LINKÖPINGS UNIVERSITET
Matematiska institutionen
Milagros Izquierdo

Tentamen i Diskret Matematik, TATA32 (916G24), TEN1, 2021–03–18, kl 08–13.

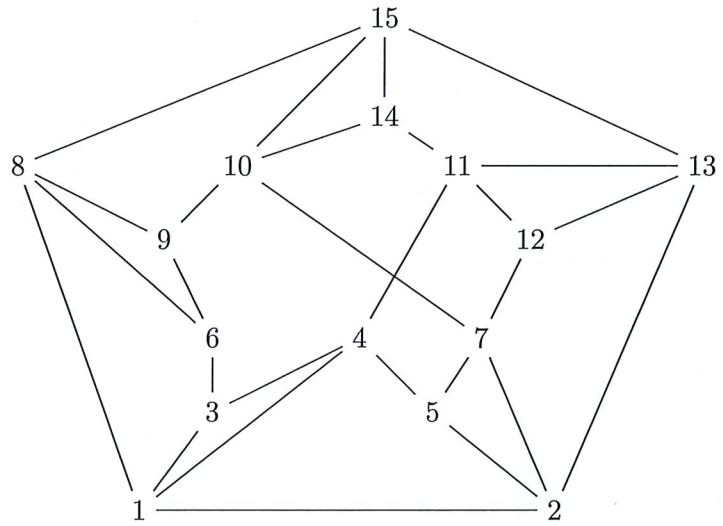
Inga hjälpmedel. Ej räknedosa. Fullständiga motiveringar krävs.

För betyg 3 behövs 20 poäng, för betyg 4, 26 poäng och 32 poäng för betyg 5, inklusive eventuella bonuspoäng.

---

1. Visa att för alla naturliga tal $n \geq 0$ gäller att $1 - \frac{n}{4} \leq (\frac{3}{4})^n$ (Vi behöver inte visa att $(\frac{3}{4})^n < 1$, det är välkänt). Olikheten ovan är ett exempel på Bernouillis olikhet, som används i uppskattning av sannolikheter. (5p)

2. Studera om grafen nedan är eulersk, hamiltonsk, bipartit och planär, samt visa att dess kromatiska tal är 3. (1p/fråga)



3. Hur många heltal t mellan 1 och 2021 är relativt prima med $2020 = (2)^2(5)(101)$? (5p)

4. En aktuell tjuv får viktig information om en medlem i en klubb som använder RSA-kryptering med totalnummer $N = pq$. Tjuven får den offentliga nyckeln till användare $(N, k = 1399)$ samt att $p = 43$ och att Eulerstal av N, $\varphi(N) = 1932$.

   (a) Bestäm heltalen N och q. (1p)

   (b) Bestäm medlmmens privata nyckel som passar den offentlig nyckeln $(N, k = 1399)$. (2p)

   (c) Medlemmen använder sin privata nyckel för att autentisera sig. Medlemmen knappar meddelande 1,8. Vilket meddelande får banken (innan banken använder medlemmens offentliga nyckel)? (2p)

5. Lös den rekursiva ekvationen $a_n - 4a_{n-1} + 4a_{n-2} = n - 4$, $a_0 = 2$, $a_1 = 5$. (5p)

VÄND

6. Sex studenter kommer till en tentamen och de lämnar sina mobiler och klockor (6 stycker av varje) i ett skåp hos tentamenservicen. På hur många sätt kan man lämna tillbaka mobiler och klockor så att INGEN student får tillbaka varken sin egen mobil eller klocka? Att inte skriva svaret som ett heltal i kvadrat ger maximalt 4 av de 5 poängen. (5p)

7. Betrakta mängderna $\mathcal{U} = \{1, 2, 3, 4, 5\}$, mängden A bestående av alla delmängder till $\mathcal{U}$ och $F = \{1, 5\} \in A$. Vi definierar en relation $\mathcal{R}$ på A genom: $X\mathcal{R}Y$ om $X \cup F = Y \cup F$

   (a) Visa att $\mathcal{R}$ är en ekvivalensrelation på A. (3p)

   (b) Bestäm partitionen på A som $\mathcal{R}$ definierar (dvs bestäm alla ekvivalensklasser till $\mathcal{R}$). (2p)

8. Formulera och bevisa satsen: Ekvivalens av existens av ekvivalensrelation och partition på en mängd A.

   De nödvändiga begreppen som används i satsen ska definieras. (5p)

Svar till TATA32 Diskret matematik. 19/3 2021

1) Visa att för alla $n \geq 0$ gäller att $1 - \frac{n}{4} \leq \left(\frac{3}{4}\right)^n$.

