhteinen tekijä. Nyt siis $x \mid b$ ja $x \mid r_1$, joten lauseen 3.2 kohdan 7. perusteella $x \mid (q_0 b + r_1)$. Siis x on myös lukujen $(q_0 b + r_1)$ ja b yhteinen tekijä.

Olkoon y lukujen $(q_0 b + r_1)$ ja b yhteinen tekijä. Nyt lauseen 3.2 kohdan 5. mukaan $y \mid q_0 b$, ja koska $y \mid (q_0 b + r_1)$ ja $y \mid q_0 b$, niin lauseen 3.2 kohdan 6. mukaan pätee myös $y \mid ((q_0 b + r_1) - q_0 b) = r_1$. Siis y on myös lukujen b ja r_1 yhteinen tekijä.

Koska lukupareilla $(q_0 b + r_1)$ ja b sekä b ja r_1 on täsmälleen samat yhteiset tekijät, niin $\text{syt}(q_0 b + r_1, b) = \text{syt}(b, r_1)$, mikä on yhtäpitävää yhtälön $\text{syt}(a, b) = \text{syt}(b, r_1)$ kanssa.

Algoritmilla saadaan $\text{syt}(a, b) = \text{syt}(b, r_1) = \text{syt}(r_1, r_2) = \ldots = (r_{k-1}, r_k) = (r_k, 0) = r_k$, joten viimeinen nollasta eroava jakojäännös on lukujen a ja b suurin yhteinen tekijä. □

6.4 Tehtäviä

37. Määritä a) $\text{syt}(55, 132)$, b) $\text{syt}(231, 429)$ i) jakamalla tekijöihin, ii) Eukleideen algoritmilla.

38. Määritä

    (a) $\text{pyj}(231, 429)$

    (b) $\text{pyj}(13, 16, 65)$.

39. Määritä $\text{syt}(240, 280, 334)$.

40. Määritä kokonaisluku a, kun $\text{pyj}(a, 19) = 228$ ja $a < 19$, [1, s. 124]

41. Supista

    (a) $\frac{963}{3081}$

    (b) $\frac{20767}{46702}$

    (c) $\frac{62963}{104407}$.

42. Päiväntasaajalla olevassa kylässä paikallinen tähtiharrastaja havaitsee kaksi satelliittia yhtä aikaa suoraan päänsä yläpuolella. Hän tarkkailee satelliitteja pidemmän aikaa ja toteaa niiden kiertoajoiksi 90 ja 98 minuuttia. Minkä ajan kuluttua satelliitit ovat seuraavan kerran yhtä aikaa havaitsijan yläpuolella? [1, s. 124]

43. Oletetaan, että $\text{syt}(a, b) = 3$. Voiko tällöin olla $a + b = 100$? [2, s. 74]

44. Kahden kokonaisluvun tulo on 1935 ja niiden pienin yhteinen jaettava on 645. Määrää luvut. (Huom! Kaksi ratkaisua.) [3, s. 65]

45. Etsi kaksi kokonaislukua, joiden suurin yhteinen tekijä on 140 ja pienin yhteinen jaettava on 9800. Määrää kaikki tehtävän ratkaisut. [3, s. 65]

46. Osoita, ettei murtolukua $\frac{21n+4}{14n+3}$ voida sieventää, olipa kokonaisluku n mikä tahansa. [1, s. 124]

47. Osoita, että jos $\text{syt}(a, b) = 1$, niin $\text{syt}(a + b, a - b) = 1$ tai 2. [1, s. 124]

7 Kongruenssi

- Lähdet matkalle maanantaina klo 6.00. Matkasi kestää 700 tuntia. Milloin palaat takaisin?
- Montako lukua keksit, jotka jaettuna 5:llä antavat jakojäännökseksi luvun 1? Mikä yleinen lauseke niille saadaan?

Esimerkki 7.1

Kirjoita jakoyhtälönä a) $16 : 7$ b) $93 : 7$ c) $2 : 7$.

a) Jakoyhtälö: $16 = 2 \cdot 7 + 2$
b) Jakoyhtälö: $93 = 13 \cdot 7 + 2$
c) Jakoyhtälö: $2 = 0 \cdot 7 + 2$

Esimerkissä nähdään, että yhteistä luvuille 2, 16 ja 93 on se, että niillä on sama jakojäännös, kun ne jaetaan seitsemällä. Sanotaan, että nämä luvut ovat *kongruentteja* keskenään modulo 7.

Määritelmä 7.1: Kongruenssi

Olkoon m positiivinen kokonaisluku. Kun a ja b ovat kokonaislukuja, niin luku a on *kongruentti* luvun b kanssa (tai toisin sanoen luvut a ja b ovat *kongruentteja*) *modulo* m, jos $m \mid (a - b)$. [8, s. 142]

Merkintä 7.1

Kun luku a on kongruentti luvun b kanssa, niin $a \equiv b \pmod{m}$.
Kun luku a ei ole kongruentti luvun b kanssa, niin $a \not\equiv b \pmod{m}$.

Jakoyhtälön perusteella jaettava on aina kongruentti jakojäännöksensä kanssa modulo jakaja, sillä kun $a = qb + r$, niin $a - r = dq$ eli $d \mid (a - r)$.

Esimerkki 7.2

Kellonajat ovat yleisimmin käytetty kongruenssi, sillä

$$\begin{aligned} 13 &\equiv 1 \pmod{12} \\ 15 &\equiv 3 \pmod{12} \\ 20 &\equiv 8 \pmod{12} \\ 24 &\equiv 0 \pmod{12}. \end{aligned}$$

Esimerkki 7.3

- Kongruenssi $10 \equiv 1 \pmod{3}$ pätee, sillä $3 \mid (10 - 1) = 9$.
- Kongruenssi $15 \not\equiv 0 \pmod{8}$ pätee, sillä $8 \nmid (15 - 0) = 15$.
- Kongruenssi $32 \equiv 2 \pmod{5}$ pätee, sillä $5 \mid (32 - 2) = 30$
- Kongruenssi $x \equiv 0 \pmod{m}$ pätee silloin, kun $m \mid (x - 0)$, eli silloin kun $m \mid x$.

Lause 7.1

Kokonaisluvut a ja b toteuttavat kongruenssin $a \equiv b \pmod{m}$, jos ja vain jos on olemassa kokonaisluku k, jolle pätee $a = b + km$.

Todistus (vrt. [7, s.129]). Kun $a \equiv b \pmod{m}$, niin $m \mid (a - b)$. On siis olemassa kokonaisluku k, jolle pätee $km = a - b$, eli $a = b + km$. Vastaavasti, jos on olemassa kokonaisluku k, joka toteuttaa yhtälön $a = b + km$, eli $km = a - b$, niin silloin $m \mid (a - b)$ ja $a \equiv b \pmod{m}$. □

Esimerkki 7.4

Kun $17 \equiv 2 \pmod{3}$, niin $k = 5$ ja $17 = 2 + 5 \cdot 3$. Yhtälö $21 = 1 + 5k$ pätee, kun $k = 4$, joten $21 \equiv 1 \pmod{5}$.

