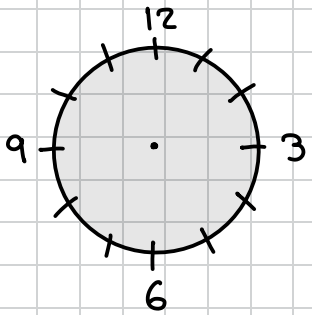
Forelesning 13

KONGRUENSREGNING

- Kongruens og klokkearitmetikk
  $a \equiv b \pmod m$
- Regneregler for kongruenser
  $a \pm k \equiv b \pm k \pmod m$, og lignende
- Modulære inverser
  $a^{-1} \cdot a = 1 \pmod m$
- Modulære potenser
  $a^n \bmod m$ for store n
- Diskrete logaritmer
  $x \equiv \log_a b \pmod m \Leftrightarrow a^x \equiv b \pmod m$

Klokkearitmetikk



På en analog klokke er f.eks.
2 og 14 ekvivalente

Hvis klokka er 10 nå så er den
14 = 2 om fire timer

På en måte er 10 + 4 = 2

Mer korrekt sier vi at vi regner "modulo 12" på en slik klokke og at
"14 er kongruent med 2 modulo 12"

Med symboler skriver vi $14 \equiv 2 \pmod{12}$
Tilsvarende er $21 \equiv 9 \pmod{12}$ og $24 \equiv 12 \equiv 0 \pmod{12}$

Definisjon

La a, b og m være heltall med $m > 0$.
Hvis m deler a − b, sier vi at
a er kongruent med b modulo m
og vi skriver
$a \equiv b \pmod m$

(Dette er det samme som at $m \mid (a-b)$ eller at $a - b = q \cdot m$ eller $a = q \cdot m + b$)

Dersom $m|a$ så er $a \equiv 0 \pmod m$.
Eks: $36 \equiv 24 \equiv 12 \equiv 0 \pmod{12}$ og $21 \equiv 0 \pmod 7$

Videre har vi f.eks. at
$34 \equiv 22 \equiv 10 \pmod{12}$
men $16 \not\equiv 5 \pmod{12}$ fordi $12 \nmid (16-5)$

likhetstegn ↓

Merk: $\equiv$ oppfører seg ofte (men ikke alltid) som $=$

Eksempel

$x + 8 \equiv 1 \pmod{11}$
$x \equiv 1 - 8 \pmod{11}$
$x \equiv -7 \pmod{11}$
$x \equiv 4 \pmod{11}$

Kan skrive $x \equiv 1 - 8 = -7 \equiv 4 \pmod{11}$

Regneregler

① $a \equiv b \pmod m \Rightarrow a \pm k \equiv b \pm k \pmod m$

② $a \equiv b \pmod m \Rightarrow a \cdot k \equiv b \cdot k \pmod m$

③ $a \equiv b \pmod m \Rightarrow a \equiv b \pm m \pmod m$

Men!

$a \cdot k = b \cdot k \pmod m \not\Rightarrow a \equiv b \pmod m$

Moteksempel: $18 \equiv 10 \pmod 8$, men $9 \not\equiv 5 \pmod 8$
($18 = 9 \cdot 2$, $10 = 5 \cdot 2$)
(fordi: $9 \equiv 1 \pmod 8$)

Men vi kan vise at
$a \cdot k \equiv b \cdot k \pmod m \Rightarrow a \equiv b \left(\mod \frac{m}{\gcd(k,m)}\right)$

Vi har f.eks. at
$\gcd(2,8) = 2$ så $18 \equiv 10 \pmod 8$
$\Rightarrow 9 \equiv 5 \pmod{8/2}$
$9 \equiv 5 \pmod 4$
(Fordi både 9 og 5 er kongruente med $1 \pmod 4$)

$a \bmod b$ vs. $a \equiv b \pmod m$

$a \bmod b$ er resten vi får når vi deler a på b.
(Eks: $7 \bmod 3 = 1$ fordi $7 = 2 \cdot 3 + 1$)

Dette er ikke <u>helt</u> samme mod som i $a \equiv b \pmod m$ men de har en sammenheng.

Dersom $a \equiv b \pmod m$ har a og b samme rest når de deles på m.

M.a.o. $a \equiv b \pmod m$ hvis og bare hvis
$a \bmod m \equiv b \bmod m$

Så $a \bmod m \equiv r$ der r oppfyller både
$a \equiv r \pmod m$ og $0 \leq r < m$

Eksempel

$17 \bmod 7 = 3$ fordi $17 = 2 \cdot 7 + 3$
og $38 \bmod 7 = 3$ fordi $38 = 5 \cdot 7 + 3$

Så $38 \equiv 17 \pmod 7$
(og forøvrig $17 \equiv 10 \equiv 3 \pmod 7$)

Modulære inverser

Si vi ønsker å løse ligningen $ax \equiv b \pmod m$.
Vi kan ikke gange med $\frac{1}{a}$, for vi jobber kun med heltall.

