TAMPEREEN YLIOPISTO
Filosofian maisterin tutkielma

Tiina Vuorimaa

Kongruenssin sovelluksia

Matematiikan, tilastotieteen ja filosofian laitos
Matematiikka
Toukokuu 2006

Tampereen yliopisto
Matematiikan, tilastotieteen ja filosofian laitos
Vuorimaa, Tiina: Kongruenssin sovelluksia
Pro gradu -tutkielma, 24 s.
Matematiikka Toukokuu 2006

Tiivistelmä

Tässä työssä seurataan ensisijaisesti Thomas Koshyn kirjaa Elementary Number Theory with Applications. Monipuolisuuden vuoksi rinnalla on käytetty joissain kohdin myös Kenneth Rosenin kirjaa Elementary Number Theory and its Applications. Tämä työn pohjana on kokonaislukujen jaollisuus. Kappaleissa 1-3 on esitelty kaikki tarvittavat esitiedot. Kappaleessa 1 on todistettu jaollisuuden peruslauseita. Kappaleen 2 jakoalgoritmi perustuu jaollisuuteen. Siinä käydään läpi termit jaettava, jakaja, jakojäännös ja osamäärä sekä niiden osallisuus jaollisuudessa. Kappaleessa 3 määritellään lattiafunktio, joka on kattofunktion sukulainen. Lattiafunktiota käytetään ikikalenterissa. Lattiafunktio antaa annetusta reaaliluvusta suurimman kokonaisluvun, joka on yhtäsuuri tai pienempi, kuin kyseinen reaaliluku. Neljäs kappale esittelee kongruenssin. Kappale 5 sisältää monia kongruenssin sovelluksia. Alussa on erilaisia jaollisuustestejä. Jaollisuus kymmenjärjestelmässä luvuilla $10, 5, 2^i, 5^i, 3, 9, 11, 7$ ja 13 sekä eräillä luvuilla b-kantaisessa esityksessä. Suurin yksittäinen sovellus on ikikalenteri, jossa voidaan määrittää viikonpäivä halutulle päivämäärälle vuodesta 1600 eteenpäin. Muita sovelluksia ovat turnausaikataulun laatiminen sekä kuningattarien asettaminen pxp -shakkilaudalle, missä p on alkuluku.

Sisältö

Johdanto **1**

1 Jaollisuus **2**

2 Jakoalgoritmi **3**

3 Lattiafunktio **4**

4 Kongruenssi **5**

5 Kongruenssin sovelluksia **7**
5.1 Jaollisuustestejä 7
5.1.1 Jaollisuustesti luvulle 10 7
5.1.2 Jaollisuustesti luvulle 5 7
5.1.3 Jaollisuustesti luvulle 2^i 7
5.1.4 Jaollisuustesti luvulle 5^i 8
5.1.5 Jaollisuustesti luvuille 3 ja 9 8
5.1.6 Jaollisuustesti luvulle 11 8
5.1.7 Jaollisuustesti yhdessä luvuille $7, 11$ ja 13 9
5.1.8 Numerosumma modulo 9 11
5.1.9 Redusoitu numerosumma 12
5.2 Ikikalenteri 13
5.3 Turnausaikataulu 17
5.4 Kuningatarpulma 21

Viitteet **24**

Johdanto

Tässä työssä seurataan ensisijaisesti Thomas Koshyn kirjaa Elementary Number Theory with Applications. Monipuolisuuden vuoksi rinnalla on käytetty joissain kohdin myös Kenneth Rosenin kirjaa Elementary Number Theory and its Applications.

Kokonaislukujen joukkoa merkitään symbolilla $\mathbf{Z}$. Kaikki tämän tutkielman luvut ovat kokonaislukuja ellei toisin mainita. Lukijalta edellytetään kokonaisluvun käsitteen muistamista sekä peruslaskutoimitusten hallintaa. Muut kongruenssin sovelluksissa vastaan tulevista laskutoimituksista on esitelty kappaleissa 1 - 4.

Luvun 5 alku käsittelee jaollisuustestejä. Niissä selvitetään kuinka pystyy helposti tarkistaa onko jokin kokonaisluku jaollinen kyseisellä luvulla. Luvun 5 loppuosassa on kolme ongelman ratkaisua. Ensin luodaan ikikalenteri, jolla voidaan selvittää esimerkiksi viikonpäivä milletahansa päivämäärälle vuodesta 1600 eteenpäin. Kuningatarpulma ja turnausaikataulu liittyvat toisiinsa. Kuningatarpulmassa asetetaan $p \cdot p$ -shakkilaudalle p kappaletta kuningattaria siten, että ne eivät voi lyodä toisiaan. Luku p on alkuluku eli se on luku, joka on jaollinen vain luvulla 1 ja itsellään. Alkulukuja ovat esimerkiksi $2, 3, 5, 7$ ja 11. Turnausaikataulussa ratkaistaan kuinka monta ottelua turnauksessa pitää otella, jotta jokainen turnaukseen osallistuva joukkue pelaa tasan kerran jokaista muuta joukkuetta vastaan.

1 Jaollisuus

Monet kokonaisluvut voidaan esittää pienempien kokonaislukujen tulona.

Määritelmä 1.1 *Luku a on luvun b* monikerta*, jos $a = bm$, missä a, b, $m \in \mathbf{Z}$. Sanotaan myös, että luku a on luvun b* tekijä *tai että luku a* jakaa *luvun b. Jos luku a jakaa luvun b, merkitään $a \mid b$. Muutoin $a \not\mid b$. Edelleen, jos $a \neq 0$ ja $a \mid b$, niin $m = b/a$.*

Lause 1.1 *Olkoot a, b ja c kokonaislukuja ja $\neq 0$. Silloin*
(a) *$a \mid a$,*
(b) *$a \mid b$ ja $b \mid c \Rightarrow a \mid c$,*
(c) *$b \mid a$ ja $b \mid c \Leftrightarrow b \mid (ma + nc)$, missä $m, n \in \mathbf{Z}$.*

Todistus.
(a) Selvästi $a = a \cdot 1$. Koska $1 \in \mathbf{Z}$, niin $a \mid a$.
(b) Jos $a \mid b$ ja $b \mid c$, niin voidaan merkitä, että $b = am$ ja $c = bn$, missä $m, n \in \mathbf{Z}$. Siis $c = bn = (am)n = a(mn)$ ja mn $\in \mathbf{Z}$. Näin ollen $a \mid c$.
(c) Oletetaan, että $b \mid a$ ja $b \mid c$. Silloin voidaan merkitä, että $a = bp$ ja $c = bq$, missä $p, q \in \mathbf{Z}$. Siis $ma + nc = m(bp) + n(bq) = b(mp + nq)$. Silloin $b \mid (ma + nc)$.
Toisaalta oletetaan, että $b \mid (ma + nc)$, $m, n \in \mathbf{Z}$. Silloin jos $m = 1$ ja $n = 0$, saadaan, että $b \mid a$. Toisaalta, jos $m = 0$ ja $n = 1$, saadaan, että $b \mid c$.
Lause 1.1 on todistettu. □

Lause 1.2 *Jos a ja b ovat positiivisia kokonaislukuja ja $a \mid b$, niin $a \leq b$.*

Esimerkki 1.1 Koska $21 = 7 \cdot 3$, niin $7 \mid 21$. Koska $24 = 6 \cdot 4$, niin $6 \mid 24$. Koska ei ole olemassa sellaista kokonaislukua m, että $12 = 5 \cdot m$, niin $5 \not\mid 12$.

Apulause 1.1 *Jos a, $b \in \mathbf{Z}^+$ sekä $a \mid b$ ja $b \mid a$, niin $a = b$.*

Lause 1.3 *Jos $a \mid b$ ja $b \mid a$, niin $a = b$ tai $a = -b$.*

Todistus. Jos $a > 0$ ja $b > 0$, niin apulauseen 1.1 mukaan $a = b$
Jos $a < 0$ ja $b > 0$. Silloin $-a > 0$ ja $(-a) \mid b$ ja $b \mid (-a)$. Silloin apulauseen 1.1 mukaan $b = -a$ eli $a = -b$.

