Lösningar Inledande diskret matematik 19/1 - 13

1) $\dfrac{\begin{array}{c} p \to (q \wedge r) \\ \neg q \end{array}}{\neg p}$

ett motexempel måste ha

$\neg p : F \quad p : S$

$\neg q : S \quad q : F$

då blir $p \to (q \wedge r)$ F

oberoende av r så motex. saknas

tautologi

$\dfrac{\begin{array}{c} p \to q \\ r \end{array}}{p \to (q \wedge r)}$

ett motex måste ha $r : S$

$p \to (q \wedge r)$ F vilket ger

$p : S$: $q : F$ och

$p \to q$ blir F

så motex. saknas

tautologi

$\dfrac{\begin{array}{c} p \wedge q \\ r \end{array}}{p \to (q \wedge r)}$

som ovan måste ett motex ha

$r : S \quad p : S \quad q : F$

vilket gör $p \wedge q : F$

motex saknas

tautologi

2) $2^{18} = 2^{4\cdot 4+2} = 16^4\cdot 4 \equiv 1\cdot 4 \mod 5$

$3^{18} = 3^{3\cdot 6} = 27^6 \equiv 2^6 = 16\cdot 4 \equiv 1\cdot 4$

<u>Svar:</u> $4+4=8\equiv \underline{\underline{3}}$

3) $34x+28y=8$

$17x+14y=4$

Euklides alg: $17 = 14+3$

$14 = 4\cdot 3+2$

$3 = 2+1$

Bezouts id: $1 = 3-2 = 3-(14-4\cdot 3) =$

$= 5\cdot 3 - 14 = 5(17-14)-14 = 5\cdot 17 - 6\cdot 14$

$4 = 4(5\cdot 17 - 6\cdot 14) = 20\cdot 17 - 24\cdot 14 =$

$= 20\cdot 17 - 24\cdot 14 + n\cdot 14\cdot 17 - n\cdot 14\cdot 17$

$= 17(20-14n) + 14(-24+17n)$

<u>Lösn:</u> $\begin{cases} x = 20-14n \\ y = -24+17n \end{cases}$

eller $\begin{cases} x = 6-14n \\ y = -7+17n \end{cases}$

4) $\begin{cases} x \equiv 3 \mod 17 \\ x \equiv 2 \mod 10 \end{cases}$

Euklides alg: $17 = 10 + 7$

$10 = 7 + 3$

$7 = 2 \cdot 3 + 1$

Bezouts id: $1 = 7 - 2\cdot 3 = 7 - 2(10-7) =$

$= 3\cdot 7 - 2\cdot 10 = 3(17-10) - 2\cdot 10 = 3\cdot 17 - 5\cdot 10$

$X = 3\cdot 2\cdot 17 - 5\cdot 3\cdot 10 + n\cdot 17\cdot 10 =$

$= -48 + n\cdot 170 = \underline{\underline{122 + m\cdot 170}}$

5) R är reflexiv ty

$f(0) = f(0)$ och $g(0) = g(0)$

R är symmetrisk ty

$f(0) = g(0)$ och $f(1) = g(1) \Rightarrow g(0) = f(0)$ och $g(1) = f(1)$

R är transitiv ty

$f(0) = g(0)$ och $f(1) = g(1)$ och $g(0) = h(0)$ och

$g(1) = h(1) \Rightarrow f(0) = h(0)$ och $f(1) = f(1)$

$[f]$ bestäms av f:s värden i 0 och 1

och som representant kan man välja

den linjär funktion som har rätt värden (entydigt bestämd). Detta blir en bijektion: alla linjära funktioner kommer med och en och endast en linjär funktion i varje klass.

$$\Phi[f] = (f(1) - f(0))X + f(0)$$

6) En udda summa kan bara fås om en kula är udda och en jämn.
En av 5 udda, en av 5 jämna

Svar: $5 \cdot 5 = 25$

7) Injektiva $\mathbb{Z}_3 \to \mathbb{Z}_4$

~~f Z [0] kan~~ $f[0]$ kan ha 4 värden
$f[1]$ — " — 3 — " —
$f[2]$ — " — 2 — " —

Svar: $4 \cdot 3 \cdot 2 = 24$

Surjektiva $\mathbb{Z}_4 \to \mathbb{Z}_3$

2 element måste ha samma bild, de övriga olika. De två elementen kan väljas på $\binom{4}{2}$ sätt och bilderna kan väljas på $3!$ sätt

Svar: $\binom{4}{2} \cdot 3! = \frac{4!}{2! \cdot 2!} 3! = 3 \cdot 4 \cdot 3 = \underline{\underline{36}}$

8) mod 8 är

$[0]^2 = [0]$

$[1]^2 = [1]$

$[2]^2 = [4]$

$[3]^2 = [9] = [1]$

$[4]^2 = [16] = [0]$

$[5]^2 = [25] = [1]$

$[6]^2 = [36] = [4]$

$[7]^2 = [49] = [1]$

så de enda kvadraterna är

$[0]$, $[1]$ och $[4]$

$[8k-1] = [-1] = [7]$ kan inte fås

som summan av 3 kvadrater. Det närmaste man kan komma är $[4]+[1]+[1] = [6]$

eller $[4]+[4]+[0] = [8]$