2011-(02)feb-03: dag 6

1) Ekvivalent: Finn x, k så att $16x - 42k = 26$

En linjär diofantisk ekvation.

Dividera med z (= sgd(16; 42)): $\mathbf{8}x - \boldsymbol{21}k = \underline{13}$

Euklides' algoritm:

$$
\begin{aligned}
21 &= 2\cdot 8 + 5 && (4)\\
8 &= 1\cdot 5 + 3 && (3)\\
5 &= 1\cdot 3 + 2 && (2)\\
3 &= 1\cdot 2 + \mathit{1} && (1)
\end{aligned}
$$

Så:

$$
\begin{aligned}
\mathit{1} &= 3 - 2 = && (1)\\
&= 3 - (5 - 3) = && (2)\\
&= -5 + 2\cdot 3 = &&\\
&= -5 + 2(\mathbf{8} - 5) = && (3)\\
&= 2\cdot\mathbf{8} - 3\cdot 5 = &&\\
&= 2\cdot\mathbf{8} - 3\cdot(\boldsymbol{21} - 2\cdot\mathbf{8}) = && (4)\\
&= 8\cdot\mathbf{8} - 3\cdot\boldsymbol{21} &&
\end{aligned}
$$

Så:

$$
\begin{aligned}
\underline{13} &= 13\cdot(8\cdot\mathbf{8} - 3\cdot\boldsymbol{21}) = \mathbf{8}\cdot(8\cdot 13) + \boldsymbol{21}\cdot(-3\cdot 13) =\\
&= \mathbf{8}\cdot 104 - \boldsymbol{21}\cdot 39
\end{aligned}
$$

Detta ger: $13 = 8x - 21k$

Skillnaden: $0 = 8(x - 104) - 21(k - 39)$

$8(x - 104) = 21(k - 39)$

$x - 104 = 21\cdot c$, något $c \in \mathbb{Z}$

Så alla lösningar:

$x = 104 + 21c = 20 + 21n$ $(21\cdot 4 = 84)$

Det vill säga:

<u>Två</u> lösningar: 20 och 41 i $\mathbb{Z}_{42}$

Ty: sgd(16; 42) = 2

2) $x \equiv 5 \pmod 8$ (1)

Innebär: $x/8 = k$, rest 5

Det första ger: $x = 5 + 8k$ $k \in \mathbb{Z}$

Den andra: $5 + 8k \equiv_{81} 73$

Det vill säga: $8k \equiv_{81} 68$

Som förra uppgiften, med Euklides' algoritm.

$81 = 10 \cdot 8 + 1$

$1 = 81 \cdot 1 + 8(-10)$

$68 = 8(-680) + 81 \cdot 68$

Så alla lösningaar: $k = -680 + 81 \cdot m$ $m \in \mathbb{Z}$

Det vill säga: $k = 49 + 81 \cdot n$ $n \in \mathbb{Z}$

Alla lösningar, x, till (1):

$$x = 5 + 8(49 + 81n) = 397 + 648n$$

Om man ska lösa flera problem med samma moduler

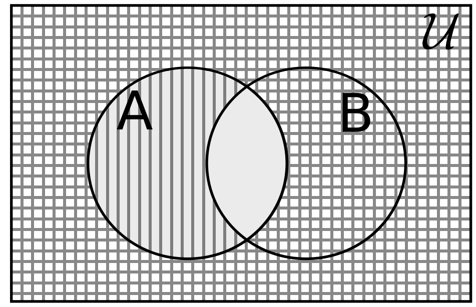
finna d_1, d_2 så att $d_1 \equiv 1 \pmod 8$ $\equiv 0 \pmod{81}$
$d_2 \equiv 1 \pmod 8$ $\equiv 0 \pmod{81}$

3) Att visa: $((A^C \cup B^C) \setminus A)^C = A$ för godtyckliga mängder, A och B.

Med Venn-diagram:

Horisontella sträck: $A^C \cup B^C$
Verticalla sträck: $(A^C \cup B^C) \setminus A$
Grått: $((A^C \cup B^C) \setminus A)^C$

Alltså är $((A^C \cup B^C) \setminus A)^C = A$ $\blacksquare$



Med boolesk algebra:

$$
\begin{aligned}
&((A^C \cup B^C) \setminus A)^C = \\
&= ((A^C \cup B^C) \cap A^C)^C = \\
&= (A^C \cup B^C)^C \cup A^{CC} = \\
&= (A^{CC} \cap B^{CC}) \cup A = \\
&= (A \cap B) \cup A = A \qquad \blacksquare
\end{aligned}
$$

