Afsnit 4.1 – fortsat

Kongruens kan defineres på mange måder:

Def. 4.1.3 ⇕ $a \equiv b \pmod{n}$

$m \mid (a-b)$ (*)

Sætn. 4.1.3 ⇕ $a \bmod m = b \bmod m$

Sætn. 4.1.4 ⇕ $\exists k \in \mathbb{Z} : a = b + km$ (**)

Bevis for Sætning 4.1.3: Opgave 4.1.13

Bevis for Sætning 4.1.4:

(**) er en ren omskrivning af (*):

$m \mid (a-b)$

Def. 4.1.1 ⇕ $a - b = km, \quad k \in \mathbb{Z}$

⇕ $a = b + km, \quad k \in \mathbb{Z}$

Eks:

$5 \equiv 15 \pmod 5$? $\quad 15-5 = 10 = 2 \cdot 5$ ✓

$7 \equiv 16 \pmod 5$? $\quad 16-7 = 9 = 5+4$ ✗

$7 \equiv 16 \pmod 3$? $\quad 16-7 = 3 \cdot 3$ ✓

Sætning 4.1.5:

Lad $m \in \mathbb{Z}^+$. Da gælder

$$\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d \pmod m \\ ac \equiv bd \pmod m \end{cases}$$

(Man må addere og gange med det "samme" tal på begge sider.)

Eks:

$$5 \equiv 8 \pmod 3$$
$$4 \equiv 10 \pmod 3$$
$$\Rightarrow \begin{cases} 9 \equiv 18 \pmod 3 & \text{(addr på begge sider)} \\ 20 \equiv 80 \pmod 3 & \text{(mult. ——— " ———)} \end{cases}$$

Må man trække det "samme" tal fra på begge sider?

Ja: $c \equiv d \pmod m \iff -c \equiv -d \pmod m$

Må man dividere med det "samme" tal på begge sider, hvis det går op?

Nej, ikke generelt:

- $20 \equiv 30 \pmod 5$, men $4 \not\equiv 6 \pmod 5$

Bevis: (lidt anderledes end bogen, som bruger Sætn 4.1.4 til begge)

$$a \equiv b \pmod m \quad \wedge \quad c \equiv d \pmod m$$

Def 4.1.3 $\Updownarrow$

$$m \mid (a-b) \quad \wedge \quad m \mid (c-d)$$

Sætn. 4.1.1 (i) $\Downarrow$

$$m \mid (a-b+c-d)$$

$\Updownarrow$

$$m \mid ((a+c)-(b+d))$$

Def. 4.1.3 $\Uparrow$

$$a+c \equiv b+d \pmod m$$

$$a \equiv b \pmod m \quad \wedge \quad c \equiv d \pmod m$$

Sætn. 4.1.4 $\Updownarrow$

$$a = b + km \quad \wedge \quad c = d + \ell m \,, \quad k, \ell \in \mathbb{Z}$$

$\Downarrow$

$$a \cdot c = (b+km)(d+\ell m) \,, \quad k, \ell \in \mathbb{Z}$$

$\Downarrow$

$$a \cdot c = bd + b\ell m + kmd + k\ell m^2$$

$$= bd + \underbrace{(b\ell + kd + k\ell m)}_{\in \mathbb{Z}} m$$

Sætn 4.1.4 $\Updownarrow$

$$ac \equiv bd \pmod m$$

Korollar 4.1.2 :

Lad $a, b \in \mathbb{Z}$ og $m \in \mathbb{Z}^+$. Da gælder

- $(a+b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$
- $ab \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$

Praktisk, da det kan spare en for at regne med store tal.

Bevis:

$$a \equiv (a \bmod m) \pmod m$$
$$b \equiv (b \bmod m) \pmod m$$

Eks:

$$12 \equiv 2 \pmod 5$$
$$24 \equiv 4 \pmod 5$$

D.u.s.

