Stockholms Universitet
Institutionen för Data och Systemvetenskap
Johan Andersson

Diskret Matematik
Vårterminen 2012
2012-03-13

Lösningsförslag - inlämningsuppgifter - Omgång 3

1. Definiera a_n rekursivt genom $a_0 = 2$ samt $a_n = 3a_{n-1} - 2$ för $n \geq 1$. Bevisa att $a_n = 3^n + 1$ för alla naturliga tal n.

   Svar: Vi använder oss av induktionsbevis.

   (a) Basfallet: $n = 0$, $3^0 + 1 = 1 + 1 = 2 = a_0$. OK!

   (b) Induktionsantagandet: $a_n = 3^n + 1$.

   (c) $a_{n+1} = 3a_n - 2 \stackrel{\text{IA}}{=} 3(3^n + 1) - 2 = 3 \cdot 3^n + 3 \cdot 1 - 2 = 3^{n+1} + 1$. OK!

   (d) Enligt induktionsprincipen så gäller det att $a_n = 3^n + 1$ för alla $n \geq 0$.

2. Från divisionsalgoritmen för division med 2 så följer det att $n = 2q + r$ för något heltal q och $r = 0$ eller $r = 1$. En algoritm för att beräkna $b \cdot a^n \pmod m$ bygger på att använda kongruenserna

   $$b \cdot a^n \equiv d \cdot c^q \pmod m$$

   där $c \equiv a^2 \pmod m$, $d \equiv ba^r \pmod m$ och $0 \leq c, d < m$ rekursivt samt att använda faktumen att $a^1 = a$, samt $a^0 = 1$.

   (a) Beräkna $7^{37} \pmod{13}$ genom att använda algoritmen ovan (Redovisa varje steg noggrant).

      i. Steg 1. Vi har $b = 1$, $a = 7$, $n = 37$. Vi får att $37 = 2 \cdot 18 + 1$, dvs $q = 18$ och $r = 1$. Detta ger att $d \equiv ba^1 \equiv 1 \cdot 7 \equiv 7 \pmod{13}$, dvs $d = 7$, samt att $c \equiv a^2 = 7^2 = 49 = 3 \cdot 13 + 10 \equiv 10 \pmod{13}$, dvs $c = 10$, dvs $7^{37} \equiv 7 \cdot 10^{18} \pmod{13}$.

      ii. Steg 2. Vi har nu att $b = 7$, $a = 10$, $n = 18$. Vi får att $18 = 2 \cdot 9 + 0$, dvs $q = 9$ och $r = 0$. Detta ger att $d \equiv b = 7 \pmod{13}$, dvs $d = 7$, samt att $c \equiv 10^2 = 100 = 9 + 7 \cdot 13 \equiv 9 \pmod{13}$, dvs $c = 9$, dvs $7^{37} \equiv 7 \cdot 9^9 \pmod{13}$.

      iii. Steg 3. Vi har nu att $b = 7$, $a = 9$, $n = 9$. Vi får att $18 = 2 \cdot 4 + 1$, dvs $q = 4$ och $r = 1$. Detta ger att $d \equiv b \cdot a = 63 \equiv 11 \pmod{13}$, dvs $d = 11$, samt att $c \equiv 9^2 = 81 = 3 + 6 \cdot 13 \equiv 3 \pmod{13}$, dvs $c = 3$, dvs $7^{37} \equiv 11 \cdot 3^4 \pmod{13}$.

      iv. Steg 4. Vi har nu att $b = 11$, $a = 3$, $n = 4$. Vi får att $4 = 2 \cdot 2 + 0$, dvs $q = 2$ och $r = 0$. Detta ger att $d \equiv b \equiv 11 \pmod{13}$, dvs $d = 11$, samt att $c \equiv 3^2 \equiv 9 \pmod{13}$, dvs $c = 9$, dvs $7^{37} \equiv 11 \cdot 9^2 \pmod{13}$.

v. Steg 5. Vi har nu att $b = 11$, $a = 9$, $n = 2$. Vi får att $2 = 2 \cdot 1 + 0$, dvs $q = 2$ och $r = 0$. Detta ger att $d \equiv b \equiv 11 \pmod{13}$, dvs $d = 11$, samt att $c \equiv 9^2 \equiv 81 = 3 + 6 \cdot 13 \equiv 3 \pmod{13}$, dvs $c = 3$, dvs $7^{37} \equiv 3 \cdot 11 \equiv 33 = 2 \cdot 13 + 7 \equiv 7 \pmod{13}$.

