LINKÖPINGS UNIVERSITET
Matematiska institutionen
Milagros Izquierdo

Tentamen i Diskret Matematik, TATA82, TEN1, 2019–11–01, kl 08–13.

Inga hjälpmedel. Ej räknedosa. Fullständiga motiveringar krävs.

För betyg 3 behövs 9 poäng, för betyg 4, 12 poäng och 16 poäng för betyg 5.

---

1. Visa med induktionsprincipen att $\sum_{k=1}^{n}(4k+2) = 2n(n+2)$ för alla $n \geq 1$.

2. Är grafen nedan planär? hamiltonsk? eulersk? I så fall ange en hamiltonsk cykel och en sluten eulersk väg.

3. Visa att parametrarna $N = 1517, k = 1001$ och $a = 761$ är en bra publiknyckel k med motsvarande privatnyckel a i ett RSA-kryptosystem.

4. Lös den rekursiva ekvationen $a_n - 2a_{n-1} + a_{n-2} = 2n^2 + 2n$, $n \geq 2$, $a_0 = 1, a_1 = 5$.

5. I ett lotto väljer man 5 tal ur talen 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 och 15. Varje val av fem tal kallas en **lottorad**. Ange dina svar i heltal.

   (a) Hur många lottorader finns det i detta lotto? (1p)

   (b) En person har som spelidé att aldrig använda ett tal som valdes en gång till nästa gång. Personen spelar två dagar i rad. Hur många lottorader finns det till dag 2? (2p)

6. (a) I ett kortspel delar man ut 52 kort bland 4 spelare. På hur många sätt kan man göra det? (1p)

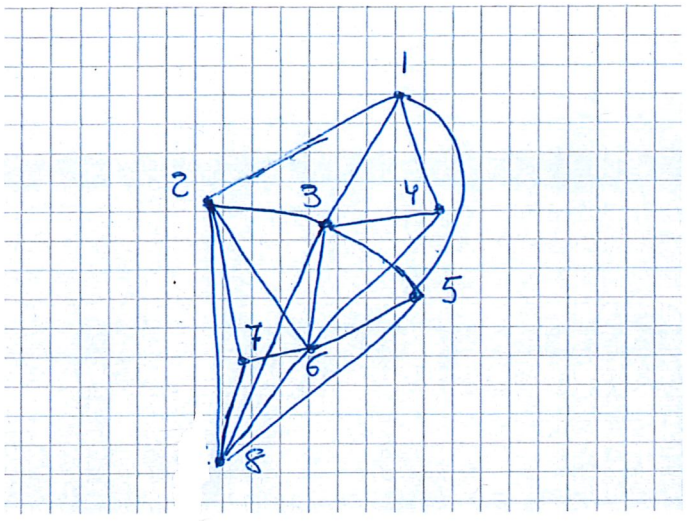
   (b) Vad är sannolikheten att få krona 5 gånger när man singlar slant 10 gånger? Ange sannolikheten i procent. (2p)

7. Betrakta alla punkter i planet $\mathbb{R}^2$ och den fixerade punkten $C = (1,2) \in \mathbb{R}^2$. Vi definierar en relation $\mathcal{R}$ på punkterna som följer: givet två punkter P, Q säger vi att $P\mathcal{R}Q$ om $d(P,C) = d(Q,C)$, där d är euklidiska avståndet mellan två punkter i planet.

   (a) Visa att $\mathcal{R}$ är en ekvivalensrelation.

   (b) Visa att mängden av ekvivalnesklasser är intervallet $[0, +\infty)$.

   (c) Visa att ekvivalensklassen av $P = (4,6)$ är cirkeln med medelpunkt C och radie 5..



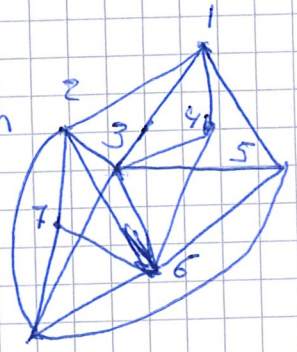
Svar TATA82 Discrete Mathematics 7/11 2019

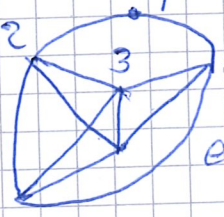
1) Show with MathInd that $\sum_{i=1}^{n}(4i+2) = 2n(n+2)$

i) for $n=1$ $VL_1 = 4(1)+2 = 6 = (2)(1)(1+2) = HL$, True

ii) Assume that $\sum_{i=1}^{n}(4i+2) = 2n(n+2)$ for some $n \geq 1$. We check that $VL_{n+1} = \sum_{i=1}^{n+1}(4i+2) = \sum_{i=1}^{n}(4i+2) + 4n+6 \overset{IndH}{=}$

$= 2n(n+2)+4n+6 = 2n^2+8n+6 = 2(n^2+4n+3) = 2(n+1)(n+1+2) = HL_{n+1}$ as wanted

2a) The graph 

is not planar since the subgraph 

is an edge-division of K_5

b) The graph is Hamiltonian. A Hamilton cycle is

$1 \to 2 \to 7 \to 8 \to 6 \to 5 \to 3 \to 4 \to 1$

c) The graph is not Eulerian since $\deg(2) = 5$, $\deg(4) = \deg(7) = 3$

3) The parameters $N = 1517 \Rightarrow k = 1001$ and $a = 761$ are good parameters for a RSA-cryptosystem, where k can be a public and a the corresponding private key.

