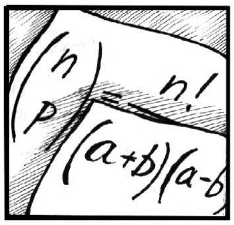

Yksinkertaisista jaollisuustesteistä

Timo Tossavainen
Lehtori
Savonlinnan OKL, Joensuun yliopisto

Lukion pitkässä matematiikassa jaollisuustestejä käsitellään ainakin jossakin laajuudessa logiikan ja lukuteorian syventävällä kurssilla. Solmussa jaollisuustestien kannalta keskeistä kongruenssin käsitettä on puolestaan tarkasteltu ainakin artikkeleissa [2] ja [5]. Tämä kirjoitus on jonkinlainen yhteenveto siitä matematiikasta, jota yksinkertaisten jaollisuustestien konstruoimiseksi tarvitaan.

Jakoyhtälö ja kongruenssi

Jakoalgoritmin tai oikeammin jakoyhtälön nimellä tunnettu lause on eräs keskeisimmistä lukuteorian työkaluista. Se voidaan ilmaista esimerkiksi seuraavassa muodossa.

Lause 1. Olkoot a ja n kokonaislukuja siten, että $n > 0$. Tällöin on olemassa yksikäsitteiset kokonaisluvut q ja r siten, että

$$a = qn + r \quad \text{ja} \quad 0 \leq r < n.$$

Todistus. Olkoon

$$E = \{r \in \mathbb{Z} : r \geq 0 \text{ ja } r = a - qn \text{ jollakin } q \in \mathbb{Z}\}.$$

Tällöin E on epätyhjä, sillä jos $a \geq 0$, on $a \in E$, ja jos $a < 0$, on $a - an \in E$. Näin ollen joukossa E on pienin alkio $r_0 = a - q_0 n$. Lisäksi $r_0 < n$, sillä muuten

$$r_1 = a - (q_0 + 1)n = r_0 - n \geq 0$$

ja siksi $r_1 \in E$, mikä olisi ristiriita.

Oletetaan, että

$$a = qn + r = q'n + r', \text{ missä } 0 \leq r < n \text{ ja } 0 \leq r' < n.$$

Tällöin

$$r' - r = (q - q')n,$$

joten $r' - r$ on jaollinen luvulla n. Koska $0 \leq r < n$ ja $0 \leq r' < n$, on

$$-n < r' - r < n.$$

Näin ollen $r' - r = 0$ eli $r = r'$, jolloin myös $q = q'$, koska $n > 0$. $\square$

Usein sanotaan, että luku a on *jaettava*, n *jakaja*, q *osamäärä* ja r *jakojäännös*. Jos luvuilla a ja b on yhteisen jakajan n suhteen samat jakojäännökset, tällöin luvut a ja b ovat *kongruentit modulo* n, ja tätä merkitään kirjoittamalla

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

Määritelmästä seuraa välittömästi, että luvut a ja b ovat kongruentit modulo n, jos ja vain jos $a - b$ on jaollinen luvulla n.

Esimerkki. Koska $17 = 3 \cdot 5 + 2$ ja $-18 = -4 \cdot 5 + 2$, niin

$$17 \equiv -18 \pmod 5.$$

Toisaalta sama asia nähdään siitä, että $17 - (-18) = 35 = 7 \cdot 5$.

Kongruenssi modulo n on ekvivalenssirelaatio kokonaislukujen joukossa (ks. esim. [5]), joten se toimii ikäänkuin relaatio $=$ kokonaislukujen tavallisessa aritmetiikassa. Jakojäännösten aritmetiikka muistuttaa muutenkin monessa suhteessa kokonaislukujen tavallista aritmetiikkaa, sillä voimme todistaa muun muassa seuraavat kongruentteja lukuja koskevat laskusäännöt.

Lause 2. Olkoon $a \equiv b \pmod n$ ja $c \equiv d \pmod n$. Tällöin

$$a + c \equiv b + d \pmod n$$

ja

$$ac \equiv bd \pmod n.$$

Todistus. Koska $a - b = kn$ ja $c - d = ln$ joillakin $k, l \in \mathbb{Z}$, on

$$(a + c) - (b + d) = (a - b) + (c - d) = (k + l)n.$$

Lukujen $a + c$ ja $b + d$ erotus on siis jaollinen luvulla n, joten ne ovat kongruentit modulo n.