Vi får alltså att $7^{37} \equiv 7 \pmod{13}$.

Anmärkning: I just detta fall kan slutsatsen lättare inses från Fermats lilla sats $7^{12} \equiv 1 \pmod{13}$ och alltså $7^{37} \equiv 7^{3 \cdot 12 + 1} = (7^{12})^3 \cdot 7 \equiv 1^3 \cdot 7 \equiv 7 \pmod{13}$, men nu var det ju algoritmen ovan som skulle användas. Algoritmen ovan är användbar exempelvis i tillämpningar av RSA-algoritmen där betydligt större tal förekommer.

(b) Vad är tidskomplexiteten av algoritmen ovan om n är ett k-bitars tal (k binära siffror)? (a, b och m är fixa tal, men n kan variera.)

Svar: I varje steg så halveras talet n, så tidskomplexiteten är $O(\log n)$ (eller $O(k)$).

3. Låt R vara en relation definierad på mängden $\{1, 2, 3, 5, 6, 9, 15, 30\}$ så att aRb om $a|b$.

(a) Visa att R är en partiell ordning

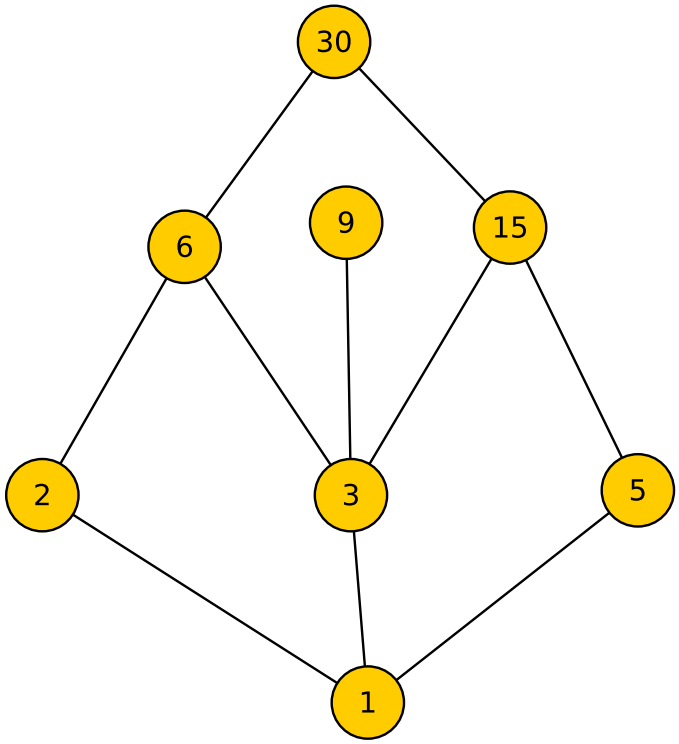
Svar: Vi behöver visa

i. Reflexivitet: Sant eftersom $a = 1 \cdot a$ och alltså $a|a$ och aRa.

ii. Antisymmetri: Antag att aRb och bRa. Då gäller att $a|b$ och $b|a$ och från definitionen på delare att det finns heltal d_1, d_2 så att $b = ad_2$ och $a = bd_1$. Insättning av första ekvationen i andra ekvationen ger $a = ad_1d_2$, dvs $d_1d_2 = 1$. Då mängden består av positiva heltal måste $d_1 = d_2 = 1$ och $a = b$.

