Kongruensseilla laskeminen

Kongruensseja voidaan käsitellä suunnilleen samalla tavalla kuin yhtälöitä. Ainoa eroavuus tulee esille jakolaskun tapauksessa. Kongruenssien sievennyksissä voidaan moduli, eli merkintä $(\mathrm{mod}\ n)$, kirjoittaa vasta viimeisen lausekkeen loppuun.

Lause, kongruenssin säilyminen yhteen/vähennys- ja kertolaskussa:
Jos

$$a \equiv b \pmod{n} \quad \text{ja} \quad c \equiv d \pmod{n},$$

niin

$$a \pm c \equiv b \pm d \pmod{n} \quad \text{ja} \quad ac \equiv bd \pmod{n}.$$

Todistus: Kirjassa LAUDATUR-11 sivut 91 - 92.

Esimerkki Lasketaan yhteen todet kongruenssit $2 \equiv 7 \pmod{5}$ ja $13 \equiv -2 \pmod{5}$, jolloin saadaan $15 \equiv 5 \pmod{5}$, OK ja vastaavasti kertomalla saadaan $26 \equiv -14 \pmod{5}$, OK.

Asettamalla $c = d = k$ huomataan, että kongruenssiin voidaan lisätä mikä tahansa luku ja kongruenssi voidaan kertoa millä tahansa luvulla.

Lause, kongruenssin säilyminen lisättäessä luku ja kerrottaessa sillä:
Jos $a \equiv b \pmod{n}$,
niin $a \pm k \equiv b \pm k \pmod{n}$ ja $ak \equiv bk \pmod{n}$.

Todistus: Seuraa edellisen lauseen todistuksesta, merkitse $c = d = k$.

Edelleen induktiolla voidaan osoittaa, että jokainen potenssi ja kokonaislukukertoiminen polynomifunktio $p(x)$ säilyttää kongruenssin.

Lause, kongruenssin säilyminen potensseille ja polynomeille:
Jos $a \equiv b \pmod{n}$,
niin $a^m \equiv b^m \pmod{n}$ kaikilla luonnollisilla luvuilla m ja
$p(a) \equiv p(b) \pmod{n}$ kaikilla kokonaislukukertoimisilla polynomeilla $p(x)$.

Todistus: Potensseille LAUDATUR-11 kirjassa, sivut 92-93. Polynomeille induktiolla polynomin asteen suhteen → harjoitustehtävä.

Esimerkkejä **a)** Mikä on jakojäännös, kun luku $753 + 6^{1201}$ jaetaan luvulla 7? Kongruenssin laskusääntöjä hyödyntäen, saadaan

$$\begin{aligned} 753 + 6^{1201} &\equiv \overbrace{107 \cdot 7 + 4}^{=753} + 6^{1201} && \mid 753 \equiv 4 \pmod 7 \\ &\equiv 4 + 6^{1201} && \mid 6 \equiv -1 \pmod 7 \\ &\equiv 4 + (-1)^{1201} && \mid (-1)^{1201} \equiv -1 \pmod 7 \\ &\equiv 4 - 1 \\ &\equiv 3 \pmod 7 \end{aligned}$$

b) Laske jakojäännös jakolaskussa $2^{20}:3$. Laskun voisi suorittaa laskimella, mutta perustellaan tulos kongruensseja käyttäen.
Koska $2^2 = 4 \equiv 1 \pmod 3$, on $2^{2k} = (2^2)^k \equiv 1 \pmod 3$ kaikilla luonnollisilla luvuilla k. Arvolla $k = 10$ saadaan $2^{20} \equiv 1 \pmod 3$, joten kysytty jakojäännös on 1.

c) Laske jakojäännös jakolaskussa $2^{63}:3$. Nyt ei laskinkaan enää auta, mutta kongruenssit toimivat edelleen. Arvolla $k = 31$ on **b)**-kohdan mukaan $2^{63} = 2 \cdot 2^{62} \equiv 2 \pmod 3$, joten kysytty jakojäännös on 2.

Esimerkkejä(jatkuu)
d) Määritä pienin luonnollinen luku, jonka kanssa luku $2^{42} + 7$ on kongruentti $\pmod 5$.

Koska $2^4 = 16 \equiv 1 \pmod 5$ ja $7 \equiv 2 \pmod 5$, niin

$$2^{40} = (2^4)^{10} \equiv 1^{10} = 1 \pmod 5$$

ja edelleen

$$2^{42} + 7 = 2^{40} \cdot 4 + 7 \equiv 4 + 2 = 6 \equiv 1 \pmod 5.$$

Havaitse yhtäsuuruusmerkin $=$ ja kongruenttimerkin $\equiv$ sujuva rinnakkain käyttö ja ero!

e) Olkoon n luonnollinen luku. Osoita, että luku $13^n + 5 \cdot 7^n$ on jaollinen luvulla 6.

Koska $13 \equiv 1 \pmod 6$ ja $7 \equiv 1 \pmod 6$, on $13^n \equiv 1 \pmod 6$ ja vastaavasti $7^n \equiv 1 \pmod 6$. Edelleen

$$13^n + 5 \cdot 7^n \equiv 1 + 5 \cdot 1 = 6 \equiv 0 \pmod 6.$$

Normaali yhtälö voidaan jakaa puolittain nollasta poikkeavalla (kokonais)luvulla, mutta kongruensseille ei aina voida tehdä vastaavasti:

Esimerkki Kongruenssi $10 \equiv 6 \pmod 4$ on tosi, mutta siitä 2:lla jakamalla saatu kongruenssi $5 \equiv 3 \pmod 4$ on epätosi. Jos myös moduli jaetaan luvulla 2, niin saadaan tosi kongruenssi $5 \equiv 3 \pmod 2$, joka tosin ei ole kiinnostava, koska moduli muuttuu.