Esimerkki 7.5

Kuten esimerkissä 7.3:

- Yhtälö $10 = 1 + 3k$ pätee, kun $k = 3$.
- Ei löydy kokonaislukua k, joka toteuttaisi yhtälön $15 = 8k$.
- Yhtälö $32 = 2 + 5k$ pätee, kun $k = 6$.
- Yhtälö $x = km$ pätee, kun $m \mid x$.

Lause 7.2

Kongruensseilla modulo m on seuraavat ominaisuudet, kun m on positiivinen kokonaisluku:

1. Kun a on kokonaisluku, niin $a \equiv a \pmod{m}$.
2. Kun kokonaisluvut a ja b toteuttavat konruenssin $a \equiv b \pmod{m}$, niin myös kongruenssi $b \equiv a \pmod{m}$ pätee.
3. Kun kokonaisluvut a, b ja c toteuttavat konruenssit $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$, niin myös kongruenssi $a \equiv c \pmod{m}$ pätee.

Todistus (vrt. [7, s.129]).

1. Kongruenssi $a \equiv a \pmod{m}$ pätee, koska $m \mid (a - a) = 0$.
2. Kun $a \equiv b \pmod{m}$, niin $m \mid (a - b)$. Siis on olemassa kokonaisluku t, joka toteuttaa yhtälön $tm = a - b$, mikä on yhtäpitävää yhtälön $-tm = -(a - b)$ kanssa. Nyt $(-t)m = -tm = -(a - b) = b - a$, joten $m \mid (b - a)$. Siis kongruenssi $b \equiv a \pmod{m}$ pätee.
3. Kun $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$, niin $m \mid (a - b)$ ja $m \mid (b - c)$. Siis on olemassa kokonaisluvut t ja u, joille $tm = a - b$ ja $um = b - c$. Siis $(a - c) = (a - b) + (b - c) = tm + um = (t + u)m$ ja tästä seuraa, että $m \mid (a - c)$, jolloin $a \equiv c \pmod{m}$.

□

Esimerkki 7.6

1. Kongruenssi $17 \equiv 17 \pmod 3$ pätee, sillä $3 \mid (17 - 17) = 0$.
2. Koska $x \equiv 1 \pmod 5$, niin myös $1 \equiv x \pmod 5$, sillä $5 \mid (x - 1)$, eli $5t = x - 1$, jolloin $5 \cdot -t = -5t = -(x - 1) = 1 - x$, joten $5 \mid (1 - x)$.
3. Koska $88 \equiv 7 \pmod 9$ ja $43 \equiv 7 \pmod 9$, niin $88 \equiv 43 \pmod 9$. Tämä pätee, sillä $9 \mid (88 - 43) = 45$.

7.1 Kongruenssien laskusäännöt

Lause 7.3

Olkoot a, b, c, d ja m kokonaislukuja ja olkoon $m > 0$. Kun $a \equiv b \pmod m$ ja $c \equiv d \pmod m$, niin

1. $a + c \equiv b + d \pmod m$,
2. $ac \equiv bd \pmod m$,

Todistus (vrt. [2, s.85]). Oletuksen mukaan $m \mid (a - b)$ ja $m \mid (c - d)$, joten on olemassa kokonaisluvut t ja u, jotka toteuttavat yhtälöt $tm = a - b$ ja $um = c - d$, joten $a = b + tm$ ja $c = d + um$.

1. Nyt $a+c = (b+tm)+(d+um) = b+d+tm+um = b+d+(t+u)m \equiv b+d \pmod m$
2. Nyt $c(a - b) = c(tm)$ ja $b(c - d) = b(um)$, jotka yhteenlaskettuna ovat

$$\begin{aligned} c(a - b) + b(c - d) &= c(tm) + b(um) \\ ac - bc + bc - bd &= ctm + bum \\ ac - bd &= (ct + bu)m \end{aligned}$$

joten $m \mid (ac - cd)$.

□

Lause 7.4

Olkoot a, b, c ja m kokonaislukuja ja olkoon $m > 0$. Kun $a \equiv b \pmod{m}$, niin

1. $a + c \equiv b + c \pmod{m}$,
2. $a - c \equiv b - c \pmod{m}$,
3. $ac \equiv bc \pmod{m}$.

Todistus (vrt. [7, s.130]). Kun $a \equiv b \pmod{m}$, niin $m \mid (a - b)$.

1. Koska $(a+c)-(b+c) = (a-b)$, niin $m \mid ((a+c)-(b+c))$ eli $a+c \equiv b+c \pmod{m}$.
2. Harjoitustehtävä
3. Kun $m \mid (a - b)$, niin myös $m \mid (a - b) \cdot c = (ac - bc)$, joten $ac \equiv bc \pmod{m}$.

□

Esimerkki 7.7

Koska $10 \equiv 0 \pmod{5}$, niin myös $13 = 10 + 3 \equiv 0 + 3 = 3 \pmod{5}$.
Koska $17 \equiv 3 \pmod{7}$, niin myös $13 = 17 - 4 \equiv 3 - 4 = -1 \pmod{7}$.
Koska $30 \equiv 3 \pmod{9}$, niin myös $60 = 30 \cdot 2 \equiv 3 \cdot 2 = 6 \pmod{9}$.

Lause 7.5

Olkoot a, b ja m kokonaislukuja ja olkoon $m > 0$. Kun $a \equiv b \pmod{m}$, niin $a^n \equiv b^n \pmod{m}$ kaikilla kokonaisluvuilla $n > 0$.

Todistus. Tämä lause on seurausta lauseen 7.3 kohdasta 2. □

On laskuja, jotka voidaan helposti laskea kongruenssilla, mutta joita laskin ei pysty laskemaan liian suurten lukujen takia. Esimerkiksi 2^{91} on liian suuri luku laskimelle.

Esimerkki 7.8

Laske jakojäännös laskussa $2^{91} : 3$.

Käytämme apunamme kongruenssia $2^2 = 4 \equiv 1 \pmod 3$. Nyt

$$2^{91} = 2^{2\cdot 45+1} = (2^2)^{45} \cdot 2^1 \equiv 1^{45} \cdot 2 = 1 \cdot 2 = 2 \pmod 3,$$

joten jakojäännös laskussa $2^{91} : 3$ on 2.

Esimerkki 7.9

Mikä on luvun 3^{255} viimeinen numero?

Luvun viimeinen numero saadaan laskemalla kongruenssi modulo 10. Käytetään apunamme tietoa $3^2 \equiv -1 \pmod{10}$. Nyt

$$3^{255} = 3^{2\cdot 127+1} = (3^2)^{127} \cdot 3^1 \equiv (-1)^{127} \cdot 3 = -1 \cdot 3 = -3 \equiv 7 \pmod{10},$$

joten luvun 3^{255} viimeinen numero on 7.

Esimerkki 7.10

Osoita, että $22^n + 5 \cdot 8^n + 1$ on jaollinen luvulla 7 kaikilla $n > 0$.

Huomataan, että $22 \equiv 1 \pmod 7$ ja $8 \equiv 1 \pmod 7$. Nyt

$$22^n + 5 \cdot 8^n + 1 \equiv 1^n + 5 \cdot 1^n + 1 = 1 + 5 + 1 = 7 \equiv 0 \pmod 7,$$

joten $22^n + 5 \cdot 8^n + 1$ on jaollinen luvulla 7 kaikilla $n > 0$.

