(Detaljerad) LÖSNING TMV200 TENTA 2011-12-15

1. $4x+10y=16 \iff 2x+5y=8$.

$x_0=-1,\ y_0=2$ en speciell lösn.

Den allmänna lösningen är $x=-1+5n,\ y=2-2n$.

2. Beräkna mod 35. $35=5\cdot 7$. $\Phi(35)=4\cdot 6=24$.

Mod 35: $11^{49}\equiv(11^{24})^2\cdot 11\equiv 1^2\, 11\equiv 11$, ty sgd(11, 35)=1

och $11^{24}\equiv 1$ enligt Eulers Sats.

$7^2\equiv 7\cdot 7\equiv(5+2)\cdot 7\equiv 14$. $7^3\equiv 14\cdot 7\equiv(15-1)\cdot 7\equiv -7$.

$7^4\equiv -7\cdot 7\equiv -14$. $7^5\equiv -14\cdot 7\equiv(-15+1)7\equiv 7$.

$7^{24}\equiv(7^5)^4\cdot 7^4\equiv 7^4\, 7^4\equiv 7^5\, 7^3\equiv 7\, 7^3\equiv 7^4\equiv -14$.

$11^{49}-7^{24}\equiv 11-(-14)=11+14=25$.

SVAR 25.

3. $\boxed{n=1}$ $V.L.=\dfrac{2}{1\cdot 3}=\dfrac{2}{3}$. $H.L=1-\dfrac{1}{3}=\dfrac{2}{3}$.

$V.L=H.L.$

Antag den gäller för n. Vi visar för $n+1$.

$$VL=\sum_{k=1}^{n}\frac{2}{(2k-1)(2k+1)}+\frac{2}{(2n+1)(2n+3)}$$

$$=1-\frac{1}{2n+1}+\frac{2}{(2n+1)(2n+3)}$$ (enligt ind. antagandet)

$$=1-\left(\frac{1}{2n+1}-\frac{2}{(2n+1)(2n+3)}\right)=1-\frac{2n+3-2}{(2n+1)(2n+3)}=1-\frac{2n+1}{(2n+1)(2n+3)}$$

$$= 1 - \frac{1}{2n+3}.$$

$$\text{H.L.} = 1 - \frac{1}{2(n+1)+1} = 1 - \frac{1}{2n+3}.$$

V.L. = H.L. Identiteten är bevisad.

4. [a] F. Ex $x = 3,\ y = 1,\ z = 9$.

[b] S. $\text{sgd}(x, yz) = 1 \Rightarrow 1 = xu + yzv$ för något u, v. $\Rightarrow$ Varje delare av x och y delar 1

$\Rightarrow \text{sgd}(x, y) = 1$. Likadant för x och z.

[c] S. $\Phi(pq) = \Phi(p)\Phi(q) = (p-1)(q-1) = pq - p - q + 1$

$\Rightarrow x^{pq-p-q+1} \equiv 1$ enligt Eulers sats, mod pq.

$\Rightarrow x^{pq-p-q+1} \cdot x \equiv 1 \cdot x$, dvs $x^{pq-p-q+2} \equiv x$, mod pq.

5 [a] Välj 5 st. för gruppen A: $\binom{10}{5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5!} = 2^2 \cdot 9 \cdot 7$

för gruppen B: $\binom{10-5}{3} = \binom{5}{3} = \frac{5 \cdot 4 \cdot 3}{3 \cdot 2 \cdot 1} = 10$

för gruppen C: $\binom{2}{2} = 1$

Svar $\binom{10}{5} \cdot \binom{5}{3} \binom{2}{2} = 2^3 \cdot 9 \cdot 7 \cdot 5 = 2520$

[b]: $$\binom{n_1 + n_2 + \cdots + n_k}{n_1} \binom{n_2 + \cdots + n_k}{n_2} \cdots \binom{n_{k-1} + n_k}{n_{k-1}} \binom{n_k}{n_k}.$$

$$= \frac{(n_1 + n_2 + \cdots + n_k)!}{n_1!\, n_2! \cdots n_k!}$$

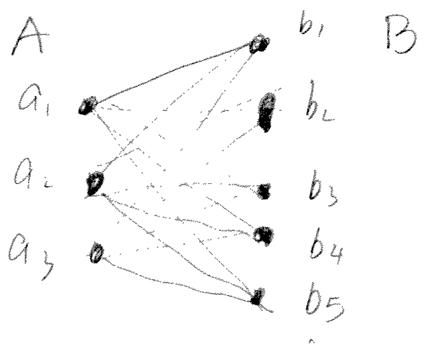
6. (1) Varje injektiv funktion $f: A=\{0, 1\} \to B=\{1, 2, \dots, n\}$ bestäms av ett ordnat par $(f(0), f(1))$, $f(0) \neq f(1)$.

Antalet är $n(n-1)$.

(2) Varje surjektiv funktion från B till A bestäms av delmängden $f^{-1}(\{0\})$ av B, som är icke-tom och skall vara äkta delmängd, ty f är surjektiv. Antalet är $2^n - 2$, ty antalet delmängder är 2^n och det icke-tomma äkta delmängder är $2^n - 2$.

(3) Varje ekvivalens klass på B med två ekvivalensklasser motsvarar en partition av B i två icke ordnat par av äkta delmängder. Enligt (2) är antalet $\frac{1}{2}(2^n-2) = 2^{n-1} - 1$.

7



Enkla vägar som ej gå genom a_2 bestäms en nod i B:

5 st

Enkla vägar som gå genom a_2 bestäms av 2 ordnade noder i B.

$5 \cdot 4 = 20$ st

Svar 25.

8 Bevis Antag n är primt tal. Då är varje element $x \in \mathbb{Z}_n$, $x \neq 0$ inverterbar, dvs det finns $y \in \mathbb{Z}_n$, $y \neq 0$, $xy = 1$.

Symmetry: $aRb \Rightarrow ax = b$, $x \neq 0$,

$\Rightarrow axy = by$, $a = by$. eller $by = a$.

$\Rightarrow bRa$ ty $y \neq 0$

Reflexivitet. aRa ty $a \cdot 1 = a$

Transitivitet: aRb, $bRc \Rightarrow ax = b$. $by = c$

$\Rightarrow axy = by = c$, men $xy \neq 0$ (ty

x och y är relativt prima med n, mod n $\Rightarrow xy$

relativt primt med n, mod n)

dvs R är en ekvivalensrelation.

Antag n är ej primt, dvs $n = n_1 n_2$ där $1 < n_1 < n$, $1 < n_2 < n$. Då är $[n_2] \neq 0$, och $0 = [n] = [n_1][n_2]$.

dvs $[n_1] R 0$, men $0 \not R [n_1]$, ty $[n_1] \neq 0$. $\Rightarrow$

R ej symmetrisk därmed ej ekvivalensrelation.