Answers to TATA82 Discrete Maths 21/10 2022

1) Show with Math Induction that

$$\sum_{k=1}^{n} k^3+k^2-k-1 = \frac{n(n-1)(n^2 3+13n+16)}{12}, \quad \forall n \geq 1$$

We show: i) The formula is true for $n=1$

$$VL_1 = (1)^3+(1)^2-(1)-1 = 0 = \frac{(1)(0)(32)}{12} = HL_1, \text{ true}$$

ii) Assuming that $\sum_{1}^{n}(k^3+k^2-k-1) = \frac{n(n-1)(3n^2+13n+16)}{12}$ for some $n \geq 1$, we show that the formula still true for $n+1$. Now

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

$$\underset{\text{Assumpt}}{=} \frac{n(n-1)(3n^2+13n+16)}{12} + (n+2)((n+1)^2-1)$$

$$= \frac{n(n-1)(3n^2+13n+16)+12(n+2)^2 n}{12} =$$

$$= \frac{n(3n^3+22n^2+51n+32)}{12} = \frac{n(n+1)(3(n+1)^2+13(n+1)+16)}{12} = HL_{n+1}$$

v.s.v.

2a) A simple, connected, planar graph satisfies the equations

$$\begin{cases} V - E + F = 2 \\ 2E = \sum_{1} \deg(v_i) \\ 2E = \sum_{1}^{F} \deg(f_i) \end{cases}$$

V = no. nodes
E = no. edges
F = no. faces

i.e. $x+y=V$

$$\begin{cases} (x+y)-E+F=2 \\ 6x+3y=2E \\ 12+3(F-2)=2E \end{cases} \iff \begin{cases} 10 = E-F \\ 6x+3(12-x)=2E \\ 3F = 2E-6 \end{cases}$$

$\Leftarrow$ We get $\begin{cases} V=12, \text{ ~~of~~ which 4 has deg 6 and 8 deg 3} \\ E=24 \\ F=14 \end{cases}$

2b) A bipartite graph G is a subgraph of $K_{n,m}$ where $n+m=V$, then $E \leq n(V-n)$; the function $x(V-x)$ achieves a maximum for $n = \frac{V}{2}$. So $E \leq \frac{V}{2}\left(V-\frac{V}{2}\right) = \frac{V^2}{4}$.

3) How many results are possible in a votation with 5 candidates and 100 votes if each candidate gets at least 4 and at most 25 votes?

The question is equivalent to the number of non-negative integer solutions of

$x_1+x_2+x_3+x_4+x_5=100$, $4 \le x_i \le 25$, $1\le i\le 5$

(equiv.) $x_1+x_2+x_3+x_4+x_5 = 80$, $0 \le x_i \le 21$, $1 \le i \le 5$

Now let $\mathcal{U} = \{\text{solutions as above of } x_1+x_2+x_3+x_4+x_5=80, \ x_i \geq 0\}$

$$|\mathcal{U}| = \binom{80+4}{4} = \binom{84}{4}$$

We consider $A_i = \{\text{solutions in } \mathcal{U} \text{ where } x_i \geq 22\}$

we look for $|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4 \cap \bar{A}_5| =$

$= |\mathcal{U}| - |A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5|$. With PIE:

$$|A_i| = \binom{80-22+4}{4} = \binom{62}{4}, \ 1 \le i \le 5$$

$$|A_{i_1} \cap A_{i_2}| = \binom{80-44+4}{4} = \binom{40}{4}, \text{ for any choice of } 1 \le i_1 < i_2 \le 5$$

$$|A_{i_1} \cap A_{i_2} \cap A_{i_3}| = \binom{80-66+4}{4} = \binom{18}{4}, \ \alpha_4 = \alpha_5 = 0$$

So $|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4 \cap \bar{A}_5| = \binom{84}{4} - 5\binom{62}{4} + 10\binom{40}{4} - 10\binom{18}{4}$

number of possible results

4a) 11 divides $(21)^{2n} + 21(23)^n \quad \forall n \geq 1$

mod 11, $21 \equiv -1 \bmod 11$ and $23 \equiv 1 \bmod 11$. So,

$(21)^{2n} + 21(23)^n \equiv (-1)^{2n} + (-1)(1)^n \equiv (1)^n(1-1)$

$\equiv 0 \bmod 11$; i.e $(21)^{2n} + 21(23)^n$ a multiple of 11 $\forall n \geq 1$.

4b) First of all $(N = 9797, k = 1333)$ is a good key for a RSA cypher since $N = 9797 = (97)(101)$ is the product of two primes and $k = 1333$ is relative prime to $\varphi(9797) = (96)(100) = (2)^7(3)(5)^2$

- The deciphering key a is such that

$$1333\ a \equiv 1 \mod 9600$$

With Euclides' algorithm we get $a = 3997$

5) A sequence of negative integers is defined by the difference equation $a_n^3 - a_{n-1}^3 = -3n^2 + 9n - 7$ $n \geq 3$ and initial value $a_2 = -1$.

