LINKÖPINGS UNIVERSITET
Matematiska institutionen
Milagros Izquierdo

Tentamen i Diskret Matematik, TATA52, TEN1, 2016–08–18, kl 8–13.

Inga hjälpmedel. Ej räknedosa. Fullständiga motiveringar krävs.

För betyg N behövs 3N-1 poäng.

---

1. Visa att $\sum_{k=1}^{n} k^3 = \frac{(n^2+n)^2}{4}$ för alla heltal $n \geq 1$.

2. Är grafen G nedan hamiltonsk? eulersk? planär? bipartit?

3. Ange svaren i denna uppgift som heltal.

   (a) Betrakta mängden $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Hur många injektiva (1-till-1) funktioner $f : \mathbb{Z}_4 \to \mathbb{Z}_8$ finns det. (1p)

   (b) Adam, Bea, Cecil, Dana, Egon, Fabiola, Gerard och Hanna ska arbeta under en tillställning som portier, kock, väktare, diskare och städare (en person till varje arbete). På hur många sätt kan de fördela dessa arbeten mellan sig? (1p)

   (c) Adam, Bea, Cecil, Dana, Egon, Fabiola, Gerard och Hanna har var sin boll i var sin färg. På hur många sätt kan man välja tre bollar? (1p)

4. En följd $\{a_n\}$ uppfyller differensekvationen
   $(n-1)(n-2)a_n - 4(n)(n-2)a_{n-1} + 3(n)(n-1)a_{n-2} = (4n+2)(n)(n-1)(n-2),\ n \geq 3$,
   där $a_1 = 5$, $a_2 = 16$.

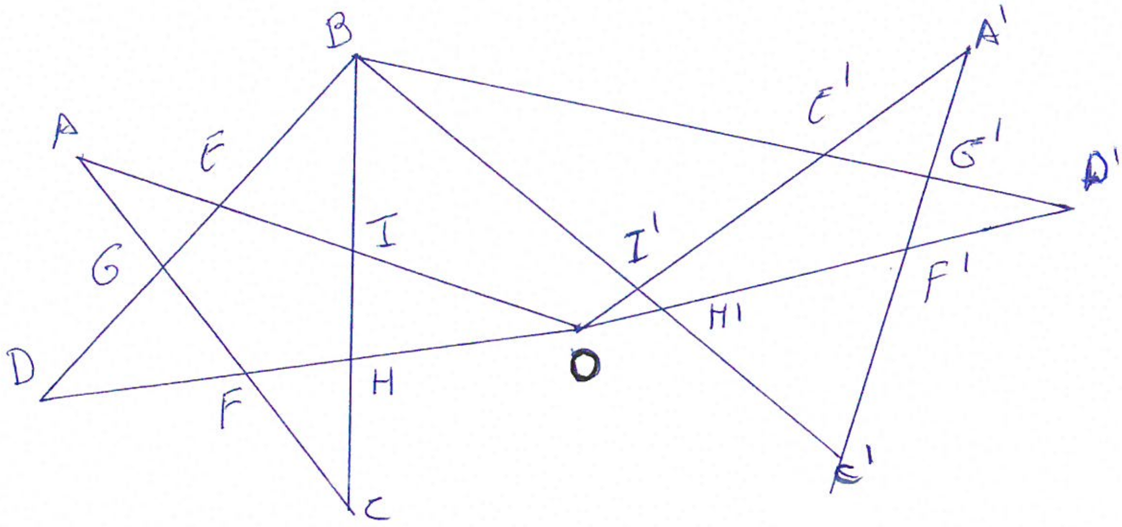
   (a) Betrakta den nya följden $\{b_n\}$ där $b_n = \frac{a_n}{n}$, för $n \geq 1$. Ange en ekvation (med begynnelsevillkor) för b_n. (1p)

   (b) Ange en formel för b_n och även för a_n. (2p)

5. (a) Bestäm $73^{1567} mod(990)$. (2p)

   (b) Är $(N, k) = (16113, 4543)$ och $a = 2154$ korrekta parametrar för ett RSA-krypteringssystem? ((N, k) är den offentliga nyckeln och a den privata). (1p)

6. Visa att ekvationen $x^2 - x - 1 \equiv 0$ har två lösningar i $\mathbb{Z}_{11}$ och ingen lösning i $\mathbb{Z}_7$. Kom ihåg: $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.



Svar TATA52 Discret matematik 18/8 2016

1) Show that $\sum_{k=1}^{n} k^3 = \frac{(n^2+n)^2}{4} \quad \forall n \geq 1$

With mathematical induktion we show

i) True for $n=1$ $\quad 1^3 = 1 = \frac{2^2}{4}$

ii) We assume that $\sum_{1}^{p} k^3 = \frac{p^2(p+1)^2}{4}$ for $p \geq 1$

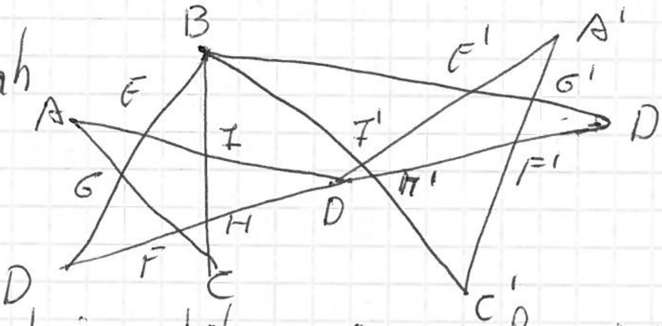
and show it for $n = p+1$

$$\sum_{1}^{p+1} k^3 = \sum_{1}^{p} k^3 + (p+1)^3 \overset{MI}{=} \frac{p^2(p+1)^2}{4} + (p+1)^3$$

