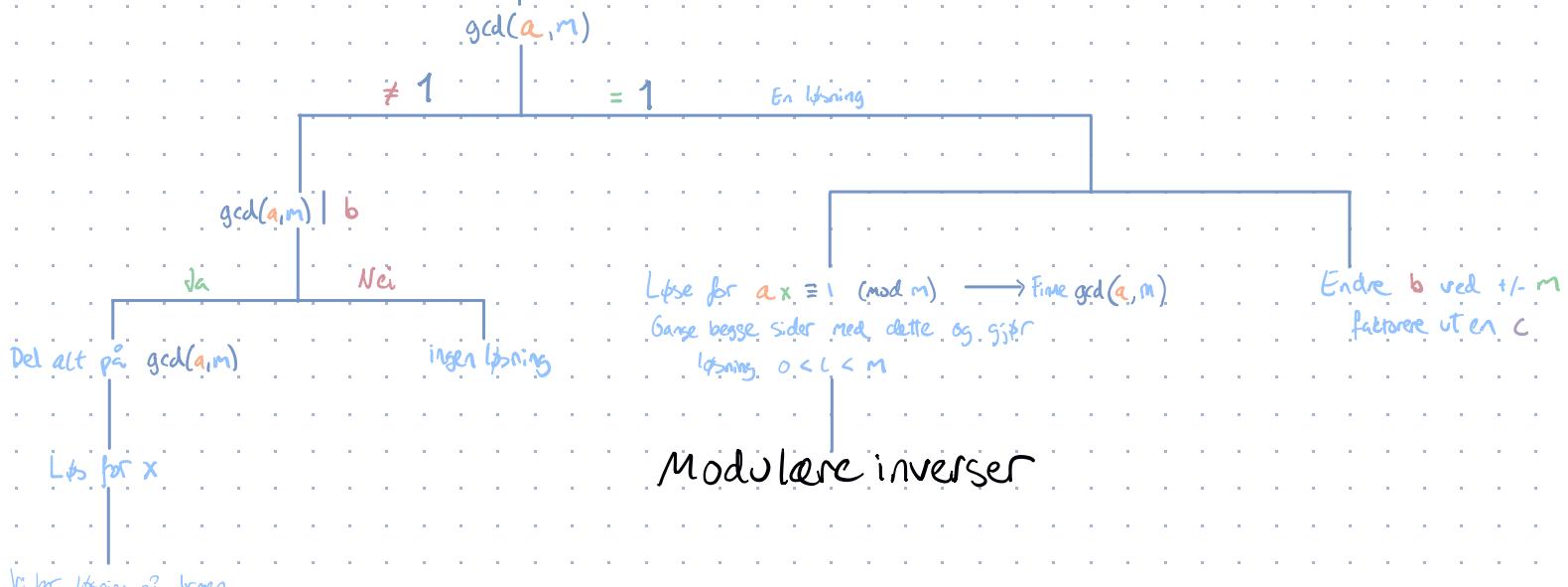


Løse kongruensligninger $ax \equiv b \pmod{m}$

Ligningssystem

Kinesiske restteoremet



Løsningene er $f + g, f + g + g, f + g + g + g$

Definisjoner

1

Kongruens

Disse betyr det samme:

- a er kongruent med b mod m
- $m \mid a - b$
- $a \equiv b \pmod{m}$ a og b har samme rest i universet M
- $a \text{ mod } m = b \text{ mod } m$

Eks: $50 \equiv 2 \pmod{12}$

$$50 \text{ mod } 12 = 2 \quad \text{og} \quad 2 \text{ mod } 12 = 2$$

Oppskrifter

1 Løse kongruens ligninger

Hva kan vi gjøre:

- Pluss og minus begge sider
- Endre svar ved å leggetil / trekke fra m [for å få svar $0 \leq x < m$]

Metoder:

- Felles faktor c slik at vi får $c \cdot a \equiv c \cdot b$

3 muligheter

- $\gcd(c, m) = 1$

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

- $d = \gcd(c, m) \neq 1$

$$a \equiv b \pmod{m/d}$$

Merk: Her ender

vi m

- $\text{mod}(p)$ og $p + c$

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

- Finne invers i for a

$$i \cdot a \cdot x \equiv i \cdot b \pmod{m}$$

$$x \equiv i \cdot b$$

2 Finne invers til $a \pmod{m}$

i er en invers til a mod m dersom $i \cdot a \equiv 1 \pmod{m}$

- a har en invers hvis og bare hvis $a \perp m$

- Løse $ax \equiv 1 \pmod{m}$ for x

3

Løse kongruens - flere løsninger

Hvordan vet vi: $\gcd(a, m) \neq 1$ og $\gcd(a, m) \mid b$

Hvor mange løsninger: $c = \gcd(a, m)$ løsninger

- Oppskrift:
- Del alle ledd på $c = \gcd(a, m)$. Fortsett å dele hvis man kan det.
 - Løs ligningen $a/c x \equiv b/c \pmod{m/c}$
 - Når har man $x = f \pmod{g}$. Det finnes c løsninger innenfor den opprinnelige modulusen m .
- $f, f+g, f+g+g, f+g+g+g, \dots$

$$x = f + g \cdot k \pmod{m} \quad \text{for } 0 \leq k \leq c.$$

3 Det kinesiske restteoremet

$m \perp n$: Vi har noen ligninger

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_3 \pmod{m_3}$$

Vet at $x = (a_1 k_1 M_1) + (a_2 k_2 M_2) + \dots + (a_3 k_3 M_3) \pmod{M}$

Finner tallene:

M :

$$M = m_1 \cdot m_2 \cdot m_3$$

$$M_1 = M / m_1$$

$$M_2 = M / m_2$$

$$M_3 = M / m_3$$

k :

$$M_1 k_1 \equiv 1 \pmod{m_1}$$

$$M_2 k_2 \equiv 1 \pmod{m_2}$$

$$M_3 k_3 \equiv 1 \pmod{m_3}$$

Eks:

V: har

$$x \equiv 1 \pmod{3}$$

$$x \equiv 3 \pmod{4}$$

$$x \equiv 2 \pmod{5}$$

$$a_1 = 1 \quad M_1 = 20$$

$$a_2 = 3 \quad M_2 = 15$$

$$a_3 = 2 \quad M_3 = 12$$

$$M_1 k_1 = a_1 \pmod{m_1} : 20 k_1 \equiv 1 \pmod{3}$$

$$20 k_1 \equiv 1 \pmod{3}$$

$$5 k_1 \equiv 1 \pmod{3}$$

$$5 k_1 \equiv 10 \pmod{3}$$

$$k_1 \equiv 5 \pmod{3}$$

$$k_1 = 2$$

$$M_2 k_2 = a_2 \pmod{m_2} \quad 15 k_2 \equiv 1 \pmod{4}$$

$$15 k_2 \equiv 1 \pmod{4}$$

$$3 k_2 \equiv 1 \pmod{4}$$

$$k_2 = 3 \pmod{4}$$

$$M_3 k_3 = a_3 \pmod{m_3} \quad 12 k_3 \equiv 1 \pmod{5}$$

$$4 k_3 \equiv 1 \pmod{5}$$

$$3 \equiv 9 \pmod{5}$$

$$k_3 = 3$$

$$x = (1 \cdot 20 \cdot 2) + (3 \cdot 15 \cdot 3) + (2 \cdot 12 \cdot 3) \pmod{60}$$

$$x = 247 \pmod{60}$$

$$x = 7$$

$m \nmid n$: - Se om noen moduler er i konflikt med hverandre

Vet at $x \equiv a \pmod{mn}$ er det samme som

$$x \equiv a \pmod{m} \wedge x \equiv a \pmod{n}$$

Merk:

Bare dersom m og n er relativt primstørre

Hvis 2 ligninger har like faktorer og a er forskjellig er de i konflikt

Eks:

$$x \equiv 12 \pmod{20}$$

$$x \equiv 29 \pmod{35}$$

Vi får: $x \equiv 12 \pmod{4} \wedge x \equiv 12 \pmod{5}$

$$x \equiv 0 \pmod{4} \wedge x \equiv 2 \pmod{5}$$

$$x \equiv 29 \pmod{7} \wedge x \equiv 29 \pmod{5}$$

$$x \equiv 1 \pmod{7} \wedge x \equiv 4 \pmod{5}$$

Dette er i konflikt da $x \pmod{5}$ må være både 2 og 4

- Skrive om slik at vi får parvis primstørre moduler

Dele opp og skyfe de uavkortige

Eks:

$$x \equiv 3 \pmod{4}$$

$$x \equiv 0 \pmod{7}$$

$$x \equiv 5 \pmod{9}$$

$$x \equiv 11 \pmod{12}$$

Skriver opp alle med moduler delt opp

$$x \equiv 3 \pmod{4}$$

$$x \equiv 0 \pmod{7}$$

$$x \equiv 5 \pmod{9}$$

$$x \equiv 11 \pmod{5} \Rightarrow x \equiv 2 \pmod{3}$$

$$x \equiv 11 \pmod{4} \quad \text{kan slette denne for: } x \equiv 3 \pmod{4}$$

Vi merker her at da som $x \equiv 5 \pmod{9}$ så må $x \equiv 2 \pmod{3}$, men ikke nødvendigvis motsatt. Kan derfor skrive $x \equiv 2 \pmod{3}$

Står igjen med:

$$x \equiv 3 \pmod{4}$$

$$x \equiv 0 \pmod{7}$$

$$x \equiv 2 \pmod{3}$$

$$a_1 = 3 \quad M_1 = 63$$

$$a_2 = 0 \quad M_2 = 36$$

$$a_3 = 2 \quad M_3 = 28$$

$$63 \cdot k_1 \equiv 1 \pmod{4}$$

$$k_1 = 3$$

$$36 \cdot k_2 \equiv 1 \pmod{7}$$

$$k_2 = 1$$

$$28 \cdot k_3 \equiv 1 \pmod{9}$$

$$k_3 = 1$$

$$x \equiv [3 \cdot 63 \cdot 3] + [0 \cdot 36 \cdot 1] + [2 \cdot 28 \cdot 1] \pmod{252}$$

$$x \equiv 207 \pmod{252}$$

$$x = 207$$

Viktige detaljer

1

$a \text{ mod } b$ og $a \equiv b \pmod{m}$ er ikke samme mod.

- $a \text{ mod } b$ er rest når vi deler a med b .

- $a \equiv b \pmod{m}$ er at a og b har samme rest i universet m .

2

En kongruensligning $x \equiv a \pmod{mn}$ kan deles opp til to

ligninger $x \equiv a \pmod{m}$ og $x \equiv a \pmod{n}$ bare hvis $m \perp n$