Vastaavasti

$$\begin{aligned} ac - bd &= (ac - bc) + (bc - bd) \\ &= (a - b)c + (c - d)b \\ &= (ck + bl)n, \end{aligned}$$

mistä toinen väite seuraa. $\square$

Olkoon $k \geq 2$ luonnollinen luku. Induktion avulla tai soveltamalla Lausetta 2 riittävän monta kertaa peräkkäin näemme edelleen, että

$$(1) \qquad \sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod n$$

ja

$$(2) \qquad a_1 a_2 \cdots a_k \equiv b_1 b_2 \cdots b_k \pmod n$$

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

Huomautus. Jakojäännösten aritmetiikka poikkeaa kuitenkin hieman kokonaislukujen tavallisesta aritmetiikasta. Koska esimerkiksi $14 \equiv 8 \pmod 6$ ja $7 \not\equiv 4 \pmod 6$, kongruenssiyhtälön puolittainen jakaminen ei onnistu kaikilla vakioilla.

Kongruenssi ja jaollisuustestit

Se, onko luku x jaollinen luvulla n, selviää yleensä helpoiten jakamalla x luvulla n esimerkiksi taskulaskimen avulla tai käsin jakokulmassa. Jos x on hyvin suuri, jakaminen ei kuitenkaan onnistu taskulaskimella. Toisaalta jakokulmassa laskemistakaan ei voida pitää erityisen tehokkaana tapana tutkia suurten lukujen jaollisuutta. Tällöin on etsittävä joko uusia tapoja suorittaa jakolasku tai sitten menetelmiä, joissa testattava luku voidaan korvata sellaisella luvulla, jonka jakaminen onnistuu helpommin. Lause 2 ja kaavat (1) ja (2) osoittautuvat tässä hyödyllisiksi.

Koska kokonaisluvun x jaollisuus luvulla $n > 0$ ei riipu sen etumerkistä, riittää tarkastella vain positiivisten kokonaislukujen jaollisuutta. Tällöin jokaista lukua x vastaa luonnollinen luku $k \geq 1$ siten, että

$$(3) \qquad x = a_k 10^k + a_{k-1} 10^{k-1} + ... + a_1 10 + a_0,$$

missä $a_i \in \{0, 1, 2, ..., 9\}$ kaikilla $i = 0, 1, ..., k$. Jakoyhtälön nojalla kaikilla $i \in \mathbb{N}$ löytyy luku b_i siten, että $0 \leq b_i < n$ ja 10^i on kongruentti luvun b_i kanssa modulo n. Tällöin Lauseen 2 ja kaavojen (1) ja (2) nojalla on x jaollinen luvulla n, jos ja vain jos

$$(4) \qquad a_k b_k + a_{k-1} b_{k-1} + ... + a_1 b_1 + a_0 \equiv 0 \pmod n.$$

Jos x on suuri, on kaavan (4) vasen puoli huomattavasti pienempi kuin x. Lisäksi kaavaa (4) voidaan soveltaa useita kertoja peräkkäin.

Kolmella jaollisuus

Olkoon $n = 3$. Koska $10 \equiv 1 \pmod 3$, on kaavan (2) nojalla $10^k \equiv 1 \pmod 3$ kaikilla $k \geq 1$. Luvut b_i ovat siis kaikki ykkösiä kaavassa (4), joten kaavan (3) muodossa esitetty luku x on jaollinen luvulla 3, jos ja vain jos

$$a_k + a_{k-1} + ... + a_1 + a_0 \equiv 0 \pmod 3.$$

Esimerkiksi 29 760 183 on jaollinen luvulla kolme, sillä

$$2 + 9 + 7 + 6 + 0 + 1 + 8 + 3 \equiv 36 \equiv 0 \pmod 3.$$

Kahdella ja viidellä jaollisuus

Olkoon $n \in \{2, 5\}$. Koska $10 \equiv 0 \pmod n$, on kaavan (2) nojalla $10^k \equiv 0 \pmod n$ kaikilla $k \geq 1$. Tällöin kaavan (3) muodossa esitetty luku x on jaollinen luvulla n, jos ja vain jos

$$a_0 \equiv 0 \pmod n.$$

Esimerkiksi 976 213 521 ei ole jaollinen kahdella eikä viidellä, sillä

$$1 \not\equiv 0 \pmod n,$$

silloin kun $n \in \{2, 5\}$.