Tapaus, jossa $a > 0$ ja $b < 0$, menee samoin kuin edellinen.
Jos $a < 0$ ja $b < 0$, niin $-a > 0$ ja $-b > 0$. Silloin $(-a) \mid (-b)$ ja $(-b) \mid (-a)$. Silloin apulauseen 1.1 mukaan $-a = -b$ eli $a = b$.
Lause 1.3 on todistettu. □

2 Jakoalgoritmi

Lause 2.1 *Jos a ja b ovat kokonaislukuja siten, että $b > 0$, niin on olemassa sellaiset yksikäsitteiset ei-negatiiviset kokonaisluvut q ja r, että $a = bq + r$, missä $0 \leq r < b$. Lukua q kutsutaan osamääräksi, luku r on jakojäännös, luku a jaettava ja luku b jakaja.*

Todistus. Käsitellään muotoa $a - bk$, missä k on kokonaisluku, olevien kokonaislukujen joukkoa S. Siis $S = \{a - bk \mid k \in \mathbf{Z}\}$. Olkoon joukon S ei-negatiivisten kokonaislukujen osajoukkojoukko T. Joukko T on epätyhjä, koska $a - bk$ on positiivinen aina kun kokonaisluku $k < a/b$.
Hyvinjärjestys-periaatteen mukaan joukossa T on pienin alkio $k = q$. Asetetaan, että $r = a - bq$. Tiedetään, että $r \geq 0$ ja $r < b$. Jos $r \geq b$, niin $r > r - b = a - bq - b = a - b(q + 1) \geq 0$, joka on ristiriita valinnalle, että $r = a - bq$ on pienin ei-negatiivinen kokonaisluku. Siksi $0 \leq r < b$.
Osoitetaan, että nämä arvot luvuille q ja r ovat yksikäsitteisiä. Oletetaan, että on kaksi yhtälöä $a = bq_1 + r_1$ ja $a = bq_2 + r_2$, missä $0 \leq r_1 < b$ ja $0 \leq r_2 < b$. Vähentämällä toinen yhtälö ensimmäisestä saadaan, että $0 = b(q_1 - q_2) + (r_1 - r_2)$. Tästä nähdään, että $r_2 - r_1 = b(q_1 - q_2)$. Tämä kertoo, että luku b jakaa luvun $r_2 - r_1$. Koska $0 \leq r_1 < b$ ja $0 \leq r_2 < b$ saadaan, että $-b < r_2 - r_1 < b$. Tästä johtuen b voi jakaa luvun $r_2 - r_1$ vain jos $r_2 - r_1 = 0$ eli jos $r_1 = r_2$. Huomataan myös, että $q_1 = q_2$. Tämä osoittaa, että osamäärä q ja jakojäännös r ovat yksikäsitteisiä.
Lause 2.1 on todistettu. □

Huomataan, että luku a on jaollinen luvulla b, jos ja vain jos jakoalgoritmin jakojäännös on 0.

Esimerkki 2.1 Jos $a = 156$ ja $b = 35$, niin $q = 4$ ja $r = 16$ koska $156 = 35 \cdot 4 + 16$. Samoin jos $a = -100$ ja $b = 7$, niin $q = -15$ ja $r = 5$ koska $-100 = 7(-15) + 5$.

Esimerkki 2.2 Selvästi $4 = 7 \cdot 0 + 4$, missä $a = 4$, $b = 7$, $q = 0$ ja $r = 4$. Samoin $13 = 5 \cdot 2 + 3$, missä $a = 15$, $b = 5$, $q = 2$ ja $r = 3$.

Esimerkki 2.3 Mitä kymmenjärjestelmän luku $(173)_{10}$ on 8 -järjestelmässä? Ratkaisu jakoalgoritmin perusteella: $173 = 8 \cdot 21 + 5 = 8(8 \cdot 2 + 5) + 5 = 2 \cdot 8^2 + 5 \cdot 8 + 5$. Siis $(173)_{10} = (255)_8$.

3 Lattiafunktio

Ennen kuin määritellään täsmällinen muoto osamäärälle ja jakojäännökselle tarvitaan seuraava määritelmä.

Määritelmä 3.1 *Suurin kokonaisluku reaaliluvussa x merkitään $\lfloor x \rfloor$, joka tarkoittaa suurinta kokonaislukua, joka on pienempi tai yhtäsuuri kuin x. Nyt $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.*

Merkintä: Lattiafunktiolle käytetään merkinnän $\lfloor x \rfloor$ sijasta myös merkintää $[x]$. Kattofunktio on lattiafunktion sukulainen. Kattofunktio reaaliluvusta x, merkitään $\lceil x \rceil$, on pienin kokonaisluku, joka on suurempi tai yhtäsuuri kuin x. Esimerkiksi $\lceil 7/2 \rceil = 4$ ja $\lceil -7/2 \rceil = -3$.

Esimerkki 3.1 Määritelmän mukaan $\lfloor 3 \rfloor = 3$, $\lfloor -2 \rfloor = -2$, $\lfloor 6/4 \rfloor = 1$, $\lfloor 9/4 \rfloor = 2$ ja $\lfloor -9/4 \rfloor = -3$.

Esimerkki 3.2 Osoitetaan, että jos n on mielivaltainen kokonaisluku, niin $\lfloor x + n \rfloor = \lfloor x \rfloor + n$, missä x on mielivaltainen reaaliluku. Olkoon $\lfloor x \rfloor = m$, jolloin m on kokonaisluku. Tästä seuraa, että $m \leq x < m + 1$. Epäyhtälöön voidaan lisätä puolittain kokonaisluku n, jolloin saadaan, että $m + n \leq x + n < m + n + 1$. Tämä epäyhtälö osoittaa, että $m + n = \lfloor x \rfloor + n$ on suurin kokonaisluku, joka on pienempi tai yhtäsuuri kuin $x + n$. Tästä seuraa, että $\lfloor x + n \rfloor = \lfloor x \rfloor = n$.

Seuraavaksi käytetään lattiafunktiota määrittämään täsmällinen muoto osamäärälle ja jakojäännökselle. Koska osamäärä on suurin kokonaisluku siten, että $bq \leq a$, ja $r = a - bq$. Siitä seuraa, että

$$q = \lfloor a/b \rfloor \; ja \; r = a - b\lfloor a/b \rfloor. \tag{3.1}$$

Esimerkki 3.3 Olkoon $a = 589$ ja $b = 20$. Silloin $a = bq+r$, missä $0 \leq r < b$. Nyt $q = \lfloor 589/20 \rfloor = 29$ ja $r = 589 - \lfloor 589/20 \rfloor \cdot 20 = 589 - 29 \cdot 20 = 9$.

Esimerkki 3.4 Olkoon $a = -420$ ja $b = 19$. Silloin $a = bq + r$, missä $0 \leq r < b$. Nyt $q = \lfloor -420/19 \rfloor = -23$ ja $r = -420 - \lfloor -420/19 \rfloor \cdot 19 = -420 - (-23) \cdot 20 = 40$.

4 Kongruenssi

Määritelmä 4.1 *Olkoon m positiivinen kokonaisluku. Nyt kokonaisluku a on* kongruentti *luvun b kanssa modulo m jos $m \mid (a - b)$. Jos a ei ole kongruentti modulo m, niin se on* epäkongruentti *modulo m ja merkitään $a \not\equiv b (mod\, m)$.*

Lause 4.1 *$a \equiv b (mod\, m)$, jos ja vain jos $a = b+km$ jollakin kokonaisluvulla k.*

Todistus. Oletetaan, että $a \equiv b (mod\, m)$. Silloin $m \mid (a - b)$, siis $a - b = km$ jollakin kokonaisluvulla k. Tästä seuraa, että $a = b + km$.
Toisaalta oletetaan, että $a = b + km$, jollakin kokonaisluvulla k. Silloin $a - b = km$ siis $m \mid (a - b)$ ja nyt $a \equiv b (mod\, m)$.
Lause 4.1 on todistettu □

Esimerkki 4.1 $56 \equiv 2 (mod\, 3)$ ja $56 = 2 + 18 \cdot 3$.

Esimerkki 4.2 Toisaalta $36 = -4 + 8 \cdot 5$ joten $36 \equiv -4 (mod\, 5)$.

Lause 4.2 *$a \equiv b (mod\, m)$, jos ja vain jos luvuista a ja b jää sama jakojäännös jaettaessa luvulla m.*

Todistus. Oletetaan, että $a \equiv b (mod\, m)$. Silloin lauseen 4.1 mukaan $a = b + km$ jollakin kokonaisluvulla k. Jakoalgoritmin mukaan $b = mq + r$, missä $0 \leq r < m$. Nyt $a = b + km = (mq + r) + km = m(q + k) + r$. Siis jakoalgoritmin mukaan luvusta a jää sama jakojäännös r jaettaessa luvulla m.
Toisaalta oletetaan, että sekä luvusta a että b jää sama jakojäännös r jaettaessa luvulla m. Taas jakoalgoritmin perusteella $a = mq + r$ ja $b = mq' + r$, missä $0 \leq r < m$. Nyt $a - b = (mq + r) - (mq' + r) = m(q - q')$ siis $a \equiv b (mod\, m)$.
Lause 4.2 on todistettu. □

Esimerkki 4.3 $34 \equiv 20(mod\,7)$. Molemmista luvuista 34 ja 20 jää jakojäännökseksi 6, kun luvut jaetaan luvulla 7. Toisaalta, kun luvut 35 ja 17 jaetaan luvulla 9 jakojäännökseksi jää 8. Siis $35 \equiv 17(mod\,9)$.

