Kongruenssiyhtälö

Kongruenssi voi myös sisältää muuttujan x. Tällöin ne muuttujan x arvot, joilla kongruenssi on tosi, ovat kongruenssin *ratkaisuja*.
Kongruenssin *ratkaisemisella* tarkoitetaan sen kaikkien ratkaisujen määrittämistä. Ratkaisumenetelminä ovat

1. *kokeilu* ja
2. *palauttaminen vast. Diofantoksen yhtälön ratkaisemiseen*.

Lineaarinen kongruenssi on muotoa $ax \equiv b \pmod{n}$, jossa x on muuttuja ja a sekä b ovat annettuja lukuja $\in \mathbb{Z}$. Lisäksi sanotaan, että kongruenssit ovat *yhtäpitävät*, mikäli niillä on samat ratkaisut, esim. $15x \equiv 18 \pmod{12}$ ja $5x \equiv 6 \pmod{4}$ ovat yhtäpitävät.

Esimerkki 1 Ratkaise kongruenssi $3x \equiv 2 \pmod{5}$.
Kokeilemalla muuttujan x eri arvoja $x = 0, 1, 2, 3$ ja 4 havaitaan, että näistä $x = 4$ toteuttaa kongruenssin ja muut eivät (esim. taulukointi), eli $3 \cdot 4 = 12 \equiv 2 \pmod{5}$ ja $3 \cdot 2 = 6 \not\equiv 2 \pmod{5}$.

Esimerkki(jatkuu)
Kokeilla ei tarvitse tämän enempää, sillä nyt jokainen muotoa $4 + 5t, t \in \mathbb{Z}$ oleva luku toteuttaa kongruenssin ja muut eivät. Luvut 0 ja 5, 1 ja 6, 2 ja 7 jne. ovat ”samaa” jäännösluokkaa modulo 5.

x	$3x \equiv 2 \pmod{5}$	
0	$3 \cdot 0 = 0 \not\equiv 2 \pmod{5}$	EI
1	$3 \cdot 1 = 3 \not\equiv 2 \pmod{5}$	EI
2	$3 \cdot 2 = 6 \not\equiv 2 \pmod{5}$	EI
3	$3 \cdot 3 = 9 \not\equiv 2 \pmod{5}$	EI
4	$3 \cdot 4 = 12 \equiv 2 \pmod{5}$	OK
5	$3 \cdot 5 = 15 \not\equiv 2 \pmod{5}$	EI

Kongruenssin $3x \equiv 2 \pmod{5}$ *ratkaisujoukko* on $\{4 + 5t \mid t \in \mathbb{Z}\}$ ja usein ratkaisusta puhuttaessa tarkoitetaan nimenomaan ratkaisujoukkoa eikä yksittäistä ratkaisua. Voidaan myös sanoa, että tämän kongruenssin *yleinen ratkaisu* on $x = 4 + 5t$.

Esimerkki 2 Ratkaise kongruenssi $3x \equiv 2 \pmod{6}$.
Kokeilemalla havaitaan, ettei mikään luvuista $x = 0, 1, \ldots, 5$ toteuta tätä kongruenssia. Nyt voidaan päätellä (miksi?) ettei tällä kongruenssilla ole ratkaisuja, eli sen ratkaisujoukko on tyhjä joukko $\emptyset$.

Kokeiluun perustuen voidaan periaatteessa ratkaista mikä tahansa kongruenssiyhtälö. Kuitenkin, jos moduli n on hyvin suuri, tarvitaan paljon kokeiluja, jolloin menetelmä on työläs ja hidas.

Kongruenssi $ax \equiv b \pmod{n}$ on määritelmän nojalla yhtäpitävä yhtälön $ax - b = ny$, eli yhtälön $ax - ny = b$ kanssa, jollakin $y \in \mathbb{Z}$. Koska $y \in \mathbb{Z}$, niin voidaan kirjoittaa $ax + ny = b$. Näin on lineaarisen kongruenssiyhtälön ratkaiseminen palautettu Diofantoksen 1. asteen yhtälön ratkaisemiseen.

Lause, lineaarisen kongruenssin ratkeavuus:
Lineaarisella kongruenssilla $ax \equiv b \pmod{n}$ on ratkaisu (itse asiassa ∞ monta ratkaisua), jos ja vain jos b on $\text{syt}(a, n)$:n monikerta.