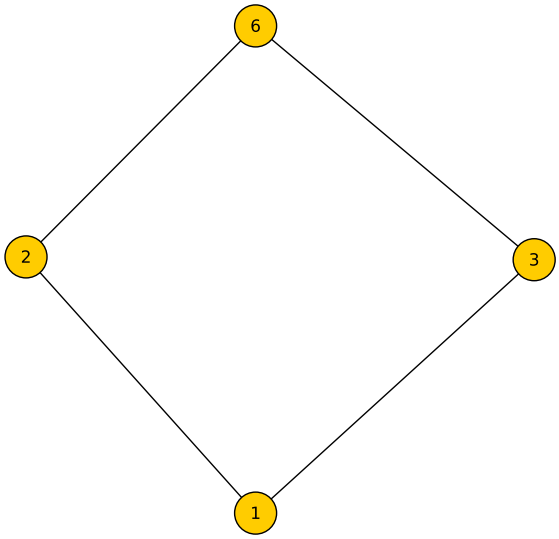
iii. Transitivitet: Om aRb och bRc så har vi att $a|b$ och $b|c$ och enligt definitionen av delare gäller $b = ad_1$ och $c = bd_2$. Vi får att $c = ad_2d_1 = ad$ där $d = d_1d_2$ är ett heltal. Alltså har vi att $a|c$ och att aRc och relationen är transitiv. (Alternativt kan Teorem 2.12 (1) användas istället för definitionen av delare)

(b) Rita ett Hasse-diagram för den partiella ordningen
Svar:



4. Låt $D_6 = \{1, 2, 3, 6\}$ och låt R vara definierad som aRb omm $a|b$.

(a) Rita upp Hasse-diagrammet för den partiella ordningen
Svar:

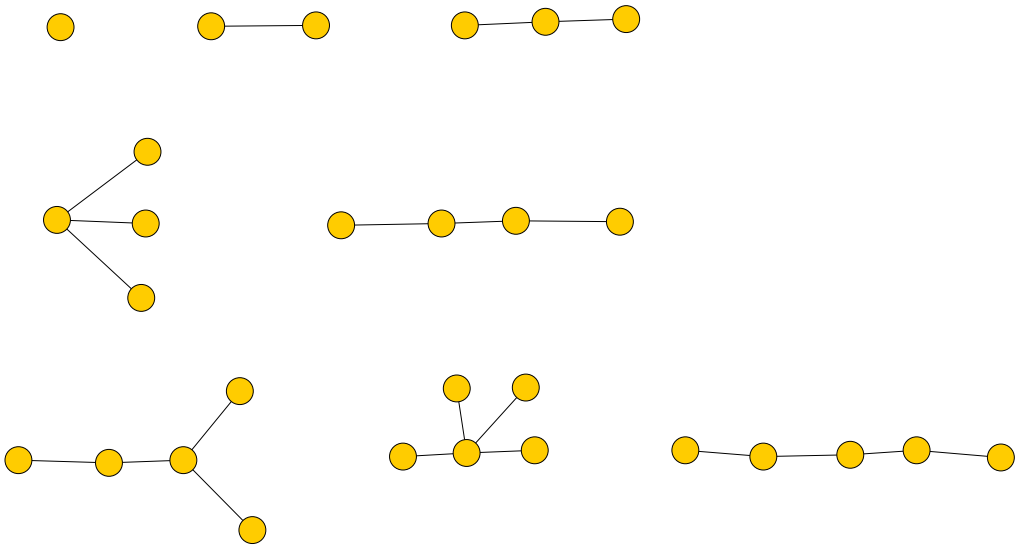


(b) Bevisa att D_6 är en Boolesk algebra där de Booleska operationerna $*, +$ definieras som $a*b = SGD(a,b)$, $a+b = MGM(a,b)$, komplementet av a definieras som $a' = 6/a$ samt 0-an samt 1-an i den Booleska algebran ges av elementen 1 och 6 i D_6. Ett sätt är att verifiera axiomen för en Boolesk algebra. Ett annat sätt är att hitta en isomorfi till en känd Boolesk algebra med 4 element (Exempelvis så kan ni använda B_2 som definieras i Exempel 7.2 i kursboken). En isomorfi mellan två Booleska algebror $(B, +_B, *_B, {}'^B, 0_B, 1_B)$ och $(A, +_A, *_A, {}'^A, 0_A, 1_A)$,är en en-entydig korrespondens mellan elementen i de Booelska algebrorna som skickar ettor på ettor, nollor på nollor, och respekterar addition, multiplikation och komplement. Detta innebär mer exakt att om $\phi : A \to B$ är en funktion som ger den en-entydiga korrespondensen, så skall $\phi(1_A) = 1_B$, $\phi(0_A) = 0_B$, $\phi(a +_A b) = \phi(a) +_B \phi(b)$, $\phi(a *_A b) = \phi(a) *_B \phi(b)$, samt $\phi(a'^A) = \phi(a)'^B$.