Lause 4.3 *Olkoon* $a \equiv b(mod\,m)$ *ja* $c \equiv d(mod\,m)$. *Silloin*

$$\begin{aligned} &(1) \quad a + c \equiv b + d(mod\,m) ja \\ &(2) \quad ac \equiv bd(mod\,m). \end{aligned}$$

Todistus. Koska $a \equiv b(mod\,m)$ ja $c \equiv d(mod\,m)$, $a = b+lm$ ja $c = d+km$ mielivaltaisilla kokonaisluvuilla l ja m. Silloin

$$\begin{aligned} (1)\ a + c &= (b + lm) + (d + km) \\ &= (b + d) + (l + k)m \\ &\equiv b + d(mod\,m) \end{aligned}$$

$$\begin{aligned} (2)\ ac - bd &= (ac - bc) + (bc - bd) \\ &= c(a - b) + b(c - d) \\ &= clm + bkm \\ &= (cl + bk)m \\ siis \quad &ac \equiv bd(mod\,m) \end{aligned}$$

Lause 4.3 on todistettu □

Esimerkki 4.4 On totta, että $21 \equiv -4(mod\,5)$ ja $34 \equiv 4(mod\,5)$. Nyt lauseen 4.3 mukaan $21 + 34 \equiv -4 + 4(mod\,5)$. Siis $55 \equiv 0(mod\,5)$. Myös $21 \cdot 34 \equiv (-4) \cdot 4(mod\,5)$. Siis $714 \equiv -16(mod\,5)$.

Lause 4.4 *Jos* a, b, k *ja* m *ovat sellaisia kokonaislukuja, että* $k > 0$, $m > 0$ *ja* $a \equiv b(mod\,m)$, *niin* $a^k \equiv b^k(mod\,m)$.

Todistus. Koska $a \equiv b(mod\,m)$, saadaan, että $m \mid (a - b)$ ja koska

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1}),$$

nähdään, että $(a - b) \mid (a^k - b^k)$. Näin ollen lauseesta 1.1 seuraa, että $m \mid (a^k - b^k)$. Täten $a^k \equiv b^k(mod\,m)$.
Lause 4.4 on todistettu. □

5 Kongruenssin sovelluksia

5.1 Jaollisuustestejä

Kongruenssin teoriaa käytetään kehittämään yksinkertaisia testejä tarkistamaan onko annettu kokonaisluku n jaollinen kokonaisluvulla m. Tässä kappaleessa esitellään muutama tällainen testi. Merkintä $n_2n_1n_0$ tarkoittaa kolminumeroista lukua. Esimerkiksi luku $n = 542$, $nyt\, n_2 = 5, n_1 = 4\, ja\, n_0 = 2$.

5.1.1 Jaollisuustesti luvulle 10

Koska $10 \equiv 0(mod\, 10)$, niin lauseiden 4.2 ja 4.3 perusteella $n \equiv n_0(mod\, 10)$. Silloin n on jaollinen luvulla 10, jos ja vain jos n_0 on jaollinen luvulla 10. Näin, jos ja vain jos $n_0 = 0$. Siis kokonaisluku on jaollinen luvulla 10, jos ja vain jos sen viimeinen numero on 0.

5.1.2 Jaollisuustesti luvulle 5

Koska $n \equiv n_0(mod\, 10)$, niin n on jaollinen luvulla 5, jos ja vain jos n_0 on jaollinen luvulla 5. Ainoat luvulla 5 jaolliset yksinumeroiset luvut ovat 0 ja 5. Siis kokonaisluku on jaollinen luvulla 5, jos ja vain jos se päättyy numeroon 0 tai 5.

5.1.3 Jaollisuustesti luvulle 2^i

Koska $10 \equiv 0(mod\, 2)$, niin $10^i \equiv 0(mod\, 2^i)$ kaikilla positiivisilla kokonaisluvuilla i. Nyt lauseiden 4.2 ja 4.3 mukaan saadaan:

$$\begin{aligned} n &\equiv n_0(mod\, 2) \\ &\equiv n_1n_0(mod\, 2^2) \\ &\equiv n_2n_1n_0(mod\, 2^3) \\ &\vdots \\ &\equiv n_{i-1}n_{i-2}\ldots n_0(mod\, 2^i). \end{aligned}$$

Siis kokonaisluku n on jaollinen luvulla 2^i, jos ja vain jos luvun n i viimeistä numeroa on jaollisia luvulla 2^i. Toisin sanoen kokonaisluku n on jaollinen luvulla $2(= 2^1)$, jos ja vain jos sen viimeinen numero n_0 on jaollinen luvulla 2, se on jaollinen luvulla $4(= 2^2)$ jos kaksinumeroinen luku n_1n_0 on jaollinen

luvulla 4 ja se on jaollinen luvulla $8(=2^3)$, jos kolminumeroinen luku $n_2n_1n_0$ on jaollinen luvulla 8. Jne.

Esimerkki 5.1 Olkoon $n = 4562076$. Koska $2|6$, niin $2|$n; $4|76$ niin $4|$n, mutta $8\not|076$, joten $8\not|$n.

5.1.4 Jaollisuustesti luvulle 5^i

Jaollisuustesti luvun 5 potensseille on analoginen jaollisuustestin luvun 2 potenssien kanssa. Huomataan, että koska $10 \equiv 0(mod\,5)$ saadaan, että $10^i \equiv 0(mod\,5^i)$. Näin ollen täytyy tarkistaa kokonaisluvun n i:n viimeisen numeron jaollisuus luvulla 5^i. Jos jako menee tasan, niin silloin luku n on jaollinen luvulla 5^i.

Esimerkki 5.2 Olkoon $n = 48126853125$. Koska $5 \mid 5$, niin $5 \mid n$. Koska $25 \mid 25$, niin $25 \mid n$. Koska $125 \mid 125$, niin $125 \mid n$. Koska $625 \mid 3125$, niin $625 \mid n$. Koska $3125 \mid 53125$, niin $3125 \mid n$. Koska $15625 \not| 853125$, niin $15625 \not| n$.

5.1.5 Jaollisuustesti luvuille 3 ja 9

Koska $10 \equiv 1(mod\,3)$, niin $10^i \equiv 1(mod\,3)$ lauseen 4.3 perusteella. Lauseen 4.2 mukaan $n \equiv n_n + n_{k-1} + \ldots + n_1 + n_0(mod\,3)$. Siis kokonaisluku n on jaollinen luvulla 3, jos ja vain jos sen numeroiden summma on jaollinen luvulla 3. Huomataan, että myös $10 \equiv 1(mod\,9)$. Samoin kuin luvun 3 kohdalla, koska $n \equiv n_k + n_{k-1} + \ldots + n_1 + n_0(mod\,9)$, niin kokonaisluku n on jaollinen luvulla 9, jos ja vain jos sen numeroiden summa on jaollinen luvulla 9.

Esimerkki 5.3 Olkoon $n = 234506076$. Sen numeroiden summa on $2+3+4+5+0+6+0+7+6 = 33$. Koska $3 \mid 33$, niin $3 \mid$ n, mutta $9 \not| 33$, niin $9 \not|$n.

5.1.6 Jaollisuustesti luvulle 11

Lauseen 4.2 mukaan $10 \equiv -1(mod\,11)$ ja $10^i \equiv (-1)^i(mod\,11)$. Toisaalta lauseen 4.1 mukaan $n \equiv (-1)^k n_k + \ldots - n_3 + n_2 - n_1 + n_0(mod\,11)$. Siis $11 \mid n$, jos ja vain jos $(n_0 + n_2 + \ldots) - (n_1 + n_3 + \ldots)$ on jaollinen luvulla 11. Toisin sanoen kokonaisluku n on jaollinen luvulla 11, jos ja vain jos luvun parillisten paikkojen numeroiden ja parittomien paikkojen numeroiden summien erotus on jaollinen luvulla 11.

Esimerkki 5.4 Olkoon $n = 243506076$. Etsitty erotus on $(2+3+0+0+6)-(4+5+6+7) = 11-22 = -11$. Koska $11 \mid -11, niin\, 11 \mid n$.

Lause 5.1 *Palindromiluku, jossa on parillinen määrä numeroita on jaollinen luvulla* 11.