Vi kan gjøre noe lignende, nemlig finne et tall c slik at $c \cdot a \equiv 1 \pmod m$

Dette kaller vi ofte for a^{-1} ("a invers")
Da vil $ax \equiv b \pmod m$
$a^{-1}ax \equiv a^{-1}b \pmod m$
$x \equiv a^{-1}b \pmod m$

Definisjon

La $a, c, m \in \mathbb{Z}$ med $m > 0$.
Hvis $c \cdot a \equiv 1 \pmod m$, sier vi at c er en invers til a modulo m.

Eksempel

Løs ligningen $3x \equiv 2 \pmod 5$

Hvis vi regner mod 5 får vi

$1 \cdot 3 \equiv 3$ $\quad$ $3 \cdot 3 = 9 \equiv 4$
$2 \cdot 3 = 6 \equiv 1$ $\quad$ $4 \cdot 3 = 12 \equiv 2$

} Vi ser at $3 \cdot 2 \equiv 1 \pmod 5$ så 2 er en invers til 3 modulo 5

Vi får da $3x \equiv 2 \pmod 5$

$3^{-1} \cdot 3x \equiv 3^{-1} \cdot 2 \pmod 5$

$x \equiv 3^{-1} \cdot 2 \pmod 5$

$x \equiv 2 \cdot 2 \equiv 4 \pmod 5$

Eksempel

Hva med $3x \equiv 2 \pmod 6$?

Modulo 6 har vi

$3 \cdot 1 \equiv 3$ $\quad$ $3 \cdot 4 = 12 \equiv 0$
$3 \cdot 2 = 6 \equiv 0$ $\quad$ $3 \cdot 5 = 15 \equiv 3$
$3 \cdot 3 = 9 \equiv 3$

} 3 har ingen invers modulo

Når har a en invers modulo m?

Merk at $ax \equiv 1 \pmod m$ betyr at

$m \mid (ax - 1)$

eller $ax - 1 = mq$

eller $ax + m \cdot (-q) = 1$

Så $a^{-1} \pmod m$ eksisterer $\iff ax \equiv 1 \pmod m$ har løsning

$\iff ax + my = 1$ har løsning

$\iff \gcd(a, m) = 1$

$\iff a \perp m$

Så a har en invers modulo m hvis og bare hvis a og m er relativt primiske.

Eksempel

Hvis m er et primtall har <u>alle</u> tall inverser (bortsett fra $0 \equiv m \equiv 2m \equiv n \cdot m \pmod m$)

Hvis f.eks. $m = 5$, har vi

$1 \cdot 1 \equiv 1 \pmod 5$
$2 \cdot 3 \equiv 1 \pmod 5$
$3 \cdot 2 \equiv 1 \pmod 5$
$4 \cdot 4 \equiv 1 \pmod 5$

Modulære potenser

Hvordan kan vi regne ut ting som 3^{371} mod 5?

Vi starter med litt mindre potenser

$3^2 \equiv 9 \equiv 4 \pmod 5$
$3^3 \equiv 3^2 \cdot 3 \equiv 4 \cdot 3 = 12 \equiv 2 \pmod 5$
$3^4 \equiv 3^3 \cdot 3 \equiv 2 \cdot 3 = 6 \equiv 1 \pmod 5$ ← Dette kan vi bruke!

Merk at $3^{4 \cdot k} = (3^4)^k \equiv 1^k \equiv 1 \pmod 5$

Heltallsdivisjon av 371 på 4 gir $371 = 92 \cdot 4 + 3$

Vi får

$3^{371} = 3^{92 \cdot 4 + 3} = (3^4)^{92} \cdot 3^3 \equiv 1^{92} \cdot 3^3 \equiv \underline{2 \pmod 5}$

En annen strategi hvis vi ikke finner en liten k slik at $a^k \equiv 1 \pmod m$? Toerpotenser

Eksempel

Regn ut 5^{22} mod 77. Merk at $22 = 16 + 4 + 2$

$5^2 \equiv 25 \pmod{77}$
$5^4 \equiv (5^2)^2 \equiv 25^2 \equiv$
$5^8 \equiv (5^4)^2 \equiv 9^2 \equiv 81 \equiv 4 \pmod{77}$
$5^{16} \equiv (5^8)^2 \equiv 4^2 \equiv 16 \pmod{77}$

$5^{22} = 5^{16+4+2} = 5^{16} \cdot 5^4 \cdot 5^2 \equiv 16 \cdot 9 \cdot 25 = 3600 \equiv \underline{58 \pmod{77}}$