tehtävä 211

$29x + 11y = 1$

$syt\,(29,11) = 1$. Osoitetaan tämä eukleideen algoritmilla ja ratkaistaan yhtälö

	jakojäännökset	
$29 = 2 \cdot 11 + 7$	$7 = 29 - 2 \cdot 11$	A
$11 = 7 + 4$	$4 = 11 - 7$	B
$7 = 4 + 3$	$3 = 7 - 4$	C
$4 = 3 + 1$	$1 = 4 - 3$	D

1	$= 29x + 11y$	
1	$= 4 - 3$	D
	$= 4 - (7 - 4)$	C
	$= 4 - 7 + 4$	
	$= 2 \cdot 4 - 7$	
	$= 2 \cdot (11 - 7) - 7$	B
	$= 2 \cdot 11 - 2 \cdot 7 - 7$	
	$= 2 \cdot 11 - 3 \cdot 7$	
	$= 2 \cdot 11 - 3 \cdot (29 - 2 \cdot 11)$	A
	$= 2 \cdot 11 - 3 \cdot 29 + 6 \cdot 11$	
	$= -3 \cdot 29 + 8 \cdot 11$	
	$(x,y) = (-3,8)$	

yhtälön $29x + 11y = 13$ eräs ratkaisu saadaan kertomalla edelliset luvulla 13

$(x,y) = (-3 \cdot 13,8 \cdot 13) = (-39,104)$

tehtävä 212

$syt\,(15,8) = 1$, sillä $15 = 1 \cdot 3 \cdot 5$ ja $8 = 1 \cdot 2 \cdot 2 \cdot 2$

huomataan että yhtälön $15x + 8y = 1$ eräs ratkaisu on :

$\begin{cases} x = -1 \\ y = 2 \end{cases}$, sillä $15 \cdot (-1) + 8 \cdot 2 = -15 + 16 = 1$

Näin ollen yhtälön yleinen ratkaisu on

$\begin{cases} x = -1 + 8n \\ y = 2 - 15n \end{cases}$, missä $n \in \mathbb{Z}$

edellisen perusteella yhtälön $15x + 8y = 50$ eräs ratkaisu on

$\begin{cases} x = -50 \\ y = 100 \end{cases}$

jolloin yhtälön yleinen ratkaisu on

$\begin{cases} x = -50 + 8n \\ y = 100 - 15n \end{cases}$, missä $n \in \mathbb{Z}$

tehtävä 213

$37x + 27y = 1$

Koska luku 37 ei ole jaollinen millään luvulla, $syt\,(37,27) = 1$ ja yhtälöllä on ratkaisu

Hyödynnetään eukleideen algoritmia ratkaisun etsimiseen :

	jakojäännökset	
$37 = 27 + 10$	$10 = 37 - 27$	A
$27 = 2 \cdot 10 + 7$	$7 = 27 - 2 \cdot 10$	B
$10 = 7 + 3$	$3 = 10 - 7$	C
$7 = 2 \cdot 3 + 1$	$1 = 7 - 2 \cdot 3$	D

1	$= 37x + 27y$	
1	$= 7 - 2 \cdot 3$	D
	$= 7 - 2 \cdot (10 - 7)$	C
	$= 7 - 2 \cdot 10 + 2 \cdot 7$	
	$= 3 \cdot 7 - 2 \cdot 10$	
	$= 3 \cdot (27 - 2 \cdot 10) - 2 \cdot 10$	B
	$= 3 \cdot 27 - 6 \cdot 10 - 2 \cdot 10$	
	$= 3 \cdot 27 - 8 \cdot 10$	
	$= 3 \cdot 27 - 8 \cdot (37 - 27)$	A
	$= 3 \cdot 27 - 8 \cdot 37 + 8 \cdot 27$	
	$= -8 \cdot 37 + 11 \cdot 27$	

Yhtälön eräs ratkaisu on $\begin{cases} x = -8 \\ y = 11 \end{cases}$

Koska $syt\,(37,27) = 1$, on yhtälön yleinen ratkaisu

$\begin{cases} x = -8 + 27n \\ y = 11 - 37n \end{cases}$, missä $n \in \mathbb{Z}$

yhtälön $37x + 27y = 1000$ ratkaisu saadaan kertomalla edellisen ratkaisun vakiot luvulla 1000.