We call $b_n = a_n^3$ and we get the linear equation $b_n - b_{n-1} = -3n^2 + 9n - 3$, $b_2 = -1$

Now $b_n = b_n^{(h)} + b_n^{(p)}$ where $b_n^{(h)} = A$ since the charact eq is $r - 1 = 0$; and $b_n^{(p)} = C_1 n^3 + C_2 n^2 + C_3 n$

; where $C_1 n^3 + C_2 n^2 + C_3 n - C_1(n-1)^3 - C_2(n-1)^2 - C_3(n-1) =$
$= -3n^2 + 9n - 7$

so $b_n^{(p)} = -n^3 + 3n^2 - 3n$ $(C_1 = -1, C_2 = 3, C_3 = -3)$

and by the initial value $b_2 = -1 = -8 + 12 - 6 + A$

$(A = 1)$ $\quad b_n = -n^3 + 3n^2 - 3n + 1 = (1-n)^3$ so

$$\boxed{a_n = 1 - n \quad , \quad n \geq 2}$$

6) A word in a code consists of an arrangement of 1,2,3,4,5 followed of an arrangement of A, B, C, D, E. The uncoded word is 12345ABCDE then the code consists of

$(5!)(5!) - 1 = (120)^2 - 1 = \underline{14399 \text{ coded words}}$

7) Consider $A = \{(x, y) ; x, y \in \mathbb{Z}, y \neq 0\}$ and the relation $\mathcal{R}$ on A given by

$(x_1, y_1) \mathcal{R} (x_2, y_2)$ if $x_1 y_2 = x_2 y_1$

a) Given $(0, y_1)$, $y_1 \neq 0$, Show that a pair (x, y), $y \neq 0$ is related to $(0, y_1)$ iff $x = 0$

By definition $(x, y) Q (0, y_1)$ iff $(x)(y_1) = (0)(y)$ as y_1 and y are not 0, that's to say that

$$x = 0$$

b) Q is an equivalence relation

i) Q is reflexive since $\forall (x, y) \in A \quad xy = xy$ i.e $(x, y) Q (x, y)$

ii) Q is symmetric since if $(x_1, y_1) Q (x_2, y_2)$, i.e $x_1 y_2 = x_2 y_1$, then $x_2 y_1 = x_1 y_2$ and $(x_2, y_2) Q (x_1, y_1)$

iii) Q is transitive since if $(x_1, y_1) Q (x_2, y_2)$ and $(x_2, y_2) Q (x_3, y_3)$, then $x_1 y_2 = x_2 y_1$ and $x_2 y_3 = x_3 y_2$ (multiplying) $x_1 y_2 y_3 x_2 = x_2 y_1 x_3 y_2$, as $y_2 \neq 0$ $\Longleftrightarrow x_1 y_3 x_2 = x_2 x_3 y_1$. Now

1) if $x_2 = 0$ then by a)-part $x_1 = x_3 = 0$ and $(0, y_1) Q (0, y_3)$

2) if $x_2 \neq 0$, simplying $x_1 y_3 = x_3 y_1$ and $(x_1, y_1) Q (x_3, y_3)$

c) Show that, given the pair (t, n), $n \neq 0$ and $t/n = q$ The equivalent class of (t, n) consists of the pairs (x, y), $y \neq 0$, s.t $x/y = q$.

But $[(t, n)] = \{(x, y) ; y \neq 0, \ ty = xn\} =$

$= \{(x, y) ; y \neq 0 \ \frac{t}{n} = \frac{x}{y} = q\} = \{(x, y) ; y \neq 0, \frac{x}{y} = q\}$

LINKÖPINGS UNIVERSITET
Matematiska institutionen
Milagros Izquierdo

Tentamen i Diskret Matematik, TATA82, TEN1, 2022–10–21, 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 $\sum_{k=1}^{n} k^3+k^2-k-1 = \frac{n(n-1)(3n^2+13n+16)}{12}$ för alla $n \geq 1$

2. (a) En enkel, sammanhängande, planär graf har 12 noder; några av dem har gradtal 6 och resterande gradtal 3. Av regionerna har två gradtal 6 och resterande gradtal 3. Beräkna antal noder, kanter och regioner. (2p)

   (b) Betrakta en bipartit graf G med V noder och E kanter. Visa att $E \leq \frac{V^2}{4}$. (1p)

3. I ett lokalt val röstar 100 personer på 5 kandidater. Hur många valresultat finns det om varje kandidat får minst 4% och högst 25% av rösterna?

4. (a) Visa att $(21)^{2n} + 21(23)^n$ är delbart med 11, för alla $n \geq 1$ (1p)

   (b) Visa att $(N = 9797, k = 1333)$ bildar en bra krypteringsnyckel för ett RSA kryptosystem med totalt nummer $N = 9797$. Bestäm avkrypteringsnyckeln som motsvarar k (2p)

5. En följd av negativa heltal $\{a_n\}$ ges av rekursiva ekvationen $a_n^3 - a_{n-1}^3 = -3n^2 + 9n - 7$, $n \geq 3$, $a_2 = -1$. Bestäm en formel för a_n.

6. Ord i en kod består av 5 olika siffror: 1, 2, 3, 4, 5 på positioner 1 till 5; och 5 olika bokstäver: A, B, C, D, E på positioner 6 till 10. Det okodade ordet är 12345ABCDE. Hur många kodade ord har koden? Svara med ett heltal.

7. Betrakta mängden, $A = \{(x, y);\ x, y \in \mathbb{Z},\ y \neq 0\}$. Vi definierar en relation $\mathcal{Q}$ på A genom $(x_1, y_1)\mathcal{Q}(x_2, y_2)$ om $x_1 y_2 = y_1 x_2$.

   (a) Givet $(0, y_1)$, $y_1 \neq 0$ visa att ett par $(x, y), y \neq 0$ är relaterat till $(0, y_1)$ om och endast om $x = 0$. (1p)

   (b) Visa att $\mathcal{Q}$ är en ekvivalensrelation (1p).

   (c) Visa att, givet ett par $(t, n), n \neq 0$ med $t/n = q$, q rationellt tal, består ekvivalensklassen till (t, n) av paren $(x, y), y \neq 0$ som uppfyller att $x/y = q$. (1p)