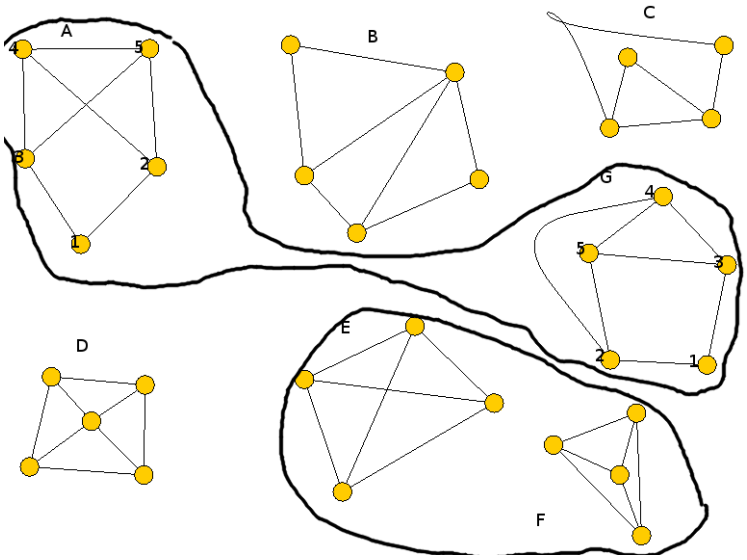
Svar: Vi använder ledningen och försöker hitta en isomorfi mellan den Booleska algebran och en känd Boolesk algebra med 4 element. Vi kan till exempel välja den booelska algebran B_2 definierad av Exempel 7.2 i kursboken. För att hitta isomorfin så kan vi ta hjälp av Hasse-diagrammet. Om Hassediagrammet till den partiella ordningen är ismorf (som riktad graf) med Hassediagrammet till den Booleska algebran så kommer isomorfin fås ifrån motsvarande grafisomorfi. Mer specifikt så följer det att om $n \in D_6$ och $n = 2^i 3^j$ (där $i, j \in \{0, 1\}$ och $\phi : D_6 \to B_2$ så ger $\phi(n) = ij$ den sökta isomorfin. Det är klart att $SGD(2^i 3^j, 2^k 3^l) = 2^{\min(i,k)} 3^{\min(j,l)}$ samt $MGM(2^i 3^j, 2^k 3^l) = 2^{\max(i,k)} 3^{\max(j,l)}$. Eftersom $ij * kl = ab$ i B_2 där $a = \min(i,k)$ samt $b = \min(j,l)$, samt $ij + kl = ab$ i B_2 där $a = \max(i,k)$ samt $b = \max(j,l)$ så följer det att för $a, b \in D_6$ att $\phi(SGD(a,b)) = \phi(a) * \phi(b)$ samt $\phi(MGM(a,b)) = \phi(a) + \phi(b)$. Då dessutom $\frac{6}{2^i 3^j} = 2^{1-i} 3^{1-j}$ för $i, j \in \{0, 1\}$ och $ij' = ab$ där $a = 1 - i$ samt $b = 1 - j$ i B_2, samt att $\phi(6) = 11$ och $\phi(1) = 00$ så följer det att ϕ är en isomorfi mellan Booleska algebror. Alltså är även D_6 en Boolesk algebra.