$\begin{cases} x = -8000 + 27n \\ y = 11000 - 37n \end{cases}$, missä $n \in \mathbb{Z}$

kokeillaan sieventää ratkaisua niin, että etsitään vakioksi lukuja, jotka ovat lähempänä nollaa

n	$-8000 + 27n$	$11000 - 37n$	
300	100	-100	
298	46	26	näistä mikä tahansa kelpaisi " erääksi ratkaisuksi "
297	19	11	
296	-8	48	

esimerkiksi $\begin{cases} x = 100 + 27n \\ y = -100 - 37n \end{cases}$ tai $\begin{cases} x = -8 + 27n \\ y = 48 - 37n \end{cases}$, $n \in \mathbb{Z}$

KONGRUENSSI

Kongruenssin avulla tutkitaan lukujen jakojäännöksiä, sekä erilaisten laskutoimitusten vaikutusta jakojäännöksiin.

täytyy tietää, minkä luvun suhteen jakojäännökset määritetään (mod n eli 'modulo n')

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

Luvut a ja b ovat kongruentit,

jos niiden erotus on jaollinen luvulla n

$17 \equiv 3 \pmod{7}$

tosi, koska $17 - 3 = 14 = 2 \cdot 7$

eli erotus $17 - 3$ on jaollinen luvulla 7

Luvut a ja b ovat kongruentit,

jos niillä on sama jakojäännös

(jaettaessa luvulla n)

$17 \equiv 3 \pmod{7}$

tosi, koska $17 = 2 \cdot 7 + 3$

eli luvun 1uvulla 17 on jakojäännöksenä 3

Jos jakolaskun $a : n$ jakojäännös *on* r, niin $a \equiv r \pmod{n}$

Ratkaise yhtälö $x \equiv 15 \pmod{7}$

$$x \equiv 15 \pmod{7}$$
$$x \equiv 1 \pmod{7}$$

$x - 1 = 7n$, missä $n \in \mathbb{Z}$

$x = 7n + 1$

$$x \equiv 15 \pmod{7}$$
$$x \equiv 1 \pmod{7}$$

$x = 7n + 1$, missä $n \in \mathbb{Z}$

Esim 2 s.97

Kongruenssi jakaa luvut ns. jäännösluokkiin sen perusteella, mikä niiden jakojäännös on

(mod 7) luvulla 7 jaettaessa, jakojäännös on 0,1,2,3,4,5,6

jakoyhtälö	*kongruenssi*
$a = 7n$	$a \equiv 0 \pmod 7$
$a = 7n + 1$	$a \equiv 1$
$a = 7n + 2$	$a \equiv 2$
$a = 7n + 3$	$a \equiv 3$
$a = 7n + 4$	$a \equiv 4$
$a = 7n + 5$	$a \equiv 5$
$a = 7n + 6$	$a \equiv 6$

Kongruenssi säilyy yhteenlaskussa, kertolaskussa ja potenssiin korotuksessa

⟶ kongruenssilaskuissa (ja jakojäännöksiä tutkittaessa), mikä tahansa luku voidaan korvata toisella samasta jäännösluokasta!

Esim. lukujen 27 ja 58 summan, tulon ja kolmannen potenssin jakojäännökset jaettaessa luvulla 5

ilman kongruenssia :	kongruenssin avulla :
	$27 \equiv 2 \pmod 5$ *ja* $58 \equiv 3 \pmod 5$
$27 + 58 = 85$, jakojäännös 0	$27 + 58 \equiv 2 + 3 \equiv 5 \equiv 0 \pmod 5$
$27 \cdot 58 = 1566 = 1565 + 1$, jakojäännös 1	$27 \cdot 58 \equiv 2 \cdot 3 \equiv 6 \equiv 1 \pmod 5$
$27^3 = 19683$, jakojäännös 3	$27^3 \equiv 2^3 \equiv 8 \equiv 3 \pmod 5$
$58^3 = 195112$, jakojäännös 2	$58^3 \equiv 3^3 \equiv 27 \equiv 2 \pmod 5$

Esim 3+4 s.101⟶

tehtävät 216, 217, 218, 220, 221, 222, 223, 226 (233-238)

Kongruenssi soveltuu erilaisiin "jaksollisiin" ilmiöihin

esim

luvun viimeinen numero 0,1,2,3,4,5,6,7,8 tai 9 (mod 10)

kellonajat 76 min = 1h 16 min $76 \equiv 16 \pmod{60}$

kellonviisarit samassa paikassa 12h välein
sama aika 24h välein

viikonpäivät toistuvat 7 vuorokauden välein

Esim 5+6 s. 102

Jäännösluokat soveltuvat jaollisuuden osoittamiseen

Esim jaollisuus luvulla 3:

aiemmin sijoitettiin n=3k, n=3k+1, n=3k+2

nyt voidaan tutkia $n \equiv 0$, $n \equiv 1$, $n \equiv 2$ (mod 3)

sijoitukset ja laskut ovat yksinkertaisemmat

(merkintöjen kanssa oltava tarkkana!)