i) $N = 1517 = (37)(41)$; i.e product of two prime nos

$\varphi(N) = (36)(40) = 1440 = (2)^5(3)^2(5)$

The parameter $k = 1001 = (7)(11)(13)$ satisfies that $\gcd(1001, 1440) = 1$ and so it is a good public key

Finally $a = 761$ is the corresponding private key if $(1001)a \equiv 1 \bmod 1440 \iff (1001)(761) \equiv 1 \bmod 1440$

It is since $(1001)(761) = 761761 = 1 + (529)(1440)$

Then a is the corresponding private key

4) Solve $a_n - 2a_{n-1} + a_{n-2} = 2n^2 + 2n$ $n \geq 2$; $a_0 = 1, a_1 = 5$

Homogeneous eq: $a_n - 2a_{n-1} + a_{n-2} = 0$

Ch. Eq $r^2 - 2r + 1 = 0$ $r_{1,2} = 1$ (double) $a_n^{(h)} = A_1 + A_2 n$

Particular sol $a_n^{(p)} = (B_1 n^2 + B_2 n + B_3) n^2$ where

$B_1 n^4 + B_2 n^3 + B_3 n^2 - 2B_1 (n-1)^4 - 2B_2 (n-1)^3 - 2B_3 (n-1)^2 + B_1 (n-2)^4 + B_2 (n-2)^3 + B_3 (n-2)^2 = 2n^2 + 2n$; where B_1, B_2, B_3 satisfy

$n^4 (B_1 - 2B_1 + B_1) + n^3 (8B_1 - 8B_1 + B_2 - 2B_2 + B_2) + n^2 (-12B_1 + 24B_1 + 6B_2 - 6B_2 + B_3 - 2B_3 + B_3) + n(8B_1 - 8B_1 - 6B_2 + 12B_2 + 4B_3 - 4B_3) + 14B_1 - 6B_2 + 2B_3 = 0n^4 + 0n^3 + 2n^2 + 2n + 0$; i.e

$$\begin{cases} 0 = 0 \\ 0 = 0 \\ 12B_1 = 2 \\ 6B_2 = 2 \\ 14B_1 - 6B_2 + 2B_3 = 0 \end{cases} \qquad B_1 = \frac{1}{6} \qquad B_2 = \frac{1}{3} \qquad B_3 = \frac{6B_2 - 14B_1}{2} = \frac{2 - \frac{7}{3}}{2} = -\frac{1}{6}$$

$$a_n = a_n^{(h)} + a_n^{(p)} = A_1 + A_2 n - \frac{n^2}{6} + \frac{n^3}{3} + \frac{n^4}{6}$$

Initial Conditions $\begin{cases} a_0 = 1 = A_1 \\ a_1 = 5 = A_1 + A_2 - \frac{1}{6} + \frac{1}{3} + \frac{1}{6} \end{cases}$ $\begin{matrix} A_1 = 1 \\ A_2 = \frac{11}{3} \end{matrix}$

$$\boxed{a_n = \frac{1}{6}\left(6 + 22n - n^2 + 2n^3 + n^4\right)}$$

5) The game consists in choosing 5 numbers out 1, 2, --, 15. Each choice is called a lotterd

a) there are then $\binom{15}{5} = \frac{(15)(14)(13)(12)(11)}{(5)(4)(3)(2)} = 12012$ lotteries

b) If we cannot use the 5 numbers used in day 1 we have $\binom{10}{5} = \frac{(10)(9)(8)(7)(6)}{(5)(4)(3)(2)} = 252$ lotteries

6) a) We must divide the 52 cards in 4 packages of 13 cards each $\binom{52}{13,13,13,13} = \frac{52!}{(13!)^4}$

b) Total number of sequences with Hr, Hl is 2^{10}

Sequences with 5 Hr and 5 Hl are $\binom{10}{5}$. Probability $\frac{\binom{10}{5}}{2^{10}}$

7) Consider the plane $\mathbb{R}^2$ and a fixed point $C(1,2)$. We define an equivalence relation $\mathcal{R}$ on $\mathbb{R}^2$ as follows $P \mathcal{R} Q$ iff $d(P,C) = d(Q,C)$

a) $\mathcal{R}$ is an equivalence relation since for every point P $d(P,C) = d(P,C)$, i.e. $\mathcal{R}$ reflexive

ii) If $P \mathcal{R} Q$, i.e $d(P,C) = d(Q,C)$, then $d(Q,C) = d(P,C)$ and $Q \mathcal{R} P$; i.e $\mathcal{R}$ symmetric

iii) If $P \mathcal{R} Q$ and $Q \mathcal{R} S$; i.e $d(P,C) = d(Q,C)$ and $d(Q,C) = d(S,C)$. Then $d(P,C) = d(S,C)$ and $P \mathcal{R} S$; i.e $\mathcal{R}$ transitive

b) An equivalence class is determined by the distance $d(P,C)$ and $\underline{0 \leq d(P,C) < \infty}$

c) $[P(4,6)] = \{ Q ; d(Q,C) = d((4,6),(1,2)) \}$

$= \{ (x,y) = Q ; (x-1)^2 + (y-2)^2 = 3^2 + 4^2 \} =$

$= \{ (x,y) ; (x-1)^2 + (y-2)^2 = 5^2 \}$