7.2 Jaollisuustestien todistukset

Nyt todistamme kongruensseilla lauseessa 3.1 esitetyt jaollisuustestit.

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

- *Jaollisuus luvulla 2:* Koska $10 \equiv 0 \pmod 2$, niin myös $10^i \equiv 0 \pmod 2$ kaikilla $i > 0$. Nyt siis $a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0 \equiv a_k \cdot 0 + a_{k-1} \cdot 0 + \cdots + a_1 \cdot 0 + a_0 = a_0 \pmod 2$, eli $x \equiv a_0 \pmod 2$. Siis $2 \mid x$, jos ja vain jos $2 \mid a_0$.

- *Jaollisuus luvulla 3:* Koska $10 \equiv 1 \pmod 3$, niin myös $10^i \equiv 1 \pmod 3$ kaikilla $i > 0$. Nyt siis $a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0 \equiv a_k \cdot 1 + a_{k-1} \cdot 1 + \cdots + a_1 \cdot 1 + a_0 = a_k + a_{k-1} + \cdots + a_0 \pmod 3$. Siis $3 \mid x$, jos ja vain jos $3 \mid (a_k + a_{k-1} + \cdots + a_0)$.

- *Jaollisuus luvulla 4:* Koska $100 \equiv 0 \pmod 4$, niin myös $10^i \equiv 0 \pmod 2$ kaikilla $i \geq 2$. Nyt siis $a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_2 100 + a_1 10 + a_0 \equiv a_k \cdot 0 + a_{k-1} \cdot 0 + \cdots + a_2 \cdot 0 + a_1 10 + a_0 = a_1 10 + a_0 \pmod 4$, eli $x \equiv a_1 10 + a_0 \pmod 4$. Siis $4 \mid x$, jos ja vain jos $4 \mid (a_1 10 + a_0)$.

- *Jaollisuus luvulla 6:* Jos $6 \mid x$, niin koska $2 \mid 6$ ja $3 \mid 6$, niin lauseen 3.2 kohdan 4. perusteella myös $2 \mid x$ ja $3 \mid x$.

  Jos $2 \mid x$, niin on olemassa kokonaisluku t, jolle pätee $x = 2t$. Kun lisäksi $3 \mid x = 2t$, niin $3 \mid t$, jolloin on olemassa kokonaisluku u, jolle $t = 3u$. Siis $x = 2t = 2(3u) = 6u$. Vastaavasti, jos $3 \mid x$, niin kokonaisluvulla t' $x = 3t'$ ja koska myös $2 \mid x = 3t'$, niin $2 \mid t'$, joten kokonaisluvulla u' $t' = 2u'$, jolloin $x = 3t' = 3(2u') = 6u'$. Molemmissa tapauksissa $6 \mid x$.

- *Jaollisuus luvulla 7:* Merkitään $y = a_k 10^{k-1} + a_{k-1}10^{k-2} + \cdots + a_1$, jolloin $x = 10y + a_0$. Nyt $5x = 50y + 5a_0 \equiv 1y - 2a_0 = y - 2a_0 \pmod 7$. Nyt siis $7 \mid 5x$, jos ja vain jos $7 \mid y - 2a_0$. Koska $7 \nmid 5$, niin $7 \mid 5x$, jos ja vain jos $7 \mid x$. Siis $7 \mid x$, jos ja vain jos $7 \mid y - 2a_0$.

Loput harjoitustehtäviä. □

7.3 Tehtäviä

48. Kello on 00:00. Paljonko kello on a) 221 b) 1141 tuntia myöhemmin?

49. Näyttävätkö a) 12-tuntinen b) 24-tuntinen kello samaa aikaa 100 ja 184 tunnin kuluttua?

50. Osoita, että a) $573 \equiv 453 \pmod 8$ b) $150 \equiv -543 \pmod 7$ c) $2^{20} \equiv 1 \pmod{11}$.

51. Määritä pienin luonnollinen luku x, joka toteuttaa kongruenssin a) $177 \equiv x \pmod 9$ b) $-21 \equiv x \pmod 5$ c) $1010 \equiv x \pmod{17}$.

52. Määritä kaikki sellaiset luvut n, jotka toteuttavat kongruenssin $35 \equiv 2 \pmod n$.

53. Laske jakojäännös, kun luvun a)6^{277} b) 3^{28} c) $234 \cdot 8^{216}$ jakaa seitsemällä?

54. Mikä on luvun a) 9^{117} b) 5^{123} ja c) 3^{1215} viimeinen numero?

55. Todista, että luvuilla $38^{25} + 3$ ja $4^{25} + 20$ on sama jakojäännös, kun ne jaetaan luvulla 17.

56. Todista, että $a - c \equiv b - c \pmod m$, kun $a \equiv b \pmod m$.

57. Todista luvun 5 jaollisuustesti.

58. Todista luvun 8 jaollisuustesti.

59. Todista luvun 9 jaollisuustesti.

8 Kongruenssien sovellukset

- Miksi $10^6 \equiv 1 \pmod 7$?
- Milloin 3 on yhtä kuin 13?

8.1 Fermat'n pieni lause

Lause 8.1

Olkoot a, b, x ja n kokonaislukuja ja olkoon n suurempi kuin 0. Kun $(x, n) = 1$ ja $ax \equiv bx \pmod n$, niin $a \equiv b \pmod n$.

Todistus sivuutetaan (ks. [8, s. 145]).

Lause 8.2: Fermat'n pieni lause

Olkoon p alkuluku ja x positiivinen kokonaisluku, niin että $p \nmid x$. Tällöin pätee

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

Todistus (vrt. [8, s. 217–218]). Tarkastellaan lukuja x, $2x$, $3x$, $\ldots$, $(p-1)x$. Yksikään joukossa olevista luvuista ei ole jaollinen luvulla p, koska $p \nmid x$ ja koska p on alkuluku.

Joukosta ei myöskään löydy kahta lukua, jotka olisivat kongruentteja modulo p. Muuten olisi olemassa j ja k, joille pätee $jx \equiv kx \pmod p$, missä $1 \leq j < k \leq p-1$. Koska $(x, p) = 1$, niin lauseen 8.1 perusteella $j \equiv k \pmod p$, mutta koska j ja k ovat molemmat pienempiä kuin p, niin todetaan tämän olevan mahdotonta. Luvut x, $2x$, $3x$, $\ldots$, $(p-1)x$ ovat siis kaikki epäkongruentteja modulo p.

Nyt tiedämme, että joukon x, $2x$, $3x$, $\ldots$, $(p-1)x$ pienimmät positiiviset jäännökset modulo p ovat 1, 2, 3, $\ldots$, $(p-1)$ jossakin järjestyksessä. Siis

$$\begin{aligned} x \cdot 2x \cdot 3x \cdots (p-1)x &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p \\ x^{p-1}(p-1)! &\equiv (p-1)! \pmod p. \end{aligned}$$

Nyt siis $p \mid (x^{p-1}(p-1)! - (p-1)!) = (p-1)!(x^{p-1} - 1)$. Mutta koska $p \nmid (p-1)!$, niin silloin täytyy olla $p \mid (x^{p-1} - 1)$. Siis $x^{p-1} \equiv 1 \pmod p$. □

Esimerkki 8.1

Laske, mikä on jakojäännös, kun luku 16^4 jaetaan luvulla 5.