Todistus. Olkoon $n = n_{2k-1}n_{2k-2}...n_1n_0$ palindromi, jossa on parillinen määrä numeroita. Nyt n $\equiv (n_0 + n_2 + ... + n_{2k-2}) - (n_1 + n_3 + ... + n_{2k-1})$ (mod 11) $\equiv 0$(mod 11), koska n on palindromi, jossa on parillinen määrä numeroita. Nyt $11 \mid$ n.
Lause 5.1 on todistettu. □

Lause 5.1 ei päde palindromeille, joissa on pariton määrä numeroita.

5.1.7 Jaollisuustesti yhdessä luvuille $7, 11$ ja 13

Huomataan, että $7 \cdot 11 \cdot 13 = 1001$ ja $10^3 = 1000 \equiv -1(mod\, 1001)$. Näin ollen

$$\begin{aligned}
(a_k a_{k-1} \dots a_0)_{10} &= a_k 10^k + a_{k-1}10^{k-1} + \dots + a_1 10 + a_0 \\
&\equiv (a_0 + 10a_1 + 100a_2) + 1000(a_3 + 10a_4 + 100a_5) + \\
&\quad 1000^2(a_6 + 10a_7 + 100a_8) + \dots \\
&\equiv (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + \\
&\quad (100a_8 + 10a_7 + a_6) - \dots \\
&= (a_2a_1a_0)_{10} - (a_5a_4a_3)_{10} + (a_8a_7a_6)_{10} - \dots (mod\, 1001).
\end{aligned}$$

Tämä kongruenssi osoittaa, että kokonaisluku on kongruentti modulo 1001, missä numerot ovat ryhmitelty alkaen oikean puoleisesta numerosta. Sen johdosta, koska 7, 11 ja 13 ovat luvun 1001 jakajia, määrittelyyn, onko kokonaisluku jaollinen luvuilla 7, 11 tai 13, tarvitsee tarkistaa onko kolmen numeron sarjojen vuorotteleva summa jaollinen luvulla 7, 11 tai 13.

Esimerkki 5.5 Olkoon $n = 65412351$. Koska kolmen numeron sarjoissa olevien kokonaislukujen vuorotteleva summa, $351-412+65 = 4$, ei ole jaollinen millään luvulla 7, 11 eikä 13, niin myöskään n ei ole jaollinen näillä luvuilla.

Esimerkki 5.6 Olkoon $n = 2033647$. Kolmen numeron sarjoissa vuorotteleva summa on $647 - 33 + 2 = 616$. Nyt $7 \mid 616$, joten $7 \mid n$. Myös $11 \mid 616$, joten $11 \mid n$, mutta $13 \not| 616$, silloin $13 \not| n$.

Kaikki jaollisuustestit, jotka tässä on esitetty perustuvat kymmenkantaesitykseen. Nyt kehitetään jaollisuustesti käyttämällä b-kanta esitystä, missä b on positiivinen kokonaisluku.

Lause 5.2 *Jos $d \mid b$ ja j ja k ovat positiivisia kokonaislukuja, missä $j < k$. Silloin $(a_k \dots a_1 a_0)_b$ on jaollinen luvulla d^j, jos ja vain jos $(a_{j-1} \dots a_1 a_0)_b$ on jaollinen luvulla d^j.*

Todistus. Koska $b \equiv 0 (mod\, d)$, siitä seuraa että $b^j \equiv 0 (mod\, d^j)$. Näin ollen

$$\begin{aligned}(a_k a_{k-1} \dots a_1 a_0)_b &= a_k b^k + \dots + a_j b^j + a_{j-1} b^{j-1} + \dots + a_1 b + a_0 \\ &\equiv a_{j-1} b^{j-1} + \dots + a_1 b + a_0 \\ &= (a_{j-1} \dots a_1 a_0)_b (mod\, d^j).\end{aligned}$$

Selvästi $d^j \mid (a_k a_{k-1} \dots a_1 a_0)_b$, jos ja vain jos $d^j \mid (a_{j-1} \dots a_1 a_0)_b$.
Lause 5.2 on todistettu. □

Lause 5.3 *Jos $d \mid (b-1)$, niin $n = (a_k \dots a_1 a_0)_b$ on jaollinen luvulla d, jos ja vain jos luvun n numeroiden summa $a_k + \dots + a_1 + a_0$ on jaollinen luvulla d.*

Todistus. Koska $d \mid (b-1)$, saadaan, että $b \equiv 1 (mod\, d)$. Nyt lauseen 4.4 perusteella saadaan, että $b^j \equiv 1 (mod\, d)$ kaikilla positiivisilla kokonaisluvuilla j. Siten $n = (a_k \dots a_1 a_0)_b = a_k b^k + \dots + a_1 b + a_0 \equiv a_k + \dots a_1 + a_0 (mod\, d)$. Tämä osoittaa, että $d \mid n$, jos ja vain jos $d \mid (a_k + \dots a_1 + a_0)$.
Lause 5.3 on todistettu. □

Lause 5.4 *Jos $d \mid (b+1)$, niin $n = (a_k \dots a_1 a_0)_b$ on jaollinen luvulla d, jos ja vain jos luvun n numeroiden vuorotteleva summa, $(-1)^k a_k + \dots - a_1 + a_0$ on jaollinen luvulla d.*

Todistus. Koska $d \mid (b+1)$, saadaan, että $b \equiv -1 (mod\, d)$. Näin ollen $b^j \equiv (-1)^j (mod\, d)$ joten $n = (a_k \dots a_1 a_0)_b \equiv (-1)^k a_k + \dots - a_1 + a_0 (mod\, d)$. Siten $d \mid n$, jos ja vain jos $d \mid ((-1)^k a_k + \dots - a_1 + a_0)$.
Lause 5.4 on todistettu □

Esimerkki 5.7 Olkoon $n = (3EA2D6)_{16}$. Nyt koska $2 \mid 16$ lauseen 5.2 perusteella tiedetään, että $2 \mid n$ koska $2 \mid 6$. Samoin koska $4 \mid 16$, nähdään, että $4 \not| n$ koska $4 \not| 6$. Lauseen 5.3 mukaan, koska $3 \mid (16-1)$, $5 \mid (16-1)$, $15 \mid (16-1)$ ja $3+E+A+2+D+6 = (30)_{16}$. Tiedetään, että $3 \mid n$ koska $3 \mid (30)_{16}$. Kun taas $5 \not| n$ ja $15 \not| n$ koska $5 \not| (30)_{16}$ ja $15 \not| (30)_{16}$. Lisäksi lauseen 5.4 mukaan, koska $17 \mid (16+1)$ ja $n = 6-D+2-A+E-3 = (D)_{16}(mod\,17)$. Tästä päätellään, että $17 \not| n$ koska $17 \not| (D)_{16}$.

Esimerkki 5.8 Olkoon $n = (1011001010)_2$. Nyt käyttämällä lausetta 5.4 saadaan, että $3 \mid n$ koska $n \equiv 0-1+0-1+0-0+1-1+0-1 \equiv 0(mod\,3)$ ja $3 \mid (2+1)$.

5.1.8 Numerosumma modulo 9

Seuraavaksi esittelemme tekniikan, jossa luvuista poistetaan numerot, joiden summa on 9. Numerosumma modulo 9 perustuu tietoon, että jokainen kokonaisluku on kongruentti sen numeroiden summan kanssa modulo 9. Tämä tekniikka voi saada esille laskennalliset virheet, kuten seuraava esimerkki osoittaa.

Esimerkki 5.9 Käytetään edellä mainittua menetelmää tarkistamaan onko lukujen 3456, 45698 ja 23489 summa 72642. Saamme, että $3456 = 3+4+5+6 \equiv 0(mod\,9)$, $45698 = 4+5+6+9+8 \equiv 5(mod\,9)$, $23489 = 2+3+4+8+9 \equiv 8(mod\,9)$. Näiden summa on kongruentti $0+5+8(mod\,9) \equiv 4(mod\,9)$. Annettu summa $72642 = 7+2+6+4+2 \equiv 3(mod\,9)$. Koska annettu summa ei ole kongruentti laskemalla saadun summan kanssa, niin voimme todeta, että annettu summa on virheellinen. Oikea summa on 72643.

Esimerkki 5.10 Käytetään nyt samaa tekniikkaa tarkistamaan tulon oikeellisuutta. Olkoon tulon tekijät 1977 ja 5876. Oletettu tulo on 61116852. $1977 \equiv 1+9+7+7 \equiv 6 \pmod 9$, $5867 \equiv 5+8+6+7 \equiv 8 \pmod 9$ Näiden tulo on $6 \cdot 8 \equiv 3 \pmod 9$. Tarkistetaan annettu tulo: $11616861 \equiv 1+1+6+1+6+8+6+1 \equiv 3 \pmod 9$. Siis oletetaan, että annettu tulo on oikein, mutta oikea tulo on 11616852. Virhe johtuu siitä, että kokonaisluvun numeroiden eri järjestykset antavat saman jäännösluvun modulo 9. Sama virhe on mahdollinen myös edellisessä esimerkissä summan tapauksessa.