$a+b \equiv (a \bmod m) + (b \bmod m) \pmod m$, iflg. Sætn. 4.1.5

Sætn. 4.1.3 $\Updownarrow$ $(a+b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$

Og $a \cdot b \equiv (a \bmod m)(b \bmod m) \pmod m$, iflg. Sætn. 4.1.5

Sætn. 4.1.3 $\Updownarrow$ $ab \bmod m = \big((a \bmod m)(b \bmod m)\big) \bmod m$

Afsnit 4.5: Anvendelser af kongruenser

- Hash-funktioner (behandles i DM507)
- Pseudo-tilfældige tal

  Simpel og hurtig metode:

  $X_{n+1} = aX_n + c \mod m$

  X_0 kaldes „seed".

  Ekstra hurtig, hvis m er en 2-potens (hvorfor?)

  $\gcd(a, m) = 1$ giver længst periode
- Check-cifre

  Eks: Paritets-bit

  (Detekterer et ulige # bit-fejl)

  Eks: ISBN10: $X = X_1 X_2 \cdots X_{10}$

  $X_{10} \in \{0, 1, \ldots, 9, X\}$ ← repr. 10

  $$X_{10} = \sum_{i=1}^{9} iX_i \mod 11$$

  ↑ så „ombytningsfejl" kan detekteres

Kryptering:

Cæsar-koder

- Hemmelig nøgle
- Let at knække v.h.a. frekvensanalyse

RSA

- Offentlig nøgle (kryptering) + hemmelig nøgle (dekryptering)
- Frekvensanalyse duer ikke

RSA: Rivest, Shamir, Adleman
↖ DM507 - Log

Offentlig nøgle: (n, e)

- $n = pq$, p, q meget store primtal
  aktuel anbefaling: n skal have ≥ 2048 bits
- $\gcd(e, (p-1)(q-1)) = 1$
  ↖ greatest common divisor

$P(M) = M^e \bmod n$
↖ Public

Hemmelig nøgle: (n, d)

- $n = pq$
- $de \equiv 1 \pmod{(p-1)(q-1)}$

$S(C) = C^d \bmod n$
↖ Secret

Eks 8:

$p = 43$
$q = 59$
$\Rightarrow \quad n = 43 \cdot 59 = 2537$

$(p-1)(q-1) = 42 \cdot 58 = \underbrace{2 \cdot 3 \cdot 7 \cdot 2 \cdot 29}_{\text{13 optræder ikke}} = 2436$

$\gcd(13, 42 \cdot 58) = 1$

$e = 13$

Offentlig nøgle: $(2537, 13)$

$937 \cdot e = 937 \cdot 13 = 5 \cdot 2436 + 1$

$d = 937$

Privat nøgle: $(2537, 937)$

Kryptering

- Omskriv hvert bogstav til et tal (som i Cæsarkode)
  Eks: $a = 00$, $b = 01$, ..., $o = 14$, ..., $s = 18$, ...
- Gruppér tallene i blokke, så hver blok repræsenterer et tal $< n$.
  Eks: stop
  $M = \underbrace{1819}_{M_1}\underbrace{1415}_{M_2}$
- Beregn $C_i = P(M_i) = M_i^e \bmod n$
  Eks: $C_1 = 1819^{13} \bmod 2537 = 2081$
  $C_2 = 1415^{13} \bmod 2537 = 2182$
  $C = 20812182$

Dekryptering:

- Beregn $M_i = S(C_i) = C_i^d \bmod n$

  Eks: $M_1 = 2081^{937} \bmod 2537 = 1819$

  $M_2 = 2182^{937} \bmod 2537 = 1415$

  $\Rightarrow M = 1819\,1415$

- Oversæt tal til bogstaver

  Eks: 18 19 14 15 ↝ stop

Der gælder altid (som i eks. ovenfor), at

$S(P(M)) = M$.

Bevises vha. Fermats Lille Sætning, Kinesiske Restklasse-Sætning og mod-regneregler

↖ gennemgås om to uger

Der gælder også, at

$P(S(M)) = M$

Kan bl.a. udnyttes til at lave digital signatur:

- Anvend „sikker" hash-funktion h til at opnå en „kort version" af M (små ændringer i M giver ændring i $h(M)$)
- Anvend privat nøgle på $h(M)$
- Send $(M, S(h(M)))$

Hvis $P(S(h(M))) = h(M)$, er det meget usandsynligt, at underskriften er falsk.