Koska luku 5 on alkuluku ja $5 \nmid 16$, niin voidaan käyttää Fermat'n pientä lausetta, jolloin

$$16^4 = 16^{5-1} \equiv 1 \pmod{5}.$$

Esimerkin 8.1 lasku voidaan laskea myös laskimella, sillä $16^4 = 65536$. Nyt käyttämällä jakoyhtälöä saadaan $65536 = 13107 \cdot 5 + 1$. Nyt nähdään, että jakojäännös on tosiaan 1 silloin kun 16^4 jaetaan luvulla 5.

Fermat'n pieni lause on hyödyllinen, kun lasketaan korkeita potensseja, joita on muuten vaikea laskea.

Esimerkki 8.2

Mikä on pienin kokonaisluku, joka on kongruentti luvun 7^{322} kanssa modulo 11?

Fermat'n pientä lausetta käyttämällä saadaan

$$7^{322} = 7^{32 \cdot 10 + 2} = (7^{10})^{32} \cdot 7^2 \equiv 1^{32} \cdot 49 \equiv 5 \pmod{11}.$$

Esimerkki 8.3

Osoita, että luku $2^{216} - 1$ on jaollinen luvulla 35.

Huomataan, että $35 = 5 \cdot 7$, ja koska luvut 5 ja 7 ovat alkulukuja, niin riittää todistaa, että luku $2^{216} - 1$ on jaollinen sekä luvulla 5, että luvulla 7. Koska $5 \nmid 2$ ja $7 \nmid 2$, niin voidaan käyttää Fermat'n lausetta, jolloin saadaan

$$2^{216} - 1 = 2^{4 \cdot 54} - 1 = (2^4)^{54} - 1 \equiv 1^{54} - 1 = 1 - 1 = 0 \pmod{5}$$

ja

$$2^{216} - 1 = 2^{6 \cdot 36} - 1 = (2^6)^{36} - 1 \equiv 1^{36} - 1 = 1 - 1 = 0 \pmod{7}.$$

Koska luku $2^{216} - 1$ on jaollinen luvuilla 5 ja 7, niin se on jaollinen myös luvulla 35.

Historiaa 2: Fermat'n suuri lause

Fermat on kuuluisa pienen lauseensa lisäksi myös suuresta lauseestaan, joka on yksi lukuteorian tunnetuimmista ongelmista. Fermat'n suuren lauseen mukaan yhtälöllä $x^n + y^n = z^n$ ei ole nollasta eroavia kokonaislukuratkaisuja, kun $n > 2$. Fermat esitti lauseen kirjeessään 1600-luvulla mutta ei liittänyt siihen todistusta, koska se oli liian pitkä. Nykyisin epäillään, että Fermat'lla ei ollut todistusta lainkaan, tai se oli virheellinen, sillä täydellisen todistuksen teki Andrew Wiles vasta 350 vuotta myöhemmin. Wiles työskenteli todistuksen parissa 7 vuotta, kunnes vuonna 1995 200-sivuinen todistus oli valmis. Wilesin todistuksessa käytetään modernia matematiikkaa, jota Fermat ei olisi voinut 1600-luvulla käyttää. [3, s. 51] [7, s. 490-492]

8.2 Jäännösluokat

Kongruenssin avulla kokonaisluvut voidaan järjestää jäännösluokkiin. Kaikki samaan jäännösluokkaan kuuluvat luvut ovat keskenään kongruentteja, ja kaikki kongruentit kuuluvat samaan jäännösluokkaan. Eri jäännösluokkiin kuuluvat luvut eivät ole keskenään kongruentteja. Kongruenssin modulo on samalla jäännösluokkien lukumäärä.

Esimerkki 8.4

Modulon 3 jäännösluokkia on kolme kappaletta, ja ne ovat:

- kolmella jaolliset $\{\ldots, -6. - 3, 0, 3, 6, 9, \ldots\}$,
- jakojäännökseksi 1 $\{\ldots, -5, -2, 1, 4, 7, \ldots\}$,
- jakojäännökseksi 2 $\{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

Määritelmä 8.1: Jäännösluokka

Olkoot x ja m kokonaislukuja. Jäännösluokka modulo m on

$$[a]_m = \{x \equiv a \pmod{m}\} = \{a + km : k \in Z\}.$$

[3, s. 101]

Esimerkki 8.5

Mitkä luvuista -9, -1, 10, 14 ja 21 kuuluvat samaan jäännösluokkaan modulo 5?

Koska

$$\begin{aligned} -9 &\equiv 1 \pmod 5 \\ -1 &\equiv 4 \pmod 5 \\ 10 &\equiv 0 \pmod 5 \\ 14 &\equiv 4 \pmod 5 \\ 21 &\equiv 1 \pmod 5, \end{aligned}$$

joten samoihin jäännösluokkiin kuuluvat

$$\begin{aligned} [0]_5 &= \{10\} \\ [1]_5 &= \{-9, 21\} \\ [4]_5 &= \{-1, 14\}. \end{aligned}$$

Lause 8.3: Jäännösluokkien ominaisuuksia

1. Jos $[a]_m = [b]_m$, niin $a \equiv b \pmod m$.
2. Jäännösluokkien lukumäärä on m, ja ne voidaan esittää muodossa $[0]_m, [1]_m, \ldots, [m-1]_m$.
3. Jokainen kokonaisluku kuuluu täsmälleen yhteen jäännösluokkaan.

Todistus. 1. Koska joillakin kokonaisluvuilla k ja l pätee $[a]_m = a + km$ ja $[b]_m = b + lm$, niin

$$\begin{aligned} [a]_m &= [b]_m \\ a + km &= b + lm \\ lm - km &= a - b \\ (l-k)m &= a - b \end{aligned}$$

ja nyt nähdään, että $m \mid (a-b)$. Siis $a \equiv b \pmod m$.

2. Lauseen 3.3 mukaan jakoyhtälö on $a = qm + r$, missä $0 \leq r < m$,

joten pienimmät mahdolliset jakojäännökset ovat $0, 1, \ldots, m-1$. Siis pienimmät jäännösluokat ovat $[0]_m, [1]_m, \ldots, [m-1]_m$.

3. Harjoitustehtävä

□

8.3 Tehtäviä

60. Laske jakojäännös kun a) 20^{123} b) 22^{211} jaetaan luvulla 11.

61. Määritä jakojäännös kun $4^{234} \cdot 10^{351}$ jaetaan luvulla 13.

62. Osoita, että $5^{1704} - 2^{2265}$ on jaollinen luvulla 7.

63. Montako jäännösluokkaa on modulo 7? Mitkä nämä jäännösluokat ovat?

64. Mitkä luvuista -14, -1, 1, 2, 10 ja 20 kuuluvat samaan jäännösluokkaan modulo 4?

65. Onko $[7]_m = [10]_m$, kun a) $m = 3$ b) kun $m = 4$?

66. Mille kahdelle positiiviselle kokonaisluvulle pätee, että $[14]_m$ kuuluu luokkaan $[4]_m$, joka on pienin mahdollinen positiivinen jäännösluokka?