5.1.9 Redusoitu numerosumma

Läheisesti Numerosumma modulo 9:ään liittyy positiivisen kokonaisluvun N redusoitu numerosumma -käsite. Se lasketaan iteraation avulla. Lasketaan luvun N numeroiden summa s ja sen jälkeen luvun s numeroiden summa. Jatketaan tätä menettelyä kunnes jäljellä on yksinumeroinen luku d. Saatu luku d on nyt luvun N redusoitu numerosumma.

Esimerkki 5.11 Etsitään luvun 1977 redusoitu numerosumma. Lasketaan luvun 1977 numerot yhteen 1+9+7+7 = 24. Nyt lasketaan vielä 2+4 = 6. Siis luvun 1977 redusoitu numerosumma on 6. Huomataan, että $1977 \equiv 6(mod\,9)$.

Määritelmä 5.1 *Yleisemmin olkoon* $N = (a_n...a_1a_0)_{10}$ *ja olkoon* d *sen redusoitu numerosumma. Nyt* $d \equiv (a_n + \ldots a_1 + a_0)(mod\,9)$. *Siis luvun* N *redusoitu numerosumma on jakojäännös, kun luku* N *jaetaan luvulla* 9. *Luvun redusoitu numerosumma on* 9 *jos jakojäännös on* 0.

Seuraava esimerkki osoittaa neliöiden mahdollisen redusoidun numerosumman.

Lause 5.5 *Jos kokonaisluku on neliö, niin sen redusoidun numerosumman täytyy olla* $1, 4, 7\,tai\,9$.

Todistus. Etsitään neliöluvun redusoitu numerosumma. Jakoalgoritmin mukaan jokainen kokonaisluku n on muotoa $9k + r$, missä $0 \leq r < 9$. Silloin $n \equiv r(mod\,9)$ ja siten $n^2 \equiv r^2(mod\,9)$. Siitä lähtien $r \equiv r - 9(mod\,9), 0^2 \equiv 0(mod\,9), (\pm1)^2 \equiv 1(mod\,9), (\pm2)^2 \equiv 4(mod\,9), (\pm3)^2 \equiv 0(mod\,9)$ ja $(\pm4)^2 \equiv 7(mod\,9)$. Siis n^2 on kongruentti lukujen $0, 1, 4\,tai\,7$ kanssa. Siis sen redusoitu numerosumma on $1, 4, 7\,tai\,9$.
Lause 5.5 on todistettu. □

Esimerkki 5.12 Ratkaise onko luku 16 151 613 924 neliö?

$$\begin{aligned} N &\equiv (1+6+1+5+1+6+1+3+9+2+4)(mod\,9) \\ &\equiv 3(mod\,9). \end{aligned}$$

Koska redusoitu numerosumma on 3, niin N ei voi olla neliö.

Esimerkki 5.13 Jos valittu kokonaisluku on neliö, niin sen redusoidun numerosumman täytyy olla 1, 4, 7 tai 9. Lause 5.2 ei toimi käänteisesti. Eli jos luvun N redusoitu numerosumma on 1, 4, 7 tai 9, niin N ei välttämättä ole neliö. Esimerkiksi luvun 43 redusoitu numerosumma on 7, mutta 43 ei ole neliö.

5.2 Ikikalenteri

Tässä kappaleessa luodaan kaava, joka antaa minkä tahansa vuoden minkä tahansa päivämäärän viikonpäivän. Koska sama viikonpäivä esiintyy joka seitsemäs päivä käytetään ratkaisussa kongruenssia modulo 7. Ensin historiaa kalenterin synnystä. Noin vuonna 738 ekr. Rooman perustaja Romulus loi kalenterin, jossa oli 10 kuukautta ja vuodessa 304 päivää. Hänen seuraajansa, Nauma, lisäsi kalenteriin kaksi kuukautta. Tätä kalenteria käytettiin kunnes Julius Caesar loi Juliaanisen kalenterin vuonna 46 ekr. vähentääkseen aurinkokalenterin ja Rooman kalenterin vääristymää. Juliaaninen kalenteri sisälsi 12 kuukautta, joissa jokaisessa oli 30 tai 31 päivää paitsi helmikuussa, jossa oli 29 päivää ja joka neljäs vuosi 30 päivää. Ensimmäinen Juliaaninen vuosi alkoi tammikuun ensimmäinen päivä 45 ekr. Se sisälsi 365,25 päivää. Se oli 11 minuuttia ja 14 sekunttia pidempi kuin aurinkovuosi ja teki joka neljäs vuosi 366 päivän pituisen karkausvuoden. Vuonna 1580 Juliaanisen kalenterin ollessa ensisijaisessa käytössä se oli kymmenen päivää poissa käytöstä. Lokakuussa 1582 ranskalaiset tähtitieteilijät Cristopher Clavius ja Aloysius Giglio esittelivät Gregoriaanisen kalenterin Pope Gregory XIII:n pyynnöstä oikaistakseen Juliaanisen kalenterin virheet. Kymmenen päivän ajan kertynyt virhe kompensoitiin hyppäämällä kymmenen päivän yli lokakuussa 1582 eli lokakuun 5. olikin lokakuun 15. Gregoriaaninen kalenteri määräsi, että vuosisadat, jotka ovat jaollisia luvulla 400 sekä muut vuodet, jotka ovat jaollisia luvulla 4 ovat karkausvuosia. Esimerkiksi vuodet 1776 ja 2000 ovat karkausvuosia, mutta 1900 ja 1974 eivät ole. Kaikkialla maailmassa käytössä oleva Gregoriaaninen kalenteri on niin tarkka, että se eroaa aurinkovuodesta vain noin 25,92 sekunttia. Tämä eroavuus esiintyy koska Gregoriaaninen vuosi kestää noin 365,2425 päivää kun taas aurinkovuosi kestää noin 365,242216 päivää. Tuloksena on kolmen päivän virhe joka 10 000. vuosi.

Nyt voidaan palata määrittämään viikonpäivää d Gregoriaanisen kalenterin mukaan jollekin annetulle päivälle r, jossakin kuukaudessa m, jossakin vuodessa y. Ensimmäinen vuosisadan karkausvuosi osui vuoteen 1600, 18 vuotta sen jälkeen kun Gregoriaaninen kalenteri oli otettu käyttöön. Kehitetään kaava, jolla lasketaan vuodet vuodesta 1600 eteenpäin. Niin ikään karkausvuodesta alkaen lisätään yksi päivä helmikuuhun, joten asetetaan uusi vuosi alkamaan päivästä 1. maaliskuuta. Esimerkiksi tammikuu vuonna 3000 on nyt yhdestoista kuukausi vuonna 2999 ja toisaalta huhtikuu vuonna 3000 on toinen kuukausi vuonna 3000. Nyt helmikuun 29. päivä 1976 on vuoden 1975 viimeisen kuukauden viimeinen päivä.

Numeroidaan kuukaudet maaliskuusta helmikuuhun luvuin 1–12 ja viikonpäivät sunnuntaista lauantaihin luvuin 0–6 seuraavasti:

Viikonpäivät	Kuukaudet	
0 = Sunnuntai	1 = Maaliskuu	7 = Syyskuu
1 = Maanantai	2 = Huhtikuu	8 = Lokakuu
2 = Tiistai	3 = Toukokuu	9 = Marraskuu
3 = Keskiviikko	4 = Kesäkuu	10 = Joulukuu
4 = Torstai	5 = Heinäkuu	11 = Tammikuu
5 = Perjantai	6 = Elokuu	12 = Helmikuu
6 = Lauantai		

Nyt $1 \leq m \leq 12$, $1 \leq r \leq 31$ ja $0 \leq d \leq 6$. Esimerkiksi $m = 3$ tarkoittaa toukokuuta ja $d = 5$ tarkoittaa perjantaita.

Johdanto on pitkä ja monimutkainen, joten luodaan kaava pienissä paloissa.