Kuva s.98

Esim 7 s. 104

tehtävät 227 - 230, (239 - 242)

Jos kongruenssiyhtälöllä on ratkaisuja, niitä on ääretön määrä.

Ratkaise yhtälö $x \equiv 15 \pmod 7$

$$\begin{aligned} x &\equiv 15 \pmod 7 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

$x - 1 = 7n$, missä $n \in \mathbb{Z}$
$x = 7n + 1$

$$\begin{aligned} x &\equiv 15 \pmod 7 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

$x = 7n + 1$, missä $n \in \mathbb{Z}$

Jos jäännösluokat sijoitettavissa:

Ratkaise yhtälö

$2x - 1 \equiv 2 \pmod 5$

jäännösluokka	$2x - 1$	
$x \equiv 0$	$2 \cdot 0 - 1 \equiv -1$	$(mod\ 5)$
$x \equiv 1$	$2 \cdot 1 - 1 \equiv 1$	
$x \equiv 2$	$2 \cdot 2 - 1 \equiv 3$	
$x \equiv 3$	$2 \cdot 3 - 1 \equiv 5 \equiv 0$	
$x \equiv 4$	$2 \cdot 4 - 1 \equiv 7 \equiv 2$	*yhtälö toteutuu*

Yhtälön toteuttavat kaikki jäännösluokan 4 luvut

$x = 5n + 4$, missä $n \in \mathbb{Z}$

Jos jäännösluokat ei sijoitettavissa, esim (mod 17), voidaan aina palauttaa diofantoksen yhtälöksi:

Ratkaise yhtälö

$$\begin{aligned} 2x - 1 &\equiv 2 \pmod{17} \\ 2x &\equiv 3 \pmod{17} \end{aligned}$$

$2x = 17n + 3$

$2x - 17n = 3$, missä $x,n \in \mathbb{Z}$

etsitään ratkaisut diofantoksen yhtälölle $2x + 17y = 3$

Koska $syt\,(2,17) = 1$, etsitään ensin ratkaisu yhtälölle $2x + 17y = 1$

$18 - 17 = 1$, joten eräs ratkaisu on $(x,y) = (9, -1)$

ja yhtälön $2x + 17y = 3$ eräs ratkaisu on $(x,y) = (27, -3)$

yhtälön yleisen ratkaisun x – koordinaatit ovat kongruenssiyhtälön ratkaisuja

$x = 27 + 17 \cdot k$, missä $k \in \mathbb{Z}$

uusi kiintopiste saadaan sijoittamalla $k = -1$

$x = 10 + 17n$, missä $n \in \mathbb{Z}$

Jos ratkaisuja ei ole, niin

⟶ sijoitusmenetelmässä mikään rivi ei toimi

⟶ diofantoksen yhtälössä $c \neq n \cdot syt(a,b)$

Kongruenssin sovelluksia:

1.12 Esimerkki kryptologiasta

Kryptologia on salakirjoituksen teoriaa. Se tutkii systeemejä, joiden avulla muunnetaan kaikkien osapuolten ymmärtämä sanoma sellaiseen muotoon, jonka ymmärtävät vain ne, jotka pystyvät purkamaan salakirjoituksen.

Terminologiaa:

$$\text{selväteksti} \xrightarrow{\text{kryptaaminen}} \text{kryptoteksti} \xrightarrow{\text{dekryptaaminen}} \text{selväteksti}$$

Sovelluksia:

- tietojenkäsittelysysteemien tietosuoja (internet, matkaviestintä)
- kauppa-, sotilas- ja diplomatiaviestintä

Kryptologia jakautuu

- kryptografiaan, joka kehittää kryptosysteemejä
- kryptoanalyysiin, joka pyrkii purkamaan nämä systeemit

Tässä käsitellään aihetta lyhyesti yhden esimerkkisysteemin avulla. Esimerkki on luonteeltaan historiallinen kuriositeetti.

Caesarin systeemi

Selväteksti koostuu kirjainjonoista, jotka aluksi muutetaan lukujonoiksi niin, että jokainen kirjain (A, ..., Z) muutetaan luvuksi: A $\leftarrow 0, \ldots,$ Z $\leftarrow 25$.