67. Paljonko on a) $[a]_m + [b]_m$ b) $[a]_m \cdot [b]_m$?

68. Todista, että jokainen kokonaisluku kuuluu täsmälleen yhteen jäännösluokkaan.

9 Tarkistusnumerot

- Mistä henkilötunnuksen loppuosa tulee?
- Mikä on tarkistusnumero?

Nykymaailmassa digitaalinen tiedonsiirto on kokoaikaista. Kun numeroketjuja siirretään paikasta toiseen, on virheiden mahdollisuus suuri. Numeroketjujen oikeellisuuden tarkistamista varten on kehitetty tarkistusjärjestelmiä, joissa usein käytetään kongruensseja.

9.1 Binäärikoodit

Binäärikoodit ovat biteiksi koodattuja viestejä. Binäärikoodiin tulleet virheet on tärkeää huomata ja korjata. Siksi binäärikoodiin $x_1x_2...x_n$ lisätään tarkistusnumero x_{n+1}, jonka avulla tarkistetaan, onko binäärikoodissa virhe. Tarkastusnumero x_{n+1} voidaan muodostaa esimerkiksi kongruenssilla $x_{n+1} \equiv x_1+x_2+...+x_n \pmod 2$. Tällöin, jos binäärikoodissa on pariton määrä lukuja 1, on tarkistusnumero 1, ja jos binäärikoodissa on parillinen määrä lukuja 1, on tarkistusnumero 0. Täten numeroiden 1 määrä on aina parillinen. [4, s. 257-258]

Esimerkki 9.1

Halutaan lähettää yhdeksän bitin koodi 1011111101. Muodostetaan tarkastusnumero $x_{10} \equiv 1+0+1+1+1+1+1+0+1 = 7 \pmod 2$. Siis $x_{10} = 1$, joten lähetettävä viesti on 1011111011.

Jos bittiketjussa on yksi virhe, niin se on helppo huomata. Bittiketjun pariton määrä 1:siä osuu heti silmään, ja korjaaminen on helppoa sitten kun tietää virheellisen bitin sijainnin.

9.2 Henkilötunnus

Suomen henkilötunnus koostuu syntymäajasta, välimerkistä, kolminumeroisesta luvusta, joka kertoo monennesta sinä päivänä syntyneestä vauvasta on kyse, ja viimeinen merkki on tarkistusmerkki.

Merkitään henkilötunnusta merkkijonolla $x_1x_2x_3x_4x_5x_6x_7x_8x_9Y$, missä x_1-x_6 kertovat syntymäajan, x_7-x_9 ovat välimerkin jälkeiset kolme lukua, ja Y on henkilötunnuksen tarkistusmerkki. Välimerkin jälkeinen kolminumeroinen luku on vauvan järjestysnumero siten että tyttövauvat saavat parillisen järjestysnumeron ja pojat parittoman. Tarkistusmerkki on määritelty

$Y \equiv x_1x_2x_3x_4x_5x_6x_7x_8x_9 \pmod{31}$, missä $Y = 0, 1, 2, ..., 29, 30$ ja merkit 10-30 on korvattu kirjaimilla A-W, mutta kirjaimet I ja O on jätetty pois sekaannuksien välttämiseksi. [1, s. 114]

Esimerkki 9.2

Poika syntyy 10.3.2001 ja on päivän 39. poikavauva. Mikä on hänen henkilötunnuksensa?

Alkuosaksi muodostuu pojan syntymäpäivä, eli 10032001. Poikavauvan järjestysnumero määräytyy kaavalla $2n - 1$, missä n on monennes poikavauva hän on. Nyt siis $2 \cdot 39 - 1 = 77$, joten pojan kolminumeroinen järjestysnumero on 077 ja pojan henkilötunnuksen ensimmäiset 9 merkkiä ovat 10032001077. Tarkistusmerkiksi saadaan kongruenssilla $10032001077 \equiv 30 \pmod{31}$. Koska tarkistusnumero 30 on korvattu kirjaimella W, niin pojan henkilötunnukseksi muodostuu 10032001-077W.

9.3 Tehtäviä

69. Onko koodissa a) 11011011011 b) 10110110111010101101 c) 11111111111111 virhettä?

70. Lisää tarkistusnumero koodiin a) 1111 b) 101010110.

71. Tarkista henkilötunnuksesi tarkistusmerkki.

72. Mikä on henkilötunnuksen 01012010-001X tarkistusmerkki X?

73. Mitkä ovat henkilötunnuksen 31121999-1xyB mahdollisia numeroita x ja y?

74. Keksi tulevaisuudessa syntyvälle lapselle mahdollinen henkilötunnus.

10 Sovellukset

- Miten julkisilla salaustiedoilla voidaan salata tietoa siten että ulkopuolisen on lähes mahdotonta purkaa salausta?
- Voiko matemaattisella kaavalla selvittää päivämäärästä, mikä viikonpäivä silloin on?

10.1 Esitiedot

Tässä kappaleessa käydään läpi muutamia määritelmiä ja lauseita, joita tarvitaan myöhemmin esiteltävissä sovelluksissa. Ensin määritellään lattiafunktio, sitten Eulerin ϕ-funktio.

Määritelmä 10.1

Reaaliluvun x lattiafunktio $\lfloor x \rfloor$ on suurin kokonaisluku, joka on pienempi tai yhtä suuri kuin luku x. Siis

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

Esimerkki 10.1

Selvästi $\lfloor \frac{3}{2} \rfloor = 1$, $\lfloor \frac{-3}{2} \rfloor = -2$, $\lfloor \pi \rfloor = 3$, $\lfloor -5 \rfloor = -5$ ja $\lfloor 0 \rfloor = 0$.

Määritelmä 10.2: Eulerin ϕ-funktio

Olkoon n positiivinen kokonaisluku. *Eulerin funktio* $\phi(n)$ on niiden positiivisten, korkeintaan luvun n suuruisten kokonaislukujen lukumäärä, joiden suurin yhteinen tekijän luvun n kanssa on 1.

Esimerkki 10.2

Paljonko on $\phi(8)$?

Tutkitaan suurimpia yhteisiä tekijöitä luvun 8 ja lukujen $1-7$ välillä. Saadaan $\text{syt}(2,8) = \text{syt}(6,8) = 2$, $\text{syt}(4,8) = 4$ ja $\text{syt}(1,8) = \text{syt}(3,8) = \text{syt}(5,8) = \text{syt}(7,8) = 1$. Siis $\phi(8) = 4$.

Lause 10.1

Kun luku p on alkuluku, niin $\phi(p) = p - 1$.

Todistus (vrt. [4, s. 331]). Lukuja, jotka ovat lukua p pienempiä, on $p - 1$ kappaletta. Koska p on alkuluku, niin sillä ei ole muita tekijöitä kuin luku 1 ja se itse ja sen takia $\text{syt}(p, a) = 1$ kaikilla $0 < a < p$. Siis $\phi(p) = p - 1$. □

Esimerkki 10.3

Paljonko on $\phi(23)$?