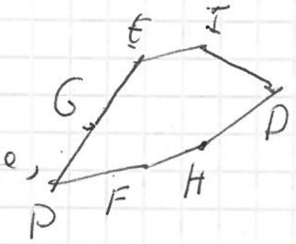
$$= \frac{(p+1)^2}{4}\left[p^2 + 4(p+1)\right] = \frac{(p+1)^2(p+2)^2}{4} \text{ as wanted.}$$

MI tells us ~~that the~~ formula is right $\forall n \geq 1$

2) The graph



a) is NOT bipartite since, for instance,



is a cycle of length 7 (odd).

b) is clearly planar (nodes in all crossings)

c) it is Eulerian, since all nodes have even degree

d) it is Hamiltonian, with a such cycle: B→

$B \to I \to E \to A \to G \to D \to F \to C \to H \to D \to J' \to H' \to C' \to F' \to D' \to G'$

$\to A' \to E' \to B$

3) 3a) There are $P(8,4) = 8\cdot 7\cdot 6\cdot 5 = 1680$ such functions

3b) In the same way there are $P(8,5) = 1680 \times 4 = 6720$ ways

3c) And equally $P(8,3) = 336$ ways of choosing balls with order and $C(8,3) = \frac{P(8,3)}{3!} = 56$ of choosing sets of three balls.

4) $(n-1)(n-2)a_n - 4n(n-2)a_{n-1} + 3n(n-1)a_{n-2} = (4n+2)n(n-1)(n-2)$

$a_1 = 5$, $a_2 = 16$ $\qquad n \geq 3$

a) Equation for $b_n = \frac{a_n}{n}$ is $b_1 = \frac{5}{1} = 5$, $b_2 = \frac{16}{2} = 8$
and for $n \geq 3$

$$\cancel{(n-1)(n-2)n}\, b_n - 4\cancel{n(n-2)(n-1)}\, b_{n-1} + 3\cancel{n(n-1)(n-2)}\, b_{n-2} = (4n+2)\cancel{n(n-1)(n-2)}, \quad (n, n-1 \text{ and } n-2 \text{ not } 0)$$

$$b_n - 4b_{n-1} + 3b_{n-2} = 4n+2, \quad b_1 = 5, \; b_2 = 8$$

b) We can solve b_n, $b_n^{(h)}$ solves $b_n - 4b_{n-1} + 3b_{n-2} = 0$
and it is $b_n^{(h)} = A_1 (1)^n + A_2 (3)^n$

So $b_n^{(p)} = (B_1 n + B_2) n$, setting them in the equation
we get $n^2(0B_1) + n(0B_2 - 4B_1) + (-2B_2 + 8B_1) = 4n+2$

so $-4B_1 = 4$, $B_1 = -1$ and $-2B_2 - 8 = 2$; $B_2 = -5$

From the initial conditions we get

$b_1 = 5 = A_1 + 3A_2 - 1^2 - 5$ $\qquad \left\{ \begin{array}{l} 11 = A_1 + 3A_2 \\ 22 = A_1 + 9A_2 \end{array} \right.$

$b_2 = 8 = A_1 + 9A_2 - 4 - 10$

$A_2 = \frac{11}{6}$, $A_1 = \frac{11}{2}$

$$\boxed{b_n = \frac{11}{6}(3)^n - n^2 - 5n + \frac{11}{2}, \quad a_n = \frac{11}{6}(3)^n n - n^3 - n^2 + \frac{11}{2} n}$$

5) As $990 = (9)(11)(2)(5)$ we use Chinese Remainder th.

$73^{1567} \equiv 1 \bmod 2$, $73^{1567} \equiv 1 \bmod 9$, $73^{1567} \equiv 6 \bmod 11$, $73^{1567} \equiv 2 \bmod 5$

$N = 990$, $N_1 = 495$, $x_1 = 1$	$N_2 = 110$, $x_2 = 5$	$N_3 = 90$, $x_3 = 6$	$N_4 = 198$, $x_4 = 2$

$73^{1567} \equiv (495)(1)^2 + (110)\times(1)\times 5 + (90)\times(6)\times(6) + (198)\times(2)\times(2)$

$\equiv 5077 \equiv \underline{127 \bmod 990}$

b) $N = 16113 = (123)(131)$ which is $\underline{\text{Not}}$ a product of two prime integers.
$= (41)(3)(131)$

NO correct parameters !!

Svar TATA 52 18-8-2016

6) $x^2-x-1\equiv 0$ has no solutions in $\mathbb{Z}_7=\{0,1,2,3,4,5,6\}$

since $0^2-0-1\not\equiv 0$, $1^2-1-1\not\equiv 0$, $4-2-1\not\equiv 0$, $2-3-1\not\equiv 0$, $2-4-1\not\equiv 0$, $4-5-1\not\equiv 0$ and $1-6-1\not\equiv 0$ all modulus 7

But $x^2-x-1\equiv 0$ has two solutions in $\mathbb{Z}_{11}$, since $0^2-0-1\not\equiv 0$, $1^2-1-1\not\equiv 0$, $4-2-1\not\equiv 0$, $9-3-1\not\equiv 0$, $\underline{5-4-1\equiv 0}$; $3-5-1\not\equiv 0$, $3-6-1\not\equiv 0$, $5-7-1\not\equiv 0$, $\underline{9-8-1\equiv 0}$, $4-9-1\not\equiv 0$ and $1-10-1\not\equiv 0$, all working modulus 11.

The solutions in $\mathbb{Z}_{11}$ are $x\equiv 4$ and $x\equiv 8$