



- 1 a)  $A \times A = \{(x, x), (x, y), (y, x), (y, y)\}$   
 $A \times B = \{(x, x), (x, y), (x, z), (y, x), (y, y), (y, z)\}$

b)

$$\sum_{n=0}^{|A \times B|} \binom{|A \times B|}{n} = 2^{|A \times B|} = 64$$

- c) Det finnes  $2^4 = 16$  mulige binæroperasjoner på  $A$  og  $3^9 = 19683$  binæroperasjoner på  $B$ .
- d) Det er  $3^2 = 9$  funksjoner fra  $A$  til  $B$ . 6 er 1-1, ingen er på og ingen er isomorfier. Det er  $2^3 = 8$  funksjoner fra  $B$  til  $A$ . Ingen er 1-1, 6 er på og ingen er isomorfier.
- e) Det finnes 27 funksjoner fra  $B$  til  $B$ . Av disse er 6 stykker 1-1, på og isomorfier.

- 2 a) Anta at  $a \equiv b \pmod{n}$  og  $b \equiv c \pmod{n}$ . Da vet vi at det eksisterer heltall  $r, s$  slik at  $a = b + rn$ ,  $b = c + sn$ . Dermed får vi at

$$a = b + rn = c + rn + sn = c + (r + s)n,$$

og dermed har vi at  $a \equiv c \pmod{n}$

- b) Beviset er en mindre generell versjon av beviset i c).
- c) Anta at  $m, n \in \mathbb{Z}$  og  $n > 0$ . Ved å betrakte tallinjen, ser vi at det må eksistere et heltall  $q$  slik at

$$qn \leq m < (q + 1)n.$$

Hvis  $qn = m$ , kan vi velge  $r = 0$ . Hvis derimot  $qn \neq m$  velger vi  $r = m - qn$ . Vi har da  $m = qn + r$  og  $0 \leq r < n$ .

For å vise unikhethet av  $q$  og  $r$ , anta at  $qn + r = m = pn + s$ , der  $0 \leq s, r < n$ . Da har vi at  $qn = pn + s - r$ . Siden  $-n < s - r < n$  og  $n|s - r$ , må vi ha  $s = r$ . Vi ser da at  $qn = pn$ , så dermed er  $q = p$ .

Se eventuelt 6.3, side 60 i boka.

- d) Anta at  $a \equiv b \pmod{n}$   
La  $r$  være resten når  $a$  deles på  $n$ ; da vet vi at  $n|(a - r)$ . Dermed har vi at  $a \equiv r \pmod{n}$ , og dermed at  $b \equiv r \pmod{n}$ . Da må  $n|(b - r)$ , og vi kan skrive  $b = qn + r$ ; dermed er  $r$  også resten til  $b$ .  
Omvendt, anta at  $r$  er resten både når  $a$  deles på  $n$  og når  $b$  deles på  $n$ . Vi ser da at  $(a - r)|n$  og at  $(r - b)|n$ . Dermed er  $a \equiv r \pmod{n}$  og  $r \equiv b \pmod{n}$ . Det følger fra a) at  $a \equiv b \pmod{n}$ .