Koska 23 on alkuluku, niin $\phi(23) = 22$.

Lause 10.2: Eulerin lause

Olkoon $\text{syt}(x, n) = 1$. Tällöin

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$

Todistus on hyvin samankaltainen kuin Fermat'n pienen lauseen todistus. Sen voi katsoa esimerkiksi [4][s. 332].

10.2 RSA-salaus

Viestien salauksessa ongelmana on ollut, että salauksen lähettäjän sekä vastaanottajan tulee kummankin tietää salauksen purkamiseen vaadittavat tiedot, ja tietoja vaihtaessa myös ulkopuolinen voi saada samat tiedot. Vuonna 1976 Stanfordin yliopistossa kehitettiin julkisen avaimen salaus, joka mahdollistaa salauksen avaimen julkistamisen, ja silti ulkopuolisen on äärimmäisen vaikeaa purkaa koodia.

Perusidea on, että viestin lähettäjä i näkee vastaanottajan j julkisen avaimen E_j, mutta vain j tietää oman salaisen purkuavaimensa D_j. Nämä avaimet toimivat viesteille käänteisfunktioina, joten viestille M $M = E(D(M)) = D(E(M))$. Kun henkilö i haluaa lähettää viestin M_i henkilölle j, hän kätkee viestin julkisella avaimella $E_j(M_i) = K$, jolloin saadaan salattu koodi K. Vain vastaanottaja itse tietää salaisen purkuavaimensa, ja pystyy sitä käyttämällä purkamaan koodin $D_j(K) = D_j(E_j(M_i)) = M_i$ ja lukemaan viestin M_i.

RSA-salaus kehitettiin 2 vuotta myöhemmin. Siinä käytetään julkista avainta, ja salaus tapahtuu kongruenssin, ja salauksen purkaminen Eulerin

funktion avulla. RSA:n julkinen avain on pari (n, e), missä n on kahden alkuluvun tulo, ja e valitaan siten että $\text{syt}(\phi(n), e) = 1$. Salaus tapahtuu kaavalla

$$K = E(M) \equiv M^e \pmod{n},$$

missä $0 < K < n$.

Salaiseksi avaimeksi valitaan d siten että $de \equiv 1 \pmod{\phi(n)}$, eli $de = 1 + k\phi(n)$ jollakin kokonaisluvulla k. Nyt

$$K^d \equiv (M^e)^d = M^{ed} = M^{1+k\phi(n)} = M \cdot (M^{\phi(n)})^k \equiv M \cdot 1^k = M \pmod{n},$$

kun Eulerin lauseen perusteella $M^{\phi(n)} \equiv 1 \pmod{n}$, jos $\text{syt}(M, n) = 1$. On hyvin epätodennäköistä, että $\text{syt}(M, n) \neq 1$, mutta vaikka näin olisi, niin silti $K^d \equiv M \pmod{n}$ (ks. lähde). [4][s. 417-421]

Esimerkki 10.4

Muodosta julkinen ja salainen avain, kun $n = 7 \cdot 23 = 161$.

Huomataan, että lauseen 10.1 perusteella $\phi(161) = \phi(7 \cdot 23) = 6 \cdot 22 = 132$. Voidaan valita $e = 5$, sillä $\text{syt}(\phi(161), 5) = \text{syt}(132, 5) = 1$. Julkinen avain on siis $(161, 5)$.

Salainen avain on jokin d, jolle pätee $1 = 5d - k132$ jollakin kokonaisluvulla k. Huomataan, että kun $k = 2$, niin $1 = 5d - 264$ eli $5d = 265$, jolloin salainen avain $d = 53$.

Tässä esitellään yksinkertaistettuja esimerkkejä RSA-salauksesta, ja näissä esimerkeissä salaus on helppo purkaa. Käytännössä salausta on vaikea purkaa sen takia, koska salauksessa käytetyt alkuluvut p ja q ovat niin suuria, sata numeroa pitkiä, että luvun $n = pq$ tekijöihinjako on hankalaa.

Esimerkki 10.5

Salaa RSA-salauksella yllätysjuhlien päivämäärä 1.3. Julkinen avain on $(161, 5)$.

Muodostetaan päivämäärästä luku, joka on $0103 = 103$. Salataan viesti kaavalla $K \equiv M^e \pmod{n}$, jolloin

$$K = 103^5 \equiv 143 \pmod{161}$$

eli lähetettävä viesti on 143.

Esimerkki 10.6

Saat viestin ystävältäsi: "Yllätysjuhlien päivämäärä on kätketty koodiin 143."Milloin yllätysjuhlat pidetään? Tiedät, että salainen avain on $(161, 53)$.

Nyt $d = 53$, joten

$$\begin{aligned} M = K^d &= 143^{53} = 143^{2\cdot 26+1} = (143^2)^{26} \cdot 143 \\ &\equiv (2)^{26} \cdot 143 \equiv 39 \cdot 143 = 5577 \equiv 103 \pmod{161} \end{aligned}$$

eli alkuperäinen viesti oli 103, joten yllätysjuhlat pidetään 1.3.

10.3 Laskukaava viikonpäivän selvittämiseksi

Historiaa 3: Nykyinen kalenteri

Egyptiläisessä kalenterissa vuoden pituus oli 365 päivää. Julius Ceasar muutti vuoden pituudeksi 365,25 päivää, ja aloitti karkausvuoden käytännön. Tiedetään kuitenkin, että vuosi on tarkemmin 365,2422 päivää. Vuoteen 1582 mennessä oli kertynyt noin 10 ylimääräistä päivää, ja paavi Gregory päätti korjata tilanteen. Ensin päivämäärä vaihdettiin niin, että 4.10.1582 jälkeen seuraava päivä oli 15.10.1582. Tämän jälkeen karkausvuosia pidettiin edelleen neljän vuoden välein, mutta poikkeuksiksi päätettiin vuosisadan vaihtumiset, jotka ovat karkausvuosia vain silloin, kun ne ovat jaollisia luvulla 400. Siis vuodet 1700, 1800, 1900 ja 2100 eivät ole karkausvuosia, mutta 1600 ja 2000 ovat. Tällä järjestelyllä vuoden keskimääräiseksi pituudeksi saadaan 365,2425 päivää, joten ylimääräisiä päiviä kertyy 10 000 vuodessa vain 3.

Gregorian kalenteria ei otettu kaikkialla käyttöön heti vuonna 1582. Britanniassa se otettiin käyttöön vuonna 1752, Japanissa 1873, Venäjällä ja esimerkiksi Suomessa 1917 ja Kreikassa viimeisenä vuonna 1923. [7, s. 179-180]

Muodostamme kaavan, jolla voi kongruenssia hyväksikäyttämällä laskea, mikä viikonpäivä on tiettynä päivämääränä.

Käytetään seuraavia merkintöjä:

- n = päivä (1-31)
- k = kuukausi $(1 - 12)$, tässä kaavassa 1 = maaliskuu, 2 =huhtikuu, ..., 10 =joulukuu, 11 =tammikuu ja 12 = helmikuu, jotta mahdollinen

karkauspäivä on vuoden viimeinen päivä.