5. Rita upp representanter för alla isomorfiklasser av träd med 1,2,3,4 samt 5 noder.

   Svar:



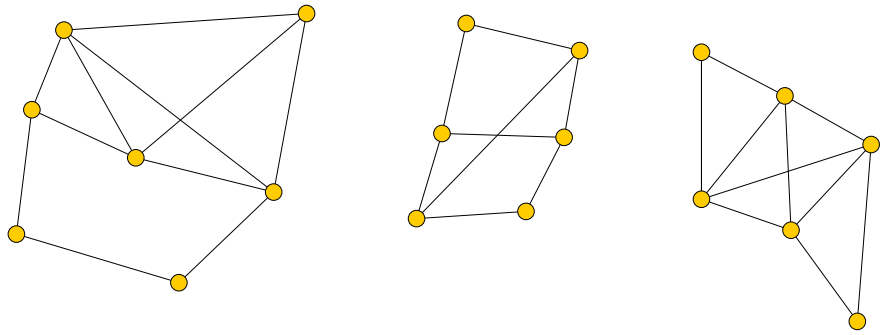
6. Vilka av följande grafer är isomorfa (indela graferna i isomorfiklasser (ekvivalensklasser under ekvivalensrelationen isomorfi))?



   Svar: Vi har indikerat ovan vilka grafer som är isomorfa med varandra. Graf C är den enda grafen med 4 noder och 5 bågar och alltså i sin egen isomorfiklass. Graf D är den enda grafen med 8 bågar och 5 noder och alltså i sin egen isomorfiklass, Graferna A,B,G har vardera 5 noder och sju bågar så skulle alltså kunna vara isomorfa. Dock så ser vi att graf B har en nod med hörngradtal 4 vilket varken graf A eller G har. Alltså är den i sin

egen isomorfiklass. Graf A och G har vardera hörngradtalen $(2, 3, 3, 3, 3)$, så skulle alltså kunna vara isomorfa. Siffrorna för noderna anger en entydig korrespondens mellan noderna i de två graferna och efter en koll av de mellanliggande bågarna ser vi att den ger en explicit isomorfi och de är således isomorfa. Graf E och F innehåller båda 4 noder och har bågar mellan alla olika noder. De är alltså båda isomorfa med den fullständiga grafen K_4 och således isomorfa.

7. Avgör vilka av följande grafer som innehåller Eulerspår respektive Eulerkretsar.



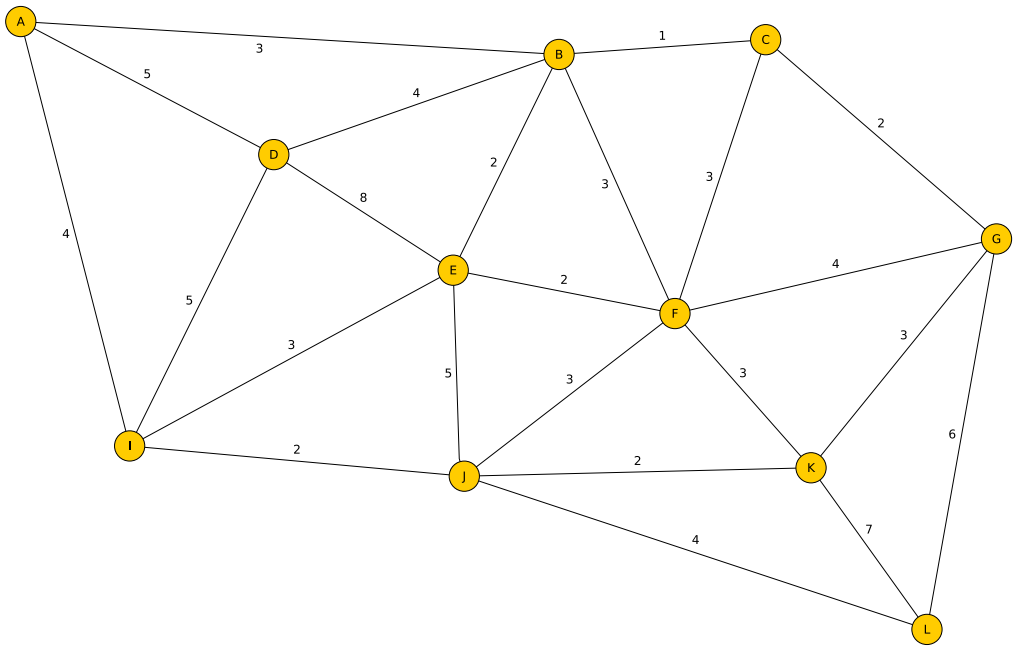
Svar:

(a) Den första grafen har 2 noder med udda gradtal. Enligt sats gäller då att den inte innehåller en Eulerkrets, men att den innehåller ett icke-slutet Eulerspår (som börjar och slutar i noderna med udda gradtal).