Todistus: Seuraa Diofantoksen yhtälön ratkeavuuslauseesta.

Esimerkki 3 Ratkaise kongruenssi $15x \equiv 18 \pmod{12}$ palauttamalla se Diofantoksen yhtälöön. (Huom. $18 \equiv 6 \pmod{12}$.)
Yhtäpitävä kongruenssi on $5x \equiv 6 \equiv 2 \pmod{4}$. Vastaava Diofantoksen yhtälö on $5x + 4y = 6$ (2). Ratkaistaan aluksi yhtälö $5x + 4y = 1$.

Esimerkki 3(jatkuu)
Eukleideen algoritmi antaa: $5 = 4 \cdot 1 + 1$, $4 = 1 \cdot 4 + 0$. Näin ollen $\text{syt}(5,4) = 1$ ja sytin lausekkeeksi saadaan: $1 = 5 \cdot 1 - 4 \cdot 1$, joka voidaan kirjoittaa muotoon $1 = 5 \cdot 1 + 4 \cdot (-1)$. Siis yksityis- ja yleinen ratkaisu yhtälölle $5x + 4y = 1$ on

$$\begin{cases} x_0 = 1 \\ y_0 = -1 \end{cases} \Rightarrow \begin{cases} x = 1 + 4t \\ y = -1 - 5t \end{cases}, \quad t \in \mathbb{Z}.$$

Ja yksityis-/yleinen ratkaisu yhtälölle $5x + 4y = 6$ on

$$\begin{cases} x_0 = 6 \\ y_0 = -6 \end{cases} \Rightarrow \begin{cases} x = 6 + 4t \\ y = -6 - 5t \end{cases}, \quad t \in \mathbb{Z}.$$

Tästä seuraa, että kongruenssin $5x \equiv 6 \pmod{4}$ ratkaisujoukko on

$$\{6 + 4t \mid t \in \mathbb{Z}\} \ (= \{2 + 4\hat{t} \mid \hat{t} \in \mathbb{Z}\}),$$

Toisin sanoen tämän kongruenssin yleinen ratkaisu on $x = 6 + 4t$.

Esimerkki 4 Ratkaise kongruenssiyhtälö

a) $13x \equiv 9 \pmod{25}$ **b)** $7x \equiv 5 \pmod{256}$

c) $2x + 7 \equiv 5x - 3 \pmod{8}$

Esimerkki 4 Ratkaise kongruenssiyhtälö

a) $13x \equiv 9 \pmod{25}$ **b)** $7x \equiv 5 \pmod{256}$

a) Ratkaistaan Diofantoksen yhtälö $13x - 25y = 9$.

Luvulle $\text{syt}(13, 25) = 1$ pätee yhtälö: $1 = 13 \cdot 2 - 25 \cdot 1$, josta edelleen $9 = 13 \cdot 18 - 25 \cdot 9$ Yksityis- ja yleinen ratkaisu on

$$\begin{cases} x_0 = 18 \\ y_0 = 9 \end{cases} \Rightarrow \begin{cases} x = 18 - \dfrac{25t}{\text{syt}(13,25)} = 18 - 25t \\ y = 9 - \dfrac{13t}{\text{syt}(13,25)} = 9 - 13t \end{cases}, \quad t \in \mathbb{Z}.$$

Koska $\text{syt}(13, 25) = 1$ ja koska $y \in \mathbb{Z}$, voidaan yhtälö kirjoittaa muotoon $13x + 25y = 9$, tällöin olisi $y_0 = -9$ ja $\begin{cases} x = 18 + 25t \\ y = -9 - 13t \end{cases}$.

Joka tapauksessa ratkaisu on $x = 18 - 25t, t \in \mathbb{Z}$.

b) Ratkaistaan yhtälö $7x - 256y = 5$. Nyt $\text{syt}(7, 256) = 1$, jolloin

$$1 = 7 \cdot (-73) - 256 \cdot (-2),$$

josta edelleen $5 = 7 \cdot (-365) - 256 \cdot (-10)$. Kongruenssin ratkaisu

$$x = -365 - 256t = \overbrace{147}^{-365-256\cdot(-2)} - 256t', \quad t, t' \in \mathbb{Z}.$$

c) $2x + 7 \equiv 5x - 3 \pmod{8}$. Muokataan aluksi kongruenssiyhtälö muotoon $3x \equiv 10 \pmod{8}$. Tätä vastaa Diofantoksen yhtälö

$$3x + 8y = 10.$$

Nyt $\text{syt}(3, 8) = 1$, jolloin ratkaisu on olemassa (luku 10 on luvun 1 monikerta, OK).