- V = vuosi, ja $V = 100C + Y$, missä C = vuosisata ja Y = vuodet vuosisadan päälle. Koska tammi- ja helmikuu ovat tässä kaavassa vuoden viimeiset kuukauden, niiden vuosiluvusta vähennetään yksi.

Esimerkki 10.7

Tätä kirjoittaessa on päivämäärä 29.1.2015, joten $n = 29$, $k = 11$ ja $V = 2015 - 1 = 2014$, eli $C = 20$ ja $Y = 14$.

Viikonpäiviä on seitsemän, ja vuodessa on 365 päivää, paitsi karkausvuosina 366. Vuodessa muutos viikonpäivälle on kongruenssin $365 \equiv 1 \pmod 7$ perusteella $+1$, joten koska tänään on torstai, niin ensi vuonna tämä päivämäärä tulee olemaan perjantai. Kun merkitään, että sunnuntai $= 0$, maanantai $= 1, \ldots,$ ja lauantai $= 6$, niin saadaan, että $p_V \equiv p_{V-1} + 1 \pmod 7$. Karkausvuonna kongruenssin $366 \equiv 2 \pmod 7$ perusteella vastaavasti $p_V \equiv p_{V-1} + 2 \pmod 7$, kun V on karkausvuosi. Laskukaavassammehan karkauspäivä on edellisen vuoden viimeinen päivä.

Laskukaava alkaa päivämäärästä 1.3.1600. Aluksi halutaan laskea karkausvuosien määrä halutun vuoden ja vuoden 1600 välissä. Karkausvuosia (x) on ollut neljän vuoden välein $\frac{V-1600}{4} = \frac{(100C+Y)-1600}{4}$. Niistä vähennetään kuitenkin vuosisatojen määrä $C - 16$, mutta lisätään ne vuodet, jotka ovat jaollisia luvulla 400, eli $\frac{C-16}{4}$. Saadaan kaava

$$\begin{aligned} x &= \lfloor \frac{(100C + Y) - 1600}{4} \rfloor - (C - 16) + \lfloor \frac{C - 16}{4} \rfloor \\ &= 25C + \lfloor \frac{Y}{4} \rfloor - 400 - C + 16 + \lfloor \frac{C}{4} \rfloor - 4 \\ &= 24C + \lfloor \frac{C}{4} \rfloor + \lfloor \frac{Y}{4} \rfloor - 388 \\ &\equiv 3C + \lfloor \frac{C}{4} \rfloor + \lfloor \frac{Y}{4} \rfloor + 4 \pmod 7 \end{aligned}$$

Aiemmin todettiin, että $p_V \equiv p_{V-1} + 1 \pmod 7$ ja karkausvuonna $p_V \equiv p_{V-1} + 2 \pmod 7$. Nyt näitä käyttäen muodostetaan kaava, jossa verrataan vuoteen 1600, ja lisätään karkausvuosien tuomat päivät, jolloin

$$\begin{aligned} p_V &\equiv p_{1600} + (V - 1600) + x \pmod 7 \\ &= p_{1600} + ((100C + Y) - 1600) + (3C + \lfloor \frac{C}{4} \rfloor + \lfloor \frac{Y}{4} \rfloor + 4) \pmod 7 \\ &\equiv p_{1600} + ((2C + Y) - 4) + 3C + \lfloor \frac{C}{4} \rfloor + \lfloor \frac{Y}{4} \rfloor + 4 \pmod 7 \end{aligned}$$

$$\equiv p_{1600} + 5C + \lfloor \frac{C}{4} \rfloor + Y + \lfloor \frac{Y}{4} \rfloor \pmod 7$$

Tiedetään, että 1.3.1600 oli keskiviikko, eli voidaan korvata $p_{1600} \equiv 3 \pmod 7$, joten $p_V \equiv 3 + 5C + \lfloor \frac{C}{4} \rfloor + Y + \lfloor \frac{Y}{4} \rfloor \pmod 7$. Nyt kaava kertoo viikonpäivän joka vuoden ensimmäisenä päivänä, joka tässä tapauksessa on 1.3.

Vielä täytyy lisätä kaavaan vuoden muut päivät. Aloitetaan kuukausista. Koska maaliskuussa on 31 päivää ja $31 \equiv 3 \pmod 7$, niin $p_{huhti} \equiv p_{maalis} + 3 \pmod 7$ ja koska huhtikuussa on 30 päivää, niin $p_{touko} \equiv p_{huhti} + 2 = p_{maalis} + 5 \pmod 7$ jne. Saadaan lopuksi, että $p_{helmi} \equiv p_{maalis} + 29 \pmod 7$. Kun lasketaan keskimääräinen muutos kuukausien välillä, saadaan $\frac{29}{11} = 2,6$, jolloin saadaan $d_k = \lfloor d_{k-1} + 2,6 \rfloor$. Tarkemman tuloksen on kokeilemalla selvittänyt Reveran Zeller ja se on $\lfloor (2,6k - 0,2) \rfloor - 2$.

Nyt kaava kertoo jo kuukauden ensimmäisen päivän viikonpäivän. Kuukauden toinen päivä saadaan lisäämällä 1, kuukauden kolmas päivä lisäämällä 2 jne. Siis päiväys kuukauden sisällä saadaan lisäämällä kaavaan $n - 1$.

Kokonaisuudessaan kaava on:

$$\begin{aligned} p_V &\equiv 3 + 5C + \lfloor \frac{C}{4} \rfloor + Y + \lfloor \frac{Y}{4} \rfloor + \lfloor (2,6k - 0,2) \rfloor - 2 + n - 1 \pmod 7 \\ &= 5C + \lfloor \frac{C}{4} \rfloor + Y + \lfloor \frac{Y}{4} \rfloor + \lfloor (2,6k - 0,2) \rfloor + n \pmod 7 \end{aligned}$$

Esimerkki 10.8

Millä viikonpäivällä käynnistyi vuosituhat 2000?

Vuosituhannen ensimmäinen päivä oli 1.1.2000. Siis $n = 1$, $k = 11$ ja $v = 2000 - 1 = 1999$, eli $c = 19$ ja $y = 99$. Nyt

$$\begin{aligned} p_{1.1.2000} &\equiv 5 \cdot 19 + \lfloor \frac{19}{4} \rfloor + 99 + \lfloor \frac{99}{4} \rfloor + \lfloor (2,6 \cdot 11 - 0,2) \rfloor + 1 \pmod 7 \\ &= 95 + \lfloor 4,75 \rfloor + 99 + \lfloor 24,75 \rfloor + \lfloor 28,4 \rfloor + 1 \\ &= 195 + 4 + 24 + 28 \\ &= 251 \\ &\equiv 6 \pmod 7 \end{aligned}$$

Päivä 1.1.2000 oli lauantai.