Andra sätt att visa detta på:

$$
\begin{aligned}
&((A^C \cup B^C) \setminus A)^C \asymp \\
&\asymp \neg((\neg a \vee \neg b) \wedge \neg a) = \\
&= \neg(\neg(a \wedge b) \wedge \neg a) = \\
&= (a \wedge b) \vee a = a \qquad \blacksquare
\end{aligned}
$$

$$
\begin{aligned}
&((A^C \cup B^C) \setminus A)^C = \\
&= ((A^C \cup B^C) \cap A^C)^C = \\
&= ((A^C \cup B^C) \cap A^C)^C = \\
&= (A^C)^C = A \qquad \blacksquare
\end{aligned}
$$

$$
\begin{aligned}
&((A^C \cup B^C) \setminus A)^C = \\
&= ((A^C \cup B^C) \cap A^C)^C = \\
&= ((A \cap B)^C \cap A^C)^C = \\
&= ((A \cap B) \cup A) = A \qquad \blacksquare
\end{aligned}
$$

(Fler liknande sätt finns)

4) Vi visar för en kvardat med sidan 2^k

Induktion

Bas Påståendet sant då $k = 0$ inget
Kvar att täcka då en bit har tagits bort.

OK

Sats:

Antag sant för $k = p$ och betrakta kvadraten med sidan 2^{p+1}.

Dela upp den i fyra 2^p kvadrater tag bort en liten bit och en L-bit i mitten. Resten täcks av antagandet.

Så påståendet för $k = p \Rightarrow$ påståendet $k = p+1$

Induktionspricipen

5) Fibonacci, rekursivt $F_0 = 0,\quad F_1 = 1$
$F_{n+2} = F_n + F_{n+1}$

Visar med induktion

$F_1^2 + F_2^2 + \ldots + F_n^2 = F_n \cdot F_{n+1}$ $\quad n = 1, 2, 3, \ldots$

Bas: $VL = F_1^2 = 1$ $\quad HL = F_1F_2 = 1\cdot 1 = 1$

Steg: Antag sant för $n = k$

$$VL_{k+1} = F_1^2 + F_2^2 + \ldots + F_n^2 = F_n \cdot F_{n+1} = VL_k + F_{k+1}^2 = HL_k + F_{k+1}^2 =$$

$$= F_k F_{k+1} + F_{k+1}^2 = F_{k+1}\left(F_k + F_{k+1}\right) = F_{k+1} \cdot F_{k+2} = HL_{k+1}$$

Så steget klart. $\quad VL_k = HL_k \Leftrightarrow VL_{k+1} = HL_{k+1}$

b)

Visa att $\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$

Bas: $VL_1 = \begin{pmatrix} F_2 & F_1 \\ F_1 & F_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^1 = HL_1$

Antag sant för n = k

$VL_{k+1} = \begin{pmatrix} F_{k+2} & F_{k+1} \\ F_{k+1} & F_k \end{pmatrix}, \qquad HL_{k+1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{k+1}$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = VL_k \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} F_{k+1}+F_k & F_{k+1} \\ F_k+F_{k-1} & F_k \end{pmatrix} = \begin{pmatrix} F_{k+2} & F_{k+1} \\ F_{k+1} & F_k \end{pmatrix} = VL_{k+1}$$

6) Finn X, Y, Z, $f : X \to Y$, $g : Y \to Z$

Så att $g \circ f : X \to Z$ är bijektiv, men varken f, g bijektiv.

g måste vara en surjektion och
f måste vara en injektion.

Så f inte surjektion och g inte injektion.

Om X = Y = Z och f : injektion, inte surjektion, måste
X = Y var oändlig.

7) Givet $f : A \to A$, $f \circ f = id_A$ det vill säga $f(f(x)) = x \ \ \forall\, x \in A$

Visa att f är bijektiv.

f är injektiv ty $f(x_1) = f(x_2) \Rightarrow f(f(x_1)) = f(f(x_2)) \Rightarrow x_1 = x_2$

f är surjektiv ty $x = f(f(x)),\ \forall\, x \in A$

Alltså f är bijektiv.

8) 2^{29} i bas 10 har 9 olika siffror, vilken siffra har 2^{29} inte?

$(a_k\, a_{k-1} \ldots a_1\, a_0)_{10} \equiv_9 a_k + a_{k-1} + \ldots + a_0$

Ty $a_n \cdot 10^n = a_n\underbrace{(999\ldots9 + 1)}_{\times n} \equiv_9 a_n$

$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 \equiv_9 ?^{?}{}_{?}{}^{?}{}_{?}{}^{?}{}_{?}?$

$2^0 \equiv_9 1,\quad 2^1 \equiv_9 2,\quad 2^2 \equiv_9 4,\quad 2^3 \equiv_9 8,\quad 2^4 \equiv_9 7$
$2^5 \equiv_9 5,\quad 2^6 \equiv_9 1$

Så $2^{29} = 2^{6 \cdot 4 + 5} \equiv_9 1^4 \cdot 5 = 5$

$0 + 1 + 2 + \ldots + 9 = 45 \equiv_9 0$

2^{29}, siffersumma $\equiv_9 5$

Om siffran x fattas så gäller

$x + 5 \equiv_9 0$

Så det är 4 som fattas.