LINKÖPINGS UNIVERSITET
Matematiska institutionen
Milagros Izquierdo

Tentamen i Diskret Matematik, TATA52, TEN1, 2015–06–04, kl 14–19.

Inga hjälpmedel. Ej räknedosa. Fullständiga motiveringar krävs.

För betyg N behövs 3N-1 poäng.

---

1. Visa att $4 + 5 + 7 + 9 + \ldots + 2n + 3 = (n + 2)^2$ för alla heltal $n \geq 1$.

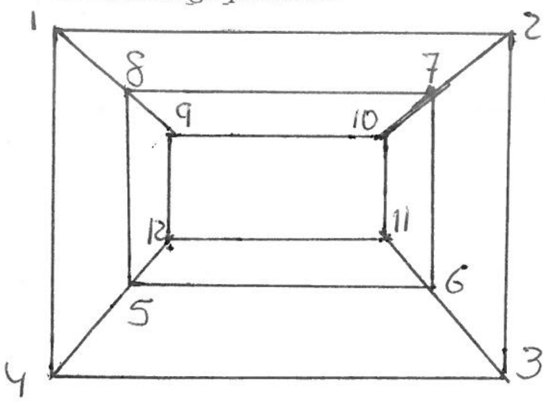
2. (a) Är graferna G_1 och G_2 nedan isomorfa?
   (b) Är grafen G_3 nedan eulersk ? hamiltonsk?

3. Lös den rekursiva ekvationen $a_{n+4} - 5a_{n+2} + 4a_n = n + 1$, $a_0 = 0$, $a_1 = 1$, $a_2 = 3$, $a_3 = 6$.

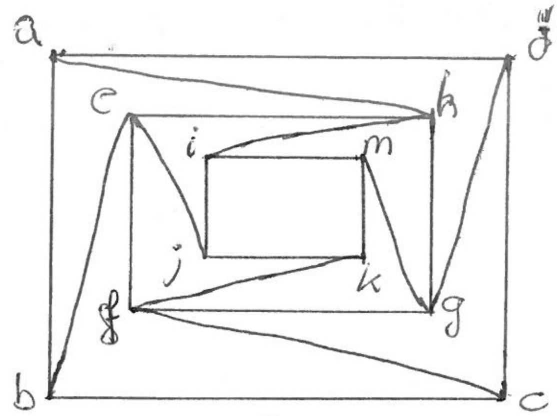
4. (a) I en kortege under student-festivalen deltar 25 vagnar och 18 lösa ekipage. På hur många sätt kan kortegen gå ut om de 2 första vagnarna hör till Aab-studenter, resp. Aba-studenter, de 2 sista vagnarna hör till Öst-studenter, resp. Öts-studenter, de 3 mellersta platser i kortegen tas av vagnar och vagnar och lösa alternerar (dvs kommer varannan) på de resterande platser?
   (b) Till en konferens i robotik kommer 100 androider som övernattar på 8 olika hotell. På hur många sätt kan konferensdeltagarna dela ut sig för att övernatta?

5. RS-klubben använder ett RSA-kryptosystem till passerkort som medlemmar får. I datorn som sköter dörrarna har man matat in den offentliga nyckeln $(5063, 1001)$. Vilken nyckel är programmerad i medlemmarnas kort? Hur mycket tid (i min) tog dig att räkna fram den privata nyckeln?

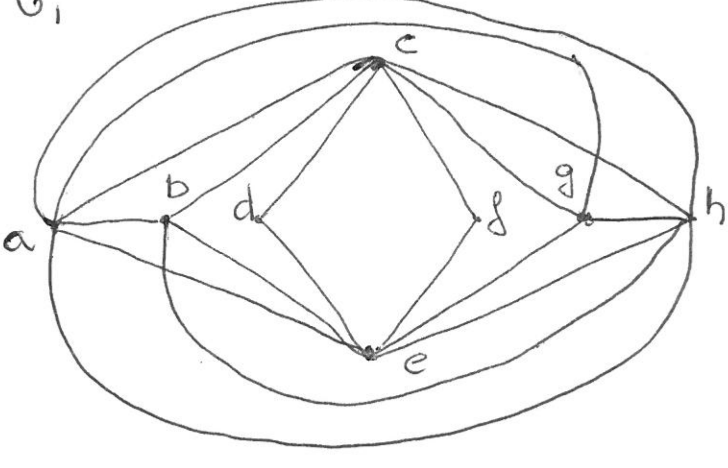
6. Hur många permutationer av $1, 2, \ldots, 10$ finns det sådana att inget udda tal hamnar på sin naturliga position?