10.4 Tehtäviä

75. Laske a) $\lfloor \frac{1}{5} \rfloor$ b) $\lfloor \frac{-4}{7} \rfloor$ c) $\lfloor \lfloor \frac{3}{4} \rfloor + \lfloor \frac{3}{4} \rfloor \rfloor$ d) $\lfloor -1 + \lfloor \frac{4}{3} \rfloor \rfloor$

76. Laske a) $\phi(18)$ b) $\phi(21)$.

77. Näytä, että jos $\text{syt}(x, n) = 1$, niin $x^{\phi(n)+1} \equiv x \pmod{n}$. [1][s.135]

78. a) Muodosta julkinen ja salainen avain, kun $n = 5 \cdot 7 = 35$. b) Salaa viesti $M = 2$. c) Pura b-kohdan viesti.

79. Luvut 61 ja 67 ovat alkulukuja. Muodosta niistä n ja laske $\phi(n)$. Valitse myös sopiva e, sekä julkinen ja salainen avain.

80. Salaa viesti 146, kun $n = 731$ ja $e = 13$.

81. Tarkista, että laskukaava viikonpäivän selvittämiseksi toimii, käyttämällä tämän hetkistä päivämäärää.

82. Laske kaavaa käyttämällä minä viikonpäivänä olet syntynyt.

83. Laske minä viikonpäivänä Suomesta tuli itsenäinen.

84. Käyttäen kaavaa $d_N \equiv p_{1600} + 5C + \frac{C}{4} + Y + \frac{Y}{4} \pmod{7}$, tarkista, että p_{1600} oli tosiaan keskiviikko.

11 Tehtävien vastaukset

1. a) $1+2+4+7+14 = 28$ b) $1+2+4+5+10+20+25+50 = 117 \neq 100$
2. $6 = 1 + 2 + 3$
3. a ja b
4. $a = \pm 1$, $a = \pm 2$, $a = \pm 3$ tai $a = \pm 6$
5. a) väärin b) oikein
6. a) $58 = 8 \cdot 7 + 2$ b) $84 = 14 \cdot 6$ c)$150 = 13 \cdot 11 + 7$
7. Kyllä voi
8. X=8, Y=5
9. -
10. -
11. a) väärin b) väärin
12. -
13. -
14. Pariton n on muotoa $n = 2m + 1$, jolloin saadaan $4 \mid (4m^2 + 4m - 8)$. Täytyy vielä todistaa, että $2 \mid (m^2 + m - 4)$.
15. a) 262209 b) 373
16. a) 69 b) 43692
17. a) 1100100_2 b) 64_{16}
18. 333_8
19. 1101111001_2
20. 11-järjestelmässä
21. 4-järjestelmässä
22. $0 = 0000$, $1 = 0001$, ... , $F = 1111$
23. 11111010000101001100
24. Esimerkiksi binäärien jakaminen ketjuihin, saadaan 4-järjestelmä, 8-järjestelmä, 32-järjestelmä jne.

25. a) 101111 b) 1000001101

26. Ainoastaan luku 2.

27. a) väärin b) väärin

28. a) $63 = 3^2 \cdot 7$ b) $129 = 3 \cdot 43$ c) $154 = 2 \cdot 7 \cdot 11$

29. a) $1155 = \cdot$ b) $1386\cdot$ c) $11800\cdot$

30. a) on b) ei c) ei

31. Alkulukuja ovat 53, 59, 61, 67, 71, 73, 79, 83, 89 ja 97.

32. -

33. a) $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ ja $M_7 = 127$ b) $M_{11} = 23 \cdot 89$ c) Esimerkiksi luku 5 ei ole Mersennen luku.

34. $a = b = 4$

35. 102 vuotta

36. Luku a on aina jaollinen luvulla 2.

37. -

38. a) 3003 b) 1040

39. 2

40. 12

41. a) $\frac{321}{1027}$ b) $\frac{1093}{2458}$ c) $\frac{79}{131}$

42. Kolmen vuorokauden, 1 tunnin ja 30 minuutin kuluttua

43. Ei

44. 3 ja 645 tai 15 ja 129

45. 140 ja 9800 tai 280 ja 4900 tai 700 ja 1960 tai 980 ja 1400

46. -

47. -

48. a) Kello on 05:00, koska $221 \equiv 5 \pmod{24}$. b) Kello on 13:00, sillä $1141 \equiv 13 \pmod{24}$.

49. a) Kyllä, sillä $184 \equiv 100 \pmod{12}$ b) Ei, sillä $184 \not\equiv 100 \pmod{24}$

50. -

51. a) $x = 6$ b) $x = 4$ c) $x = 7$

52. $n = 3$ tai $n = 11$

53. a) 6 b) 4 c) 3

54. a) 9 b) 5 c) 7

55. -

56. Koska $(a-c)-(b-c) = (a-b)$ ja $m \mid (a-b)$, niin $m \mid ((a-c)-(b-c))$, eli $a - c \equiv b - c \pmod{m}$.

57. Kuten luvun 2 jaollisuustesti

58. Kuten luvun 4 jaollisuustesti

59. Kuten luvun 3 jaollisuustesti

60. a) 3 b) 0

61. 12

62. -

63. 7 kpl, $[0]_m$-$[6]_m$

64. $[-14]_7 = [2]_7 = [10]_7$

65. a) kyllä b) ei

66. $m = 5$ tai $m = 10$

67. a) $[a + b]_m$ b) $[ab]_m$

68. -

69. a) ei b) on c) ei

70. a) 11110 b) 1010101101

71. -

72. X=U

73. xy= 16 tai xy= 47 tai xy= 78

74. Esimerkiksi 10122025-100N

75. a) 0 b) -1 c) 0 d) 0

76. a) 6 b) 12

77. Eulerin lauseen nojalla

78. a) Julkinen avain voi olla esimerkiksi $(35, 5)$ ja salainen esimerkiksi $d = 5$. b) $K = 32$

79. $n = 4087$ ja $\phi(n) = 3960$

80. 572

81. -

82. -

83. Torstaina

84. -

Viitteet

[1] Anne-Maria Ernvall-Hytönen, Kerkko Luosto, Tapio Pokela, *Pyramidi 11: Lukuteoria ja logiikka*, 1st edition, Tammi, 2006.

[2] Markku Halmetoja, Kaija Häkkinen, Jorma Merikoski, Lauri Pippola, Harry Silvferberg, Timo Tossavainen, Teuvo Laurinolli, Keijo Väänänen *Matematiikan taito 11: Lukuteoria ja logiikka*, 1st edition, WSOY, 2006.

[3] Tarmo Hautajärvi, Jukka Ottelin, Leena Wallin-Jaakkola, *Laudatur 11: Lukuteoria ja logiikka*, 1st edition, Otava, 2006.

[4] Thomas Koshy, *Elementary Number Theory with Applications*, 1st edition, Harcourt/Academic Press, 2002.

[5] Erkki Luoma-Aho, *Matematiikan peruskäsitteiden historia*, http://solmu.math.helsinki.fi/2010/kasitehist/AlgebraJaAritmetiikka.pdf

[6] Tomas Oliveira e Silva, *Goldbach conjecture verification*, http://sweet.ua.pt/tos/goldbach.html

[7] Kenneth H. Rosen, *Elementary Number Theory and its Applications*, 4th edition, Addison Wesley Longman, 2000.

[8] Kenneth H. Rosen, *Elementary Number Theory and its Applications*, 5th edition, Pearson, 2005.