(b) Den andra grafen har 4 noder med udda gradtal. Enligt sats gäller då att den varken innehåller Eulerkrets eller Eulerspår

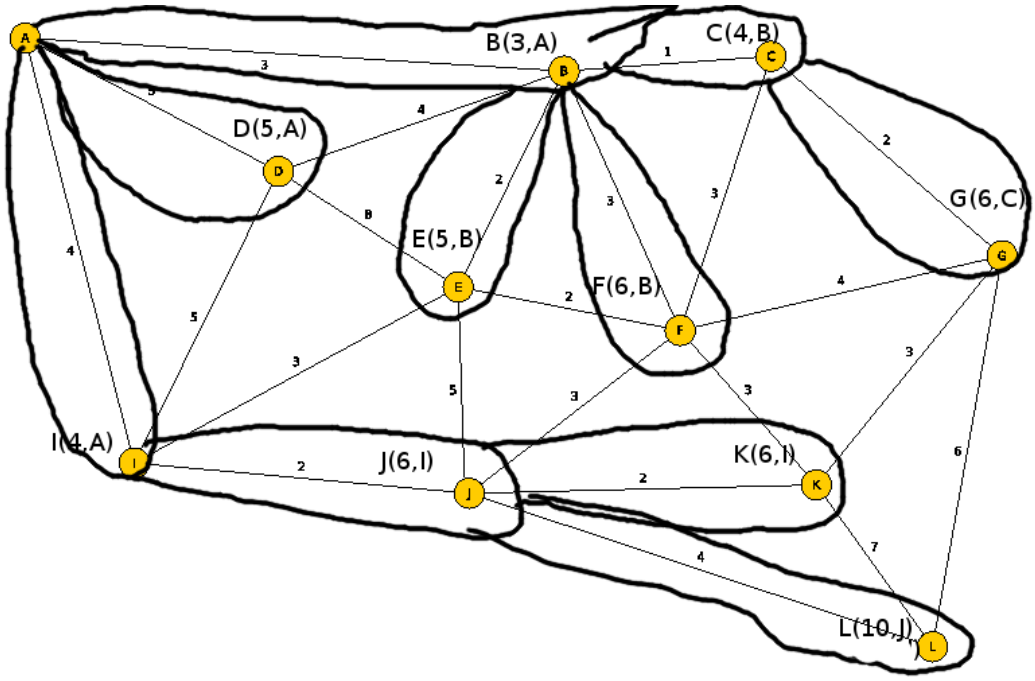
(c) I den tredje grafen har alla noder ett jämnt gradtal och enligt sats gäller då att den innehåller en Eulerkrets. Eftersom en Eulerkrets är ett slutet Eulerspår så innehåller den därmed även ett Eulerspår.

8. Den viktade grafen G ges av följande figur



(a) Använd Dijkstra's algoritm för att bestämma kortaste avståndet mellan hörn A och hörn L. Var noggrann och skriv en etikett vid kanterna så att stegen i algoritmen kan följas.

Svar. Följande graf visar uträkningarna. Avståndet blir 10.