Eukleideen algoritmi antaa: $8 = 3 \cdot 2 + 2$, $3 = 2 \cdot 1 + 1$ ja $2 = 1 \cdot 2$. Sytin lausekkeeksi saadaan

$$1 = 3 \cdot 1 - 2 \cdot 1 = 3 \cdot 1 - (8 - 3 \cdot 2) \cdot 1 = 3 \cdot 3 + 8 \cdot (-1).$$

Tällöin

$$10 = 3 \cdot 30 + 8 \cdot (-10)$$

Yhtälön $3x \equiv 10 \pmod{8}$ yksityis- ja yleisratkaisuksi saadaan

$$\begin{cases} x_0 = 30 \\ y_0 = -10 \end{cases} \Rightarrow \begin{cases} x = 30 + 8t \\ y = -10 - 3t \end{cases}, \quad t \in \mathbb{Z}.$$

Kongruenssiyhtälön $2x + 7 \equiv 5x - 3 \pmod{8}$ ratkaisujoukko on siis

$$\{30 + 8t \mid t \in \mathbb{Z}\} = \{6 + 8\hat{t} \mid \hat{t} \in \mathbb{Z}\}.$$

Esimerkki (toisen asteen kongruenssiyhtälö), T – 208, LAUDATUR 11

Kun kyseessä on melko yksinkertainen toisen asteen kongruenssiyhtälö, voidaan hyödyntää taulukointia.

a) Kongruenssin $x^2 \equiv 1 \pmod 7$ tapauksessa saadaan:

$\boldsymbol{x}$,	$\boldsymbol{x^2}$,	$\boldsymbol{x^2 \equiv 1 \pmod 7}$	
0,	0 ,	$\mathbf{0} \not\equiv 1 \pmod 7$	
1,	1 ,	$\mathbf{1} \equiv 1 \pmod 7$,	OK
2,	4 ,	$\mathbf{4} \not\equiv 1 \pmod 7$	
3,	9 ,	$9 \equiv \mathbf{2} \not\equiv 1 \pmod 7$	
4,	16,	$16 \equiv \mathbf{2} \not\equiv 1 \pmod 7$	
5,	25,	$25 \equiv \mathbf{4} \not\equiv 1 \pmod 7$	
6,	36,	$36 \equiv \mathbf{1} \pmod 7$,	OK

VASTAUS: $x = 1$ tai $x = 6$ eli jaksollisuus huomioiden

$$\begin{cases} x = 1 + 7t \\ x = 6 + 7t \end{cases}, \quad \in \mathbb{Z}.$$

HUOM! Jos jatkettaisiin luvuille 7,8,9, jne. niin saataisiin modulosykli 0,1,4,2,2,4,1,0,1,4,2,2,4,1,0, … esiin.

b) Kongruenssi $x^2 \equiv 2 \pmod{17}$, taulukointi antaa:

$\boldsymbol{x}$	$\boldsymbol{x^2}$	$\boldsymbol{\text{mod } 17}$
0	0	0
1	1	1
2	4	4
3	9	9
4	16	16
5	25	8
6	36	2
7	49	15
8	64	13

$\boldsymbol{x}$	$\boldsymbol{x^2}$	$\boldsymbol{\text{mod } 17}$
9	81	13
10	100	15
11	121	2
12	144	8
13	169	16
14	196	9
15	225	4
16	256	1
17	289	0

Ja havaitaan jälleen tietty syklisyys: $0, 1, 4, 9, 16, 8, 2, 15, 13, 13, 15, 2, 8, 16, 9, 4, 1, 0$, jne. VASTAUS: $x = 6$ tai $x = 11$ eli jaksollisuus huomioiden

$$\begin{cases} x = 6 + 17t \\ x = 11 + 17t \end{cases}, \quad t \in \mathbb{Z}.$$