Olkoon d_y maaliskuun ensimmäisen viikonpäivä vuonna y, missä $y \geq 1600$. Lasketaan d_y luvusta d_{1600}. Koska $365 \equiv 1 (mod\, 7)$ niin d_y kasvaa yhdellä jos y ei ole karkausvuosi ja kahdella jos y on karkausvuosi. Siitä saadaan

$$d_y = \begin{cases} d_y + 1, & \text{jos y ei ole karkausvuosi} \\ d_y + 2, & \text{muulloin.} \end{cases}$$

Jotta saadaan laskettua d_y luvusta d_{1600} tarvitaan karkausvuosien lukumäärä l alkaen vuodesta 1600. Osoitetaan, että karkausvuosien lukumäärän l vuodesta 1600 annettuun vuoteen y mennessä antaa seuraava funktio

$$l = \lfloor y/4 \rfloor - \lfloor y/100 \rfloor + \lfloor y/400 \rfloor - 388 \tag{5.1}$$

Todistus. Olkoon n jokin sellainen vuosi, että $1600 < n \leq y$. Johdetaan kaava osissa:

1) Etsitään luvulla 4 jaollisten vuosien lukumäärä n_1: Olkoon $4n_1$ kysytty vuosi. Nyt $1600 < 4n_1 \leq y$. Joten $400 < n_1 \leq y/4$. Siis on olemassa $n_1 = \lfloor y/4 \rfloor - 400$ kysyttyä vuotta.

2) Etsitään vuosisatojen lukumäärä n_2 siten, että $1600 < n_2 \leq y$: Olkoon $100n_2$ sellainen vuosisata, että $1600 < 100n_2 \leq y$. Silloin $16 < n_2 \leq y/100$.

Siis on olemassa $n_2 = \lfloor y/100 \rfloor - 16$ vuosisataa välillä $1600 \leq y$.

3) Etsitään niiden vuosisatojen lukumäärä, jotka ovat jaollisia luvulla 400. Koska kyseiset vuosisadat ovat muotoa $400n_3$ saadaan epäyhtälö $1600 < 400n_3 \leq y$. Silloin $4 < n_3 \leq y/400$, siis $n_3 = \lfloor y/400 \rfloor - 4$.

4) Siis

$$\begin{aligned} l &= n_1 - n_2 + n_3 \\ &= \lfloor y/4 \rfloor - 400 - \lfloor y/100 \rfloor + 16 + \lfloor y/400 \rfloor - 4 \\ &= \lfloor y/4 \rfloor - \lfloor y/100 \rfloor + \lfloor y/400 \rfloor - 388 \end{aligned}$$

Kaava (5.1) on todistettu. □

Jakoalgoritmin mukaan $y = 100C + D$, missä $0 \leq D \leq 100$. Luvulla C merkitään vuosisatoja ja luvulla D vuosisatojen ylimeneviä vuosia vuodessa y siten, että

$$C = \lfloor y/100 \rfloor \, ja \, D = y \, modulo \, 100.$$

Esimerkiksi jos $y = 2006$, niin $C = 20$ ja $D = 6$. Nyt

$$\begin{aligned} l &= \lfloor (100C + D)/4 \rfloor - \lfloor (100C + D)/100 \rfloor + \lfloor (100C + D)/400 \rfloor - 388 \\ &= \lfloor 25C + D/4 \rfloor - \lfloor C + D/100 \rfloor + \lfloor C/4 + D/400 \rfloor - 388 \\ &= 25C + \lfloor D/4 \rfloor - C + \lfloor C/4 \rfloor \ - 388, \, koska \, D \leq 100 \, ja \, D/400 \leq 1/4 \\ &= 24C + \lfloor D/4 \rfloor + \lfloor C/4 \rfloor - 388. \end{aligned}$$

Ja tästä saadaan

$$l \equiv 3C + \lfloor D/4 \rfloor + \lfloor C/4 \rfloor - 3 (mod \, 7) \tag{5.2}$$

Siis $d_y \equiv d_{1600}$+(yksi päivä jokaista vuotta kohti alkaen vuodesta 1600) + (yksi päivä jokaista karkausvuotta kohden alkaen vuodesta 1600) (mod 7) $\equiv d_{1600} + (y - 1600) + l (mod \, 7)$. Sijoitetaan nyt $y = 100C + D$ ja $l = \lfloor y/4 \rfloor - \lfloor y/100 \rfloor + \lfloor y/400 \rfloor - 388$.

$$\begin{aligned} d_y &\equiv d_{1600} + (100C + D - 1600) + 3C + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor - 3 (mod \, 7) \\ &\equiv d_{1600} + (2C + D - 4 + 3C - 3) + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor (mod \, 7) \\ &\equiv d_{1600} + 5C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor (mod \, 7) \\ &\equiv d_{1600} - 2C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor (mod \, 7). \end{aligned} \tag{5.3}$$

Kaavaa (5.3) voidaan käyttää löytämaan d_y:n, maaliskuun ensimmäisen päivän vuonna y, jos vain tunnetaan d_{1600}. Tosiallisesti voidaan käyttää tätä löytämaan d_{1600} jollakin tunnetulla arvolla d_y. Määritetään d_{1600}. Koska maaliskuun 29. päivä vuonna 2006 oli keskiviikko, niin nyt $d_{2006} = 3$. Luvulle $y = 2006$, $C = 20$ ja $D = 6$. Nyt kaavan (5.3) mukaan saadaan

$$\begin{aligned} 3 &\equiv d_{1600} - 5 + 6 + 5 + 1 (mod\, 7) \\ &\equiv d_{1600} + 0 (mod\, 7) \\ Siis\, d_{1600} &\equiv 3 (mod\, 7) \end{aligned}$$

Vuoden 1600 maaliskuun ensimmäinen päivä oli keskiviikko. Asetetaan d_{1600} kaavaan (5.3)

$$d_y \equiv 3 - 2C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor (mod\, 7) \tag{5.4}$$

Kaava (5.4) mahdollistaa määrittelyn minkä tahansa vuoden maaliskuun ensimmäiselle viikonpäivälle. Nyt laajennetaan kaava mielivaltaisen annetun vuoden kuukauden päivään.

Laajennetaan kaavaa (5.4) antamaan kuukauden m r. päivä vuonna y Kaavan (5.4) yleistykseen tarvitsee tietää päivien lukumäärä kuukauden ensimmäisestä päivästä seuraavan kuukauden ensimmäiseen päivään modulo 7. Huomataan, että $30 \equiv 2 (mod\, 7)$ ja $31 \equiv 3 (mod\, 7)$. Siis kuukauden ensimmäiseen päivään, joka seuraa kuukautta, jossa on 30 päivää, lisätään 2 päivää. Kun taas sitä seuraa kuukausi, jossa on 31 päivää, lisätään 3 päivää. Esimerkiksi 1. joulukuuta vuonna 1992 oli tiistai. Ja siis 1. tammikuuta 1993 osui päivälle $(2+3) = 5$ eli päivä oli perjantai. Tästä saadaan seuraavat yksitoista kuukausittaista lisäystä:

1. maaliskuuta - 1. huhtikuuta : 3 päivää
1. huhtikuuta - 1 toukokuuta : 2 päivää
1. toukokuuta - 1. kesäkuuta : 3 päivää
1. kesäkuuta - 1. heinäkuuta : 2 päivää
1. heinäkuuta - 1. elokuuta : 3 päivää
1. elokuuta - 1. syyskuuta : 3 päivää
1. syyskuuta - 1. lokakuuta : 2 päivää
1. lokakuuta - 1. marraskuuta : 3 päivää
1. marraskuuta - 1. joulukuuta : 2 päivää
1. joulukuuta - 1. tammikuuta : 3 päivää
1. tammikuuta - 1. helmikuuta : 3 päivää

Etsitään funktio f, joka tuottaa yllä olevat lisäykset. Ensin huomataan, että lisäyksien summa on 29 päivää. Siis keskiarvo lisäyksistä on $11/29 \approx 2,6$ päivää, Christian Zeller (1849–1899) havaitsi, että funktio $f(m) = \lfloor 2,6m - 0,2 \rfloor - 2$ tuottaa edellä mainitut lisäykset, kun $2 \leq m \leq 12$. Esimerkiksi

$$\begin{aligned} f(3) - f(2) &= (\lfloor 7,8 - 0,2 \rfloor - 2) - (\lfloor 5,2 - 0,2 \rfloor - 2) \\ &= (7 - 2) - (5 - 2) = 2 \end{aligned}$$

Siis kuukaudesta 2 (1. huhtikuuta) kuukauteen 3 (1. toukokuuta) lisäys on kaksi päivää. Tämän vuoksi kaavan (5.4) avulla kuukauden m ensimmäinen päivä d' saadaan kaavasta $d_y + \lfloor 2,6m - 0,2 \rfloor - 2(mod\,7)$. Nyt

$$\begin{aligned} d' &\equiv 3 - 2C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor + \lfloor 2,6m - 0,2 \rfloor - 2(mod\,7) \\ &\equiv 1 + \lfloor 2,6m - 0,2 \rfloor - 2C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor (mod\,7) \end{aligned}$$

Etsitään kaava kuukauden m r:nnelle päivälle. Viikonpäivä d kuukauden r:nnelle päivälle saadaan kaavasta $d' + (r-1)(mod\,7)$, joten

$$d \equiv r + \lfloor 2,6m - 0,2 \rfloor - 2C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor (mod\,7) \tag{5.5}$$

Kaava (5.5) mahdollistaa viikonpäivän määrittelyn mille tahansa annetulle päivälle Gregoriaanisessa kalenterissa.