Olkoon nyt p jokin selvätekstin luku (väliltä $0 - 25$). Merkitään vastaavaa kryptotekstin lukua symbolilla $f(p)$. (Symboli p tulee termistä "plain text" eikä siis tarkoita alkulukua.)

Kryptaaminen Caesarin systeemissä kryptoteksti muodostetaan kirjaimittain kaavalla

$$f(p) = (p+3) \bmod 26$$

eli kaavalla

$$f(p) \equiv p+3 \pmod{26} \quad \text{ja} \quad f(p) \in \{0, 1, \ldots, 25\}.$$

Esimerkki 1.12.1 Kryptataan END.

$$\text{END} \rightarrow 4\ 13\ 3 \rightarrow 7\ 16\ 6 \rightarrow \text{HQG}.$$

Dekryptaaminen Kryptoteksti puretaan kaavalla

$$p \equiv f(p) - 3 \pmod{26} \quad \text{ja} \quad p \in \{0, 1, \ldots, 25\}$$

eli kaavalla

$$p = (f(p) - 3) \bmod 26.$$

Esimerkki 1.12.2 Dekryptataan EBH.

$$\text{EBH} \leftarrow 4\ 1\ 7 \leftarrow 1\ 24\ 4 \leftarrow \text{BYE}.$$

Ratkaise kongruenssi $15x \equiv 18 \pmod{12}$

Esimerkki 4 Ratkaise kongruenssiyhtälö

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

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

Kongruenssin $x^2 \equiv 1 \pmod{7}$

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

4. Vastaa kiinalaisen munkin Sun Zin kysymykseen: Onko lukua $x \in \mathbb{Z}$, jolle lineaariset kongruenssiyhtälöt

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

ovat totta?

Harjoitustehtävä 5.8. Miten muodostuu jäännösluokkien joukko $\mathbb{Z}_5$?

Harjoitustehtävä 5.9 (Kielentämistehtävä). Laske jakojäännös, kun $17^3 + 5^{84}$ jaetaan luvulla 12. Selitä kokonaisilla lauseilla ratkaisun kulkua.

Harjoitustehtävä 5.10. Ratkaise kongruenssiyhtälö $5x \equiv 2 \pmod{6}$.

Harjoitustehtävä 5.11. Ratkaise kongruenssiyhtälö $11x \equiv 3 \pmod{7}$.

Harjoitustehtävä 5.12. Ville sai joululahjaksi lahjakortin elektroniikkakauppaan. Hän aikoo ostaa DVD -elokuvia ja CD -levyjä. DVD -elokuvat maksavat 17€ kappale ja CD-levyt 9€ kappale. Ostokset tekivät yhteensä 113€. Kuinka monta DVD -elokuvaa ja CD -levyä Ville osti?

Harjoitustehtävä 5.13 (Kielentämistehtävä). Tehtävänä on todistaa kongruenssin ja Diofantoksen yhtälön teoriaan liittyvä lause täyttämällä todistuksesta puuttuvat aukot. Lause on muotoa:

Jos syt(a,m)=1, niin kongruenssilla $ax \equiv c \pmod{m}$ *on yksikäsitteinen ratkaisu* $x \in \mathbb{Z}$ *välillä* $0 \leq x \leq m - 1$..

Todistus. Oletuksen nojalla on olemassa sellaiset 1._____ u ja v, että $au + mv =$ 2._____ ja siis

$$a(uc) + m(vc) = c.$$

Tämän perusteella kongruenssilla on ratkaisu 3._____. Ratkaisuja ovat myös edellä mainitun ratkaisun lisäksi kongruentit luvut $x =$ 4._____, missä 5._____ on jokin kokonaisluku. Kongruessin ominaisuuksien perusteella kaikki ratkaisut ovat keskenään kongruentteja mod m, sillä

$$ax_1 \equiv ax_2 \pmod{m} \Rightarrow 6.\_\_\_\_\_ \pmod{m}.$$

Lopputuloksena siis ratkaisuista tarkalleen 7._____ on välillä $0 \leq x \leq m - 1$. [14] □

1.11.1 Ratkaistaan kongruenssi $139x \equiv 8 \pmod{3}$.

Ratkaistaan kongruenssi $16x \equiv 3 \pmod{8}$.

Ratkaistaan kongruenssi $15x \equiv 9 \pmod{152}$.

Ratkaistaan kongruenssi $18x \equiv 3 \pmod{15}$.

Ratkaistaan kongruenssi $22x \equiv 4 \pmod{30}$.