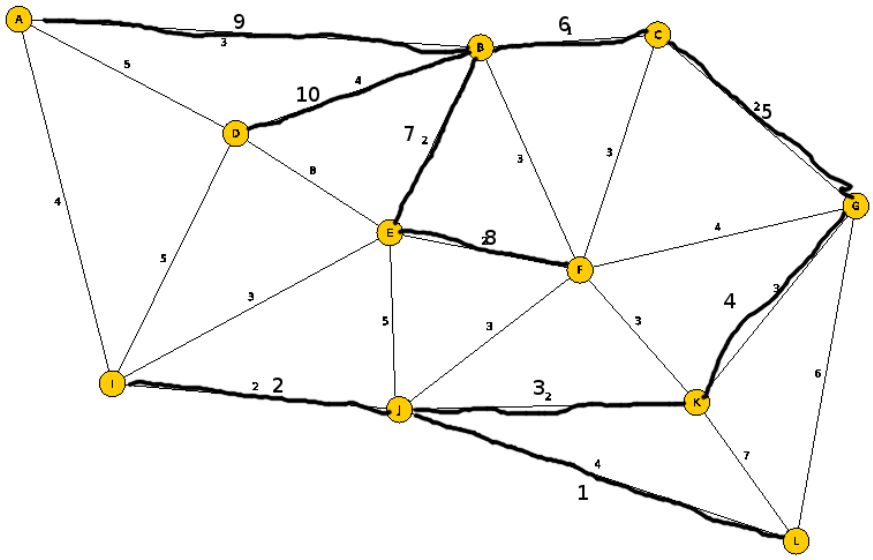


(b) Avgör hur långt avståndet är mellan A och J

Svar. Från grafen ovan kan det utläsas att avståndet blir 6.

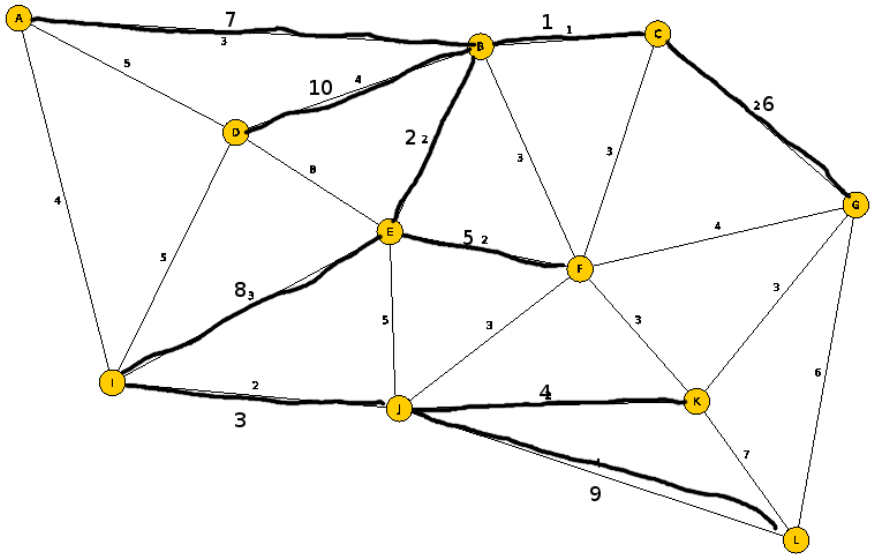
(c) Använd Prims algoritm för att hitta ett minimalt uppspännande träd. Ange vilken ordning du valt kanterna.

Svar. Vi kan börja i vilken nod som helst. Vi väljer nod L. Trädet ser ut som nedan. Siffrorna anger i vilken ordning vi valt kanterna.

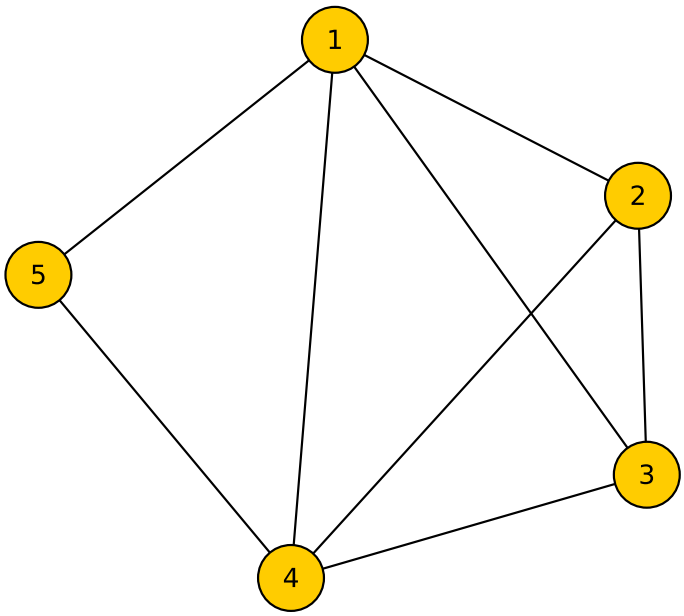


(d) Använd Kruskals algoritm för att hitta ett minimalt uppspännande träd. Ange vilken ordning du valt kanterna.

