Løsningsforslag til Skriftlig Eksamen
DM527 Matematiske redskaber i datalogi

Tirsdag, den 22. januar 2008.

Opgave 1 (20 %)

a) Falsk. Lad $A = \{0, 1, 2, \ldots\}$, og $B = \{\ldots, -2, -1, 0\}$. Da vil $A \cap B = \{0\}$.

b) Falsk. Da $A \neq \emptyset$ findes der et element $a \in A$. Da $R = \emptyset$, vil $(a, a) \notin R$. R er derfor ikke refleksiv og dermed heller ikke en ækvivalensrelation.

c) Sandt. Da $A \subseteq B$ findes der en mængde C, så $B = A \cup C$ og $A \cap C = \emptyset$. Dermed fås $|B| = |A| + |C| \geq |A|$.

d) Falsk. Modeksempel $A = \{0\}$, $B = \{1\}$. Da vil $|A| \leq |B|$, men $A \not\subseteq B$.

Opgave 2 (25 %)

Dette vises per induktion.

Basis: $n = 0$. Vi har $1 + 0x = 1$ og $(1 + x)^0 = 1$. Dermed ok.

Induktionshypotese: Antag at for et $n \in \mathbb{N}_0$ da er $1 + nx \leq (1 + x)^n$.

Induktionsskridt: Vi viser, at sætningen er sand for $n + 1$ givet induktionshypotensen for $n \geq 0$. Dette gøres ved at starte på højresiden:

$(1 + x)^{n+1} = (1 + x)^n(1 + x) \overset{hyp}{\geq} (1 + nx)(1 + x) = 1 + nx + x + nx^2 = 1 + (n + 1)x + nx^2 \geq 1 + (n + 1)x$.

Opgave 3 (20 %)

a) Dette bevises i flere små dele

   (a) R er refleksiv, idet for et vilkårligt $a \in \mathbb{Z}$ vil $a + a \equiv 2a \equiv 0 \pmod 2$.

   (b) R er symmetrisk, idet for vilkårlige $a, b \in \mathbb{Z}$ har vi $a + b \equiv b + a \pmod 2$.

   (c) R er transitiv, idet med $a, b, c \in \mathbb{Z}$ fås ud fra aRb og bRc, dvs. $a + b \equiv 0 \pmod 2$ og $b + c \equiv 0 \pmod 2$, og sætning 3.4.5, at $a + b + b + c \equiv a + 2b + c \equiv a + c \equiv 0 \pmod 2$. Dermed aRc.

   Dermed fås at R er en ækvivalensrelation.

b) Falsk. R er ikke antisymmetrisk. Fx. har vi $0R2$ og $2R0$, men ikke $0 = 2$.

c) For et x med $xR3$, har vi $x + 3 \equiv 2$, dvs. $x \equiv 1 \pmod 2$ og dermed $[3]_R = \{2i + 1 | i \in \mathbb{Z}\}$.

Opgave 4 (15 %)

a) Antag at for i og j med $i, j \in \{0, 1, \ldots, n-1\}$ giver $ai + b$ og $aj + b$ samme rest ved division med n, dvs. $ai + b \equiv aj + b \pmod n$ og dermed $ai \equiv aj \pmod n$. Da a er relativt primisk med n, fås (jvf. sætning 3.7.2) at $i \equiv j \pmod n$ og dermed $i = j$.

b) f er injektiv: $f(x) = f(y)$, hviss $ax \equiv ay \pmod n$ da a og n er relativt primiske fås $x \equiv y \pmod n$. Idet $x, y \in \mathbb{Z}_n$ fås $x = y$ og f er dermed injektiv.

   Idet f er en injektiv funktion på en endelig mængde $\mathbb{Z}_n$, vil billedmængden $|f(\mathbb{Z}_n)|$ have samme størrelse som grundmængden $|\mathbb{Z}_n|$ og f er surjektiv og dermed bijektiv.