Millä ehdolla kongruenssi $a \equiv b \pmod n$ voidaan jakaa annetulla luvulla k, jotta saataisiin yhtäpitävä kongruenssi $\pmod n$. Lähtökohtana täytyy olla, että luvut a ja b ovat jaollisia luvulla k, jolloin $a = ku$ ja $b = kv$.

Lause, kongruenssin säilyminen jakolaskussa:
Jos $\text{syt}(k, n) = 1$, niin kongruenssit

$$ku \equiv kv \pmod n, \qquad u \equiv v \pmod n$$

ovat yhtäpitäviä, eli niillä on samat totuusarvot.

Todistus: Kongruenssi säilyy kertolaskussa, joten jälkimmäisestä kongruenssista seuraa edellinen (eikä oletusta $\text{syt}(k, n) = 1$ edes tarvita).

Todistus(jatkuu): Ehdon $\text{syt}(k, n) = 1$ ollessa voimassa olkoon siis $ku \equiv kv \pmod n$. Tällöin $n|(ku - kv)$ eli $n|k(u - v)$. Koska nyt $\text{syt}(k, n) = 1$, niin on $n|(u - v)$ (perustelut!), joten $u \equiv v \pmod n$.

Itse asiassa pitäisi vielä osoittaa, että jos $\text{syt}(a, b) = 1$ ja $a|bc$, niin $a|c$. Osoitetaan tämä: Koska $\text{syt}(a, b) = 1$, löytyy sellaiset x ja y, että $1 = ax + by$ (tämä osataan, OK). Tästä seuraa, että $c = acx + bcy$, eli on kerrottu puolittain c:llä. Toisaalta, koska $a|bc$, niin on olemassa sellainen d, että $bc = ad$, koska a jakaa luvun bc. Sijoitetaan tämä tieto yhtälöön $c = acx + bcy$, jolloin

$$c = acx + bcy = acx + ady = a\overbrace{(cx + dy)}^{s} = as,$$

Mutta tämähän on sama asia kuin, että $a|c$. Älä hämäänny siitä, että c löytyy s:n lausekkeesta $cx + dy$. Tämä lauseke on toki pienempää kuin c, eihän se muuten voisi olla luvun c tekijänä. (Eli joko x tai y tai joku luku on negatiivinen.)

Jaollisuussääntöjen todistuksia (lisädiat)

Osoitetaan lukujen $2, 3, 4, 5, 6, 8, 9$ ja 11 jaollisuussäännöt:
Sitä varten olkoot luvun n numerot $a_k, a_{k-1}, \dots, a_0$, jolloin

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0.$$

2:lla jaollisuus: Koska $10 \equiv 0 \pmod 2$, on $10^i \equiv 0 \pmod 2$ kaikilla $i \geq 1$. Siksi $a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 \equiv 0 \pmod 2$, joten $n \equiv a_0 \pmod 2$, siis $2|n$, jos ja vain jos $2|a_0$. Tässä on käytetty kongruenssin säilymistä yhteen- ja kertolaskuissa – sääntöjä.

4:llä jaollisuus: Koska $100 \equiv 0 \pmod 4$, on $10^i \equiv 0 \pmod 4$ kaikilla $i \geq 2$. Siksi $a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_2 100 \equiv 0 \pmod 4$, joten $n \equiv a_1 10 + a_0 \pmod 4$, siis $4|n$, jos ja vain jos $4|(a_1 10 + a_0)$.

8:lla jaollisuus: Koska $1000 \equiv 0 \pmod 8$, on $10^i \equiv 0 \pmod 8$ kaikilla $i \geq 3$. Siksi $a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_3 1000 \equiv 0 \pmod 8$, joten $n \equiv a_2 100 + a_1 10 + a_0 \pmod 8$, siis $8|n$, jos ja vain jos $8|(a_2 100 + a_1 10 + a_0)$.

5:llä jaollisuus: Koska $10 \equiv 0 \pmod 5$, on $10^i \equiv 0 \pmod 5$ kaikilla $i \geq 1$. Siksi $a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 \equiv 0 \pmod 5$, joten $n \equiv a_0 \pmod 5$, siis $5|n$, jos ja vain jos $5|a_0$.

3:lla jaollisuus: Koska $10 \equiv 1 \pmod 3$, on $10^i \equiv 1 \pmod 3$ kaikilla $i \geq 1$. Tämä on voimassa myös, kun $i = 0$. Täten

$$a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0 \equiv a_k + \dots + a_0 \pmod 3$$

Siis $3|n$, jos ja vain jos $3|(a_k + a_{k-1} \dots + a_0)$.

9:llä jaollisuus: Kuten 3:lla jaollisuus, tarkastele kongruenssia $\pmod 9$

6:lla jaollisuus: Kuten aiemmin mainittiin, jos luku n on jaollinen luvuilla 2 ja 3, on luku n jaollinen myös luvulla 6.

11:sta jaollisuus: Koska $10 \equiv -1 \pmod{11}$, niin parillisilla i:n arvoilla on $10^i \equiv 1 \pmod{11}$ ja parittomilla $10^i \equiv -1 \pmod{11}$. Täten

$$a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0$$
$$\equiv a_0 + a_1 \cdot (-1)^1 + a_2 \cdot (-1)^2 + \dots + a_{k-1} \cdot (-1)^{k-1} + a_k \cdot (-1)^k$$
$$\equiv a_0 - a_1 + a_2 - \dots - a_{k-1} + a_k \pmod{11}$$