Joissakin jaollisuustesteissä kannattaa sallia luvuille b_i myös negatiivisia arvoja. Jos x ei ole luvun n monikerta, jakoyhtälöstä seuraa, kun alkuperäinen osamäärä korvataan yhtä suuremmalla kokonaisluvulla, että x voidaan kirjoittaa yksikäsitteisesti myös muodossa

$$x = qn + r, \quad \text{missä } \ q \in \mathbb{Z} \text{ ja } -n < r < 0.$$

Jokainen kokonaisluku, ja erityisesti jokainen 10^i, on siis kongruentti myös sellaisen luvun b_i kanssa, missä $-n < b_i \leq 0$.

Jaollisuus luvulla 11

Koska $10 \equiv -1 \pmod{11}$, kaavasta (2) seuraa, että $10^k \equiv (-1)^k \pmod{11}$ kaikilla $k \geq 1$. Näin ollen kaavan (3) muodossa esitetty luku x on jaollinen luvulla 11, jos ja vain jos

$$a_k(-1)^k + a_{k-1}(-1)^{k-1} + ... - a_1 + a_0 \equiv 0 \pmod{11}.$$

Edellisen kaavan nojalla on siis ilmeistä, että esimerkiksi 987 654 321 123 456 789 on jaollinen luvulla 11.

Joskus testattava luku x kannattaa esittää muodossa, jossa kantalukuna on 100, 1000 tai vieläkin suurempi kymmenen potenssi. (Yksinkertaisimmat kertoimet luvulla n jaollisuuden testiin saadaan tietysti silloin, kun luku x esitetään n-lukujärjestelmän mukaisessa muodossa...)

Jaollisuus luvulla 13

Koska $10 \equiv -3 \pmod{13}$, $10^2 \equiv -4 \pmod{13}$, $10^3 \equiv -1 \pmod{13}$, $10^4 \equiv 3 \pmod{13}$, $10^5 \equiv 4 \pmod{13}$, $10^6 \equiv 1 \pmod{13}$, $10^7 \equiv -3 \pmod{13}$ jne., on arvolla $n = 13$ kaavassa (4) kertoimet $b_1 = -3$, $b_2 = -4$, $b_3 = -1$, $b_4 = 3$, $b_5 = 4$, $b_6 = 1$ jne. Jos x esitetään kuitenkin muodossa

$$x = c_k 1000^k + c_{k-1} 1000^{k-1} + ... + c_1 1000 + c_0,$$

missä $c_i \in \{0, 1, 2, ..., 999\}$ kaikilla $i = 0, 1, ..., k$, saadaan luvun x kolmellatoista jaollisuuden ehto nyt kaavojen (1) ja (2) nojalla muotoon

$$c_k(-1)^k + c_{k-1}(-1)^{k-1} + ... - c_1 + c_0 \equiv 0 \pmod{13}.$$

Jos x ja n ovat molemmat hyvin suuria lukuja, edellä kuvatusta tavasta konstruoida jaollisuustestejä ei ole suuresti apua, ellei lukua n voida esittää pienempien (alku-)lukujen tulona. Suuren luvun jakaminen tekijöihin on yleensä kuitenkin hyvin työlästä. On arvioitu, että tietokoneella, joka suorittaa miljardi operaatiota sekunnissa, 100-numeroisen luvun jakaminen tekijöihin kestää noin 26 vuorokautta ja 200-numeroisen luvun jakaminen vajaat 4 miljoonaa vuotta. Vielä vuonna 1988 200-numeroisen luvun tekijöihinjako olisi maksanut suurin piirtein saman verran kuin miehittämätön kuumatka.

Viitteet

1. P. Haukkanen: Algebran luentomoniste, Tampereen yliopisto, 2003.
2. V. Latvala ja P. Smolander: Modulaarisista laskutaulukoista, Solmu 2/2003.
3. J. Merikoski, A. Virtanen ja P. Koivisto: Diskreetti matematiikka I, Tampereen yliopisto, 1998.
4. J. Merikoski, K. Väänänen ja T. Laurinolli: Matematiikan taito 11, lukion pitkä matematiikka: Lukuteoria ja logiikka, Weilin+Göös, 3. p., 1997.
5. T. Metsäkylä: Kongruenssi – lukuteorian kätevä apuväline, Solmu 3/1997–1998.
6. K.H. Rosen: Discrete Mathematics and Its Applications, McGraw-Hill International Editions, 4th Ed., 1999.