Svar. Trädet ser ut som nedan. Siffrorna anger i vilken ordning vi valt kanterna.



9. Grafen G ges av följande figur.



(a) Bestäm Förbindelsematrisen A till grafen.
Svar. Vi sätter ettor på plats (i, j) om det finns en båge mellan nod i och nod j. Vi får förbindelsematrisen

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

(b) Det är möjligt att visa att

$$A^3 = \begin{bmatrix} 8 & 9 & 9 & 9 & 7 \\ 9 & 6 & 7 & 9 & 4 \\ 9 & 7 & 6 & 9 & 4 \\ 9 & 9 & 9 & 8 & 7 \\ 7 & 4 & 4 & 7 & 2 \end{bmatrix}$$

.

i. Siffran 2 förekommer på ett ställe i matrisen. Hur kan siffran 2 tolkas i termer av promenader i grafen G. Vilka promenader motsvarar den siffran?
Svar. Siffran motsvarar antalet promenader av längd 3 från nod 5 till nod 5. I detta fall är promenaderna $5 \to 1 \to 4 \to 5$ och samma promenad baklänges, dvs $5 \to 4 \to 1 \to 5$.

ii. Siffran 4 förekomer på 4 ställen i matrisen. Tolka varje fyra i termer av promenader i grafen G. Vilka promenader motsvarar fyran?
Svar. Siffran 4 förekommer på platserna $(2,5)$, $(5,2)$ samt $(3,5)$ och $(3,5)$. Siffran motsvarar antalet promenader av längd 3 mellan respektive noder. Mer specifkt så motsvarar siffran på plats

A. $(2,5)$ promenaderna $2 \to 3 \to 1 \to 5$, $2 \to 4 \to 1 \to 5$, $2 \to 3 \to 4 \to 5$, $2 \to 1 \to 4 \to 5$.

B. $(5,2)$ Promenaderna i A baklänges.

C. $(3,5)$ promenaderna $3 \to 2 \to 1 \to 5$, $3 \to 4 \to 1 \to 5$, $3 \to 2 \to 4 \to 5$, $3 \to 1 \to 4 \to 5$.

D. $(5,3)$ Promenaderna i C baklänges.

(c) Utan att faktiskt beräkna matrisen A^4 (eller använda matrisen som vi beräknat ovan för A^3), använd teorin för promenader i grafer för att ange vilken siffra som skall stå i matrisen A^4 på den platsen i matrisen som finns i både femte raden och femte kolonnen.

Svar. Enligt teorin för promenader i grafer och Förbindelsematriser så skall talet på plats $(5,5)$ räkna antalet promenader i grafen mellan nod 5 och sig själv av längd fyra. Vi hittar följande promenader

i. Typ 1. Fram-Tillbaka-Fram-Tillbaka: $5 \to 1 \to 5 \to 1 \to 5$, $5 \to 4 \to 5 \to 4 \to 5$, $5 \to 1 \to 5 \to 4 \to 5$, $5 \to 4 \to 5 \to 1 \to 5$. 4 st promenader

ii. Typ 2. Fram-Fram-Tillbaka-Tillbaka: $5 \to 1 \to 4 \to 1 \to 5$, $5 \to 1 \to 2 \to 1 \to 5$, $5 \to 1 \to 3 \to 1 \to 5$, $5 \to 4 \to 1 \to 4 \to 5$, $5 \to 4 \to 2 \to 4 \to 5$, $5 \to 4 \to 3 \to 4 \to 5$, 6 st promenadr

iii. Cykler: $5 \to 1 \to 3 \to 4 \to 5$, $5 \to 1 \to 2 \to 4 \to 5$,: $5 \to 4 \to 3 \to 1 \to 5$, $5 \to 4 \to 2 \to 1 \to 5$, 4 st promenader

Sammanlagt så har vi $4+6+4 = 14$ st promenader av längd 4 mellan nod 5 och nod 5. Siffan som skall stå på plats $(5,5)$ i matrisen A^4 är alltså 14.