Esimerkki 5.14 Otetaan esimerkiksi syntymäpäiväni. Eli mikä viikonpäivä oli 14.11 vuonna 1977? Siis $r = 14$, $m = 9$, $y = 1977$ $C = 19$ $D = 77$. Nyt $d \equiv r + \lfloor 2,6m - 0,2 \rfloor - 2C + D + \lfloor C/4 \rfloor + \lfloor D/4 \rfloor (mod\,7)$ eli
$d \equiv 14 + 23 - 38 + 77 + 4 + 19 \equiv 1(mod\,7)$, siis 14.11.1977 oli maanantai.

5.3 Turnausaikataulu

Turnauksissa jokainen joukkue tai henkilö pelaa kerran jokaista muuta joukkuetta tai henkilöä vastaan tasan kerran. Oletetaan, että turnauksessa on n joukkuetta, numeroituna alkaen 1:stä n:ään.

Olkoon g_n otteluiden lukumäärä turnauksessa, johon osallistuu n joukkuetta. Otteluiden lukumäärä voidaan määrittää rekursiivisesti:

$$\begin{aligned} g_1 &= 0 \\ g_n &= g_{n-1} + (n-1),\ kun\, n \geq 2 \end{aligned}$$

Kun ratkaistaan tämä rekursiivinen yhteys, saadaan, että

$$g_n = \frac{n(n-1)}{2} = \binom{n}{2}.$$

Esimerkiksi kuusi joukkuetta pelaa 15 ottelua, sillä $6 \cdot 5/2 = 15$. Viisi joukkuetta pelaa 10 ottelua, sillä $5 \cdot 4/2 = 10$.
Kongruenssia voidaan helposti soveltaa, kun suunnitellaan turnausohjelmaa. Jos joukkueita on parillinen määrä niin silloin jokaiselle joukkueelle löytyy aina pari, mutta jos joukkueita on pariton määrä, niin yksi joukkue huilaa vuorollaan yhden kierroksen ajan. Siis aina, kun joukkueita on pariton määrä lisätään turnaukseen haamujoukkue, jota merkitään X:llä. Kun jonkin joukkueen pariksi sattuu X, niin silloin kyseinen joukkue huilaa sen kierroksen.
Olkoon $g(i, j)$ joukkue, joka pelaa kierroksella i joukkuetta j vastaan. Jos $g(i, j) = j$ niin silloin joukkue j on huilivuorossa kierroksella i.
Määritetään, että

$$g(i, j) \equiv i - j (mod\, p),$$

missä pienin jäännös 0 *modulo* p tulkitaan luvuksi p, missa p on joukkueiden lukumäärä.
Esimerkiksi olkoon $p = 7$. Silloin $g(1, 1) = 0(mod\, 7)$. Siis $g(1, 1) = 7$. Samoin $g(1, 2) = -1(mod\, 7)$. Siis $g(1, 2) = 6$ jne.
Voidaan siis osoittaa, että funktio g konstruoi turnausohjelman p:lle joukkueelle. Ennen sitä täytyy todistaa kolme lausetta.

Lause 5.6 *Yksi ja vain yksi joukkue huilaa kullakin kierroksella.*

Todistus. Vastaoletus. Oletetaan, että joukkueet j_1 ja j_2 huilaavat kierroksella i. Silloin

$$g(i, j_1) \equiv j_1 (mod\, p)\, ja\, g(i, j_2) \equiv j_2 (mod\, p)$$

Tapaus 1: Jos $i = j_1$, silloin $i = j_1 = p$. Koska $g(i, j_2) \equiv j_2 (mod\, p)$ ja $i - j_2 \equiv j_2 (mod\, p)$, silloin

$$p - j_2 \equiv j_2 (mod\, p)$$

$$2j_2 \equiv 0 (mod\, p)$$

$$j_2 \equiv 0(mod\, p)$$

Siis $j_2 = p$, joten $j_1 = j_2$.
Tapaus 2: Jos $i \neq j_1$, niin $g(i, j_1) \equiv i - j_1 \equiv j_1(mod\, p)$, silloin $i \equiv 2j_1(mod\, p)$. Jos $i = j_2$ ja $g(i, j_2) \equiv i \equiv p(mod\, p)$. Niin silloin $p \equiv 2j_1(mod\, p)$, siis $2j_1 \equiv 0(mod\, p)$. Tälloin $j_1 \equiv 0(mod\, p)$ tai $j_1 = p$. Silloin $i \equiv 2p \equiv 0(mod\, p)$, siis $i = p$. Nyt $i = j_1$, joka on ristiriita.
Jos $i \neq j_2$ niin $g(i, j_2) \equiv i - j_2 \equiv j_2(mod\, p)$. Tästä saadaan, että $i \equiv 2j_2(mod\, p)$, siis

$$\begin{aligned} 2j_1 &\equiv 2j_2(mod\, p) \\ j_1 &\equiv j_2(mod\, p) \end{aligned}$$

Tästä seuraa, että $j_1 = j_2$, koska nämä ovat pienimmät jäännökset modulo p. Siis molemmissa tapauksissa $j_1 = j_2$ eli jokaisella kierroksella täsmälleen yksi joukkue huilaa.
Lause 5.6 on todistettu. □

Lause 5.7 *$g(i, j) \equiv j\,(mod\, p)$, jos ja vain jos $j \equiv (\frac{p+i}{2})i(mod\, p)$.*

Todistus. Oletetaan, että $g(i, j) \equiv j(mod\, p)$. Jos $i = j$, niin $g(i, j) \equiv p(mod\, p)$, siis $i \equiv j \equiv p \equiv 0(mod\, p)$. Siksi $j \equiv (p + 1)i/2(mod\, p)$. Jos $i \neq j$, niin $g(i, j) \equiv i - j(mod\, p)$.

$$\begin{aligned} i - j &\equiv j(mod\, p) \\ i &\equiv 2j(mod\, p) \end{aligned}$$

Siis $(p+1)i/2 \equiv (p+1)2j/2 \equiv pj + j \equiv j(mod\, p)$. Näin ollen molemmissa tapauksissa joukkue j huilaa kierroksella i jos $j \equiv (p+1)i/2(mod\, p)$. Toisaalta, oletetaan, että $j \equiv (p + 1)i/2(mod\, p)$. Silloin

$$\begin{aligned} g(i, j) &\equiv i - j(mod\, p) \\ &\equiv i - (p + 1)i/2 \equiv (1 - p)i/2(mod\, p) \\ &\equiv (p + 1)i/2 \equiv j(mod\, p) \end{aligned}$$

Siis joukkue j huilaa kierroksella i.
Lause 5.7 on todistettu. □

Lause 5.8 *Funktio g on yksikäsitteinen kaikilla luvuilla i.*

Todistus. Oletetaan, että $g(i, j_1) = g(i, j_2)$. Nyt $i - j_1 \equiv i - j_2 (mod\, p)$, siis $j_1 \equiv j_2 (mod\, p)$. Näin ollen $j_1 = j_2$ ja siis g on yksikäsitteinen.
Lause 5.8 on todistettu. □

Lauseista 5.6 - 5.8 seuraa, että funktio g määrittelee yksikäsitteisesti joukkueen j vastustajan jokaisella kierroksella i, missä $1 \leq i,\ j \leq p$; kierroksella i, joukkue j huilaa, missä $j \equiv (p+1)i/2 (mod\, p)$.