G_1



G_2



G_3

4) $a_{n+4} - 5a_{n+2} + 4a_n = n+1$; $a_0=0$, $a_1=1$, $a_2=3$; $a_3=6$

karakt. ekv $\quad x^4 - 5x^2 + 4 = 0 \quad \to (x^2-1)(x^2-4)=0$

$$a_n^h = A_1 + A_2(-1)^n + A_3(2)^n + A_4(-2)^n$$

$a_n^p = (B_1 + B_2 n)n$, där

$(n+4)B_1 + B_2(n+4)^2 - 5B_1(n+2) - 5B_2(n+2)^2 + 4B_1 n + 4B_2 n^2 = n+1$

$n^2(B_2 - 5B_2 + 4B_2) + n(B_1 - 5B_1 + 4B_1 + 8B_2 - 20B_2) + (-6B_1 - 4B_2) = n+1$

$\Rightarrow 0=0$, $-12B_2 = 1$; $6B_1 + 4B_2 = -1$; $B_2 = -1/12$, $B_1 = -1/9$

$$a_n = -\frac{n}{9} - \frac{n^2}{12} + A_1 + A_2(-1)^n + A_3(2)^n + A_4(-2)^n$$

$$\begin{cases} a_0 = 0 = A_1 + A_2 + A_3 + A_4 \\ a_1 = 1 = -\frac{1}{9} - \frac{1}{12} + A_1 - A_2 + 2A_3 - 2A_4 \\ a_2 = 3 = -\frac{2}{9} - \frac{1}{3} + A_1 + A_2 + 4A_3 + 4A_4 \\ a_3 = 6 = -\frac{1}{3} - \frac{3}{4} + A_1 - A_2 + 8A_3 - 8A_4 \end{cases} \Rightarrow \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 1 & -1 & 2 & -2 & \frac{43}{36} \\ 1 & 1 & 4 & 4 & \frac{32}{9} \\ 1 & -1 & 8 & -8 & \frac{85}{12} \end{array}\right)$$

$A_1 = -\frac{211}{216}$, $A_2 = -\frac{5}{24}$, $A_3 = \frac{13}{12}$, $A_4 = \frac{11}{108}$

5) RSA-kryptosystem med offentlig nyckel (5063, 1001)

$N = 5063 = (61)(83)$; $k = 1001$, $\phi(5063) = \phi(61)\phi(83) = 4920$

Privat nyckeln a : $1001a \equiv 1 \mod 4920$, lösning av

$1001a + 4920y = 1$ med $(4920, 1001) = 1$ och

(med division algoritm) $1 = 521(1001) + (-106)(4920)$

så $\underline{a = 521}$ (som kontroll $(521)(1001) = 521521 = (106)4920 + 1$)

6) Vi letar efter $10! - |A_1 \cup A_3 \cup A_5 \cup A_7 \cup A_9|$

där A_i = {permutationer där siffran i på plats i}, $i = 1,3,5,7,9$

$|A_i| = 9!$ för alla $5 = \binom{5}{1}$ mängder A_i

$|A_{i_1} \cap A_{i_2}| = 8!$ för alla $\binom{5}{2}$ mängder $A_{i_1} \cap A_{i_2}$

$|A_{i_1} \cap A_{i_2} \cap A_{i_3}| = 7!$ för alla $\binom{5}{3}$ mängder

$|A_{i_1} \cap A_{i_2} \cap A_{i_3} \cap A_{i_4}| = 6!$ för alla $\binom{5}{4}$ mängder

$A_1 \cap A_3 \cap A_5 \cap A_7 \cap A_9 = 5!$; för mängden

så vi har $10! - \binom{5}{1}9! + \binom{5}{2}8! - \binom{5}{3}7! + \binom{5}{4}6! - \binom{5}{5}5!$ sådana permutationer

Svar TATA52 Diskret matematik 4/6 2015

1) Visa att $4+5+7+9+\dots+2n+3=(n+2)^2$ för $n\geq 1$

Med IP

i) $n=1$ $VL_1=4+5=9=(1+2)^2=HL_1$; stämmer

ii) Om $4+5+7+9+\dots+2n+3=(n+2)^2$ för $n\geq 1$ vi vill visa att $4+5+7+9+\dots+2n+2+3$ är $(n+3)^2$

Då $4+5+7+9+\dots+2n+2+3 \overset{IP}{=} (n+2)^2+2n+3+2=$

$=n^2+6n+9=(n+3)^2$ är det bevisat. Med IP

$4+5+7+9+\dots+(2n+3)=(n+2)^2$ för $n\geq 1$.

2) G_1 och G_2 är isomorfa; t.ex funktionen

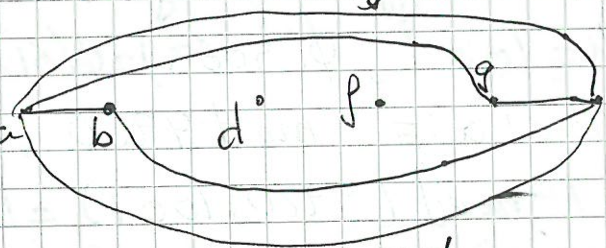
$1\to b$, $2\to a$, $3\to d$, $4\to c$, $5\to f$, $6\to g$, $7\to h$, $8\to e$

$9\to j$; $10\to i$, $11\to m$, $12\to k$.

2b) G_3 är eulersk ty alla noder har jämnt gradtal

men inte hamiltonsk, ty om vi tar bort "c" och "e"

får vi



som har 3 komponenter och $3>2$ st

3) a) Ab | Abc ... Öst | Öts

9 ger v + lös eller lös + vag

9 vagnar och 9 lösa men börjar antingen med vagn eller lös

9 vagnar lös + vagn eller vagn + lös

Så $(4)(18!)(21!)$

b) Det kan dela sig i så att antal deltagare i varje hotel n_i adderar till 100

Olika sätt $n_1+n_2+\dots+n_8=100 \to \binom{107}{7}$ olika sätt.