Esimerkki 5.15 Ratkaistaan turnausvastustajat kullekin kierrokselle, kun turnaukseen osallistuu 11 joukkuetta. Numeroidaan joukkueet luvuin $1 - 11$. Koska joukkueita on pariton määrä, lisätään haamujoukkue X. Määritellään ottelut ensimmäiselle kierrokselle: Joukkueen i vastustaja j saadaan kaavasta $i + j \equiv 1 (mod\, 11)$. Siis joukkueen 1 vastustaja: $1 + j \equiv 1 (mod\, 11)$, siis $j = 11$. Samoin saadaan muiden joukkueiden vastustajat:
joukkueen 2 vastustaja: $2 + j \equiv 1 (mod\, 11)$, siis $j = 10$,
joukkueen 3 vastustaja: $3 + j \equiv 1 (mod\, 11)$, siis $j = 9$,
joukkueen 4 vastustaja: $4 + j \equiv 1 (mod\, 11)$, siis $j = 8$,
joukkueen 5 vastustaja: $5 + j \equiv 1 (mod\, 11)$, siis $j = 7$,
joukkueen 6 vastustaja: $6 + j \equiv 1 (mod\, 11)$, siis $j = 6$.
Huomataan, että joukkue 6 sai itsensä vastustajakseen eli tämä joukkue huilaa ensimmäisellä kierroksella.
Toisen kierroksen vastustajat saadaan samoin: Toisella kierroksella joukkueen i vastustaja j saadaan kaavasta $i + j \equiv 2 (mod\, 11)$. Siis joukkueen 1 vastustaja: $1 + j \equiv 2 (mod\, 11)$, siis $j \equiv 12 \equiv 1 (mod\, 11)$ eli $j = 1$. Tästä nähdään, että joukkue 1 huilaa toisella kierroksella. Muiden joukkueiden vastustajat toisella kierroksella:
joukkueen 2 vastustaja: $2 + j \equiv 2 (mod\, 11)$, siis $j = 11$,
joukkueen 3 vastustaja: $3 + j \equiv 2 (mod\, 11)$, siis $j = 10$,
joukkueen 4 vastustaja: $4 + j \equiv 2 (mod\, 11)$, siis $j = 9$,
joukkueen 5 vastustaja: $5 + j \equiv 2 (mod\, 11)$, siis $j = 8$,
joukkueen 6 vastustaja: $6 + j \equiv 2 (mod\, 11)$, siis $j = 7$.
Näin jatkamalla saadaan kaikkien 11:den kierroksen ottelut. Ne on esitetty seuraavassa taulukossa.

i/j	1	2	3	4	5	6	7	8	9	10	11
1	11	10	9	8	7	X	5	4	3	2	1
2	X	11	10	9	8	7	6	5	4	3	2
3	2	1	11	10	9	8	X	6	5	4	3
4	3	X	1	11	10	9	8	7	6	5	4
5	4	3	2	1	11	10	9	X	7	6	5
6	5	4	X	2	1	11	10	9	8	7	6
7	6	5	4	3	2	1	11	10	X	8	7
8	7	6	5	X	3	2	1	11	10	9	8
9	8	7	6	5	4	3	2	1	11	X	9
10	9	8	7	6	X	4	3	2	1	11	10
11	10	9	8	7	6	5	4	3	2	1	11

5.4 Kuningatarpulma

Tunnettu ongelma on asettaa $n \cdot n$ -shakkilaudalle n kappaletta kuningattaria, niin, että kukaan ei pysty lyömään toista. Tässä on huomioitava, että ongelmalle ei ole ratkaisua kun $n = 2$ tai $n = 3$. Tästä kehitetään kaava, jolla voidaan asettaa p kuningatarta $p \cdot p$ -shakkilaudalle, missä p on alkuluku.

Kuningatar liikkuu pitkin niitä rivejä, linjoja ja viistorivejä, joilla se on. Asetetaan kuningattaria rivi riviltä, kun esitetään ratkaisua ongelmaan. Merkitään $f(i)$:lla i:nnen kuningattaren sijaintia, missä $1 \leq i \leq p$. Nyt $f(i)$ voidaan määrittää rekursiivisesti.

$$\begin{aligned} f \quad & (0) = 0 \\ f \quad & (i) \equiv f(i-1) + \frac{(p+1)}{2} (mod\, p),\ 1 \leq i \leq p-1 \\ f \quad & (p) = p \end{aligned}$$

Käyttämällä iteraatiota voidaan tätä määritelmää käyttää antamaan seuraava täsmällinen kaava funktiolle $f(i)$.

$$f(i) \equiv \left(\frac{p+1}{2} \right) i (mod\, p),\ jos\, 1 \leq i \leq p.$$

Tässä $f(i)$ on pienin jäännös $(p+1)i/2$ modulo p, missä jäännös 0 tulkitaan luvuksi p. Seuraavaksi todistamme muutamia funktion f ominaisuuksia.

Lause 5.9 *Funktio f on yksikäsitteinen.*

Todistus. Olkoon i ja j sellaisia pienimpiä jäännöksiä modulo p, että

$$f(i) = f(j).$$

Silloin

$$\left(\frac{p+1}{2}\right) i \equiv \left(\frac{p+1}{2}\right) j (mod\, p).$$

Koska $((p+1)/2, p) = 1$, niin tästä seuraa, että $i \equiv j (mod\, p)$. Mutta koska i ja j ovat pienimpiä jäännöksiä modulo p, niin $i = j$.
Lause 5.9 on todistettu. □

Lause 5.10 *Kaksi kuningatarta, jotka on asetettu $p \cdot p$ -shakkilaudalle säännön f mukaan, eivat voi lyödä toisiaan.*

Todistus. Koska jokaisella rivillä ja sarakkeella on vain yksi kuningatar, niin kaksi kuningatarta ei voi löydä toisiaan rivejä tai sarakkeita pitkin. Siis riittää osoittaa, että ne eivät voi lyödä toisiaan viistorivejä pitkin.
Jokaisella laskevalla viistorivillä, rivin indeksin i ja sarakkeen indeksin j summa $i + j$ on vakio k, missä $2 \leq k \leq 2p$. Selvästi tarvitsee vain tarkistaa viistorivit, joilla $3 \leq k \leq 2p - 1$.
Oletetaan, että on olemassa kaksi kuningatarta paikoilla $(i_1,\, j_1)$ ja $(i_2,\, j_2)$.Nyt

$$f(i_1) \equiv \left(\frac{p+1}{2}\right) i_1 (mod\, p)$$

$$f(i_2) \equiv \left(\frac{p+1}{2}\right) i_2 (mod\, p)$$

Silloin

$$j_1 \equiv \left(\frac{p+1}{2}\right) i_1 (mod\, p)\, ja\, j_2 \equiv \left(\frac{p+1}{2}\right) i_2 (mod\, p), \tag{5.6}$$

missä $i_1 + j_1 = k = i_2 + j_2$. Silloin

$$i_1 + j_1 \equiv \left(\frac{p+3}{2}\right) i_1 (mod\, p)$$

eli

$$k \equiv \left(\frac{p+3}{2}\right) i_1 (mod\, p).$$

Samoin

$$k \equiv \left(\frac{p+3}{2}\right) i_2 (mod\, p).$$

Nämä kaksi kongruenssia sisältävät sen, että $(p+3)i_1/2 \equiv (p+3)i_2/2 (mod\, p)$, siis $i_1 \equiv i_2 (mod\, p)$ koska $(p, (p+3)/2) = 1$. Täten $i_1 = i_2$ koska ne ovat pienin jäännös modulo p. Nyt kongruenssin (5.6) perusteella $j_1 = j_2$. Täten mikään laskeva viistorivi ei sisällä kahta kuningatarta.
Osoitetaan, että mikään nouseva viistorivi ei sisällä kahta kuningatarta. Huomataan, että jokainen tällainen viistorivi, $i - j$ on vakio l, missä $1 - p \leq l \leq p - 1$. Oletetaan, että nouseva viistorivi sisältää kaksi kuningatarta paikoilla (i_1, j_1) ja (i_2, j_2).
Silloin

$$f(i_1) \equiv \left(\frac{p+1}{2}\right) i_1 (mod\, p)$$

$$f(i_2) \equiv \left(\frac{p+1}{2}\right) i_2 (mod\, p)$$

Silloin

$$j_1 \equiv \left(\frac{p+1}{2}\right) i_1 (mod\, p)\, ja\, j_2 \equiv \left(\frac{p+1}{2}\right) i_2 (mod\, p), \tag{5.7}$$

missä $i_1 - j_1 = l = i_2 - j_2$. Nyt

$$i_1 - j_1 \equiv i_1 - \left(\frac{p+1}{2}\right) i_1 (mod\, p)$$

$$l \equiv \left(\frac{1-p}{2}\right) i_1 (mod\, p)$$

$$l \equiv \left(\frac{p+1}{2}\right) i_1 (mod\, p)$$

Samoin

$$l \equiv \left(\frac{p+1}{2}\right) i_2 (mod\, p)$$

Näistä kahdesta kongruenssista saadaan, että $i_1 = i_2$, koska $((p+1)/2, p) = 1$, ja i_1 ja i_2 ovat pienimmät jäännökset modulo p. Siis kongruenssin (5.7) perusteella $j_1 = j_2$. Siis mikään nouseva viistorivi ei sisällä kahta kuningatarta. Siis mitkään kaksi kuningatarta $p \cdot p$ shakkilaudalla eivat voi lyödä toisiaan. Lause 5.10 on todistettu. □

Viitteet

[1] Koshy, Thomas: Elementary Number Theory with Applications. Harcourt/Academic Press, San Diego 2002.

[2] Rosen, Kenneth H.: Elementary Number Theory and its Applications. Addison Wesley Longman, 2000.