Vi visar det med IP. För att göra det visar vi

i) Påstående sant för $n = 0$:

$$VL_0 = 1 - 0 = 1 \underbrace{\leq}\ 1 = \left(\frac{3}{4}\right)^0 = HL_0$$

ii) Vi antar att för något $n \geq 0$ gäller $1 - \frac{n}{4} \leq \left(\frac{3}{4}\right)^n$ och visar för $n+1$:

$$HL_{n+1} = 1 - \frac{n+1}{4} = 1 - \frac{n}{4} - \frac{1}{4} \overset{\text{Antagande}}{\leq} \left(\frac{3}{4}\right)^n - \frac{1}{4}$$

Vi behöver visa, t.ex, att $\left(\frac{3}{4}\right)^n - \frac{1}{4} \leq \left(\frac{3}{4}\right)^{n+1} = HL_{n+1}$

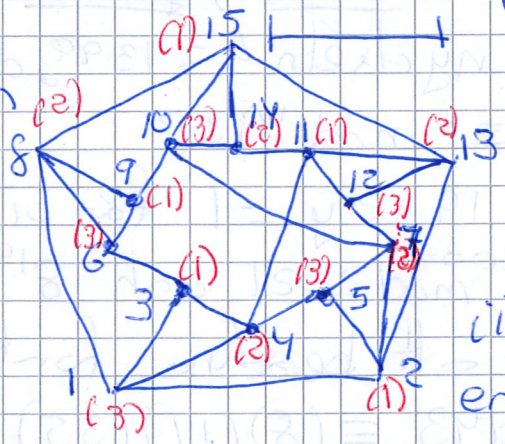
Men $\left(\frac{3}{4}\right)^n - \frac{1}{4} \leq \left(\frac{3}{4}\right)^{n+1} \iff \left(\frac{3}{4}\right)^n - \left(\frac{3}{4}\right)^{n+1} \leq \frac{1}{4}$

$\iff \left(\frac{3}{4}\right)^n \left(1 - \frac{3}{4}\right) \leq \frac{1}{4}$ som är sant ty

$\left(\frac{3}{4}\right)^n \leq 1$ och $\left(\frac{3}{4}\right)^n \left(1 - \frac{3}{4}\right) = \left(\frac{3}{4}\right)^n \left(\frac{1}{4}\right) \leq (1)\frac{1}{4}$

Så vi har sett att $1 - \frac{n+1}{4} \leq \left(\frac{3}{4}\right)^n - \frac{1}{4} \leq \left(\frac{3}{4}\right)^{n+1}$ v.s.v.

2) Grafen



i) Är inte enkelt eftersom t.ex $d(3) = d(6) = d(12) = 3$, udda

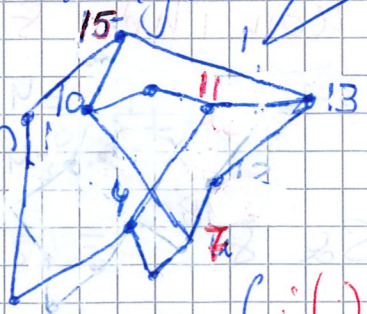
ii) Är hamiltonsk med en hamiltoncykel

15 - 8 - 1 - 2 - 13 - 11 - 12 - 7 - 5 - 4 - 3 - 6 - 9 - 10 - 14 - 15

iii) Är inte bipartit ty den innehåller trianglar

så $\chi(G) > 2$

iv) Är inte planär eftersom delgrafen är en kantindelning av $K_{3,3}$



v) Vi ser att $\chi(G) \leq 3$ med en färgning som ovan (i))

3) Vi löser detalet med PIE. Vi modellerar:

$\mathcal{U} = \{t \in \mathbb{Z};\ 1 \le t \le 2021\}$

$A_1 = \{t \in \mathcal{U};\ 2 \mid t\}$

$A_2 = \{t \in \mathcal{U};\ 5 \mid t\}$

$A_3 = \{t \in \mathcal{U};\ 101 \mid t\}$

Ett heltal $t \geq 1$ är relativt prim med 2021 om och endast om t är inte delbart med 2, 5 eller 101

Vi letar efter

$|A_1 \cup A_2 \cup A_3| = |\mathcal{U}| - |A_1 \cup A_2 \cup A_3|$

Nu $|A_1| = 1010$, $|A_2| = 404$, $|A_3| = 20$

$|A_1 \cap A_2| = 202$; $|A_1 \cap A_3| = 10$; $|A_2 \cap A_3| = 4$

$|A_1 \cap A_2 \cap A_3| = 2$

Så $|A_1 \cup A_2 \cup A_3| = 2021 - 1010 - 404 - 20 + 202 + 10 + 4 - 2 = \underline{801}$ sådana tal

4) Ett RSA-kryptering med tal numer $N = pq$

$p = 43$ $\quad \varphi(N) = (p-1)(q-1) = 1932$ och $q-1 = 46$, $q = 47$

i) $\underline{N} = pq = (43)(47) = \underline{2021}$, $\underline{q = 47}$

ii) Om den offentliga nyckeln $k = 1399$, den privata a uppfyller $1399\,a \equiv 1 \bmod 1932$

Löser vi $1399a + 1932y = 1$ får vi $\underline{a = 1903}$

iii) Banken får $1^{1903} \bmod 2021$ och $8^{1903} \bmod 2021$

Vi använder KRS för att beräkna först $8^{1903} \bmod 2021$

$8^{1903} \bmod 43 \equiv 8^{13} \bmod 43 \equiv (8)(11)(35) \equiv 27 \bmod 43$

$8^{1903} \bmod 47 \equiv 8^{17} \bmod 47 \equiv (8)(4) \equiv 32 \bmod 47$

Kom ihåg $8^{42} \equiv 1 \bmod 43$, $8^{46} \equiv 1 \bmod 47$

$N = 2021$, $n_1 = 43$, $N_1 = 47$, $x_1 = 11$ $(47x_1 \equiv 1 \bmod 43)$

$n_2 = 47$, $N_2 = 43$, $x_2 = -12$ $(43x_2 \equiv 1 \bmod 47,\ -4x_2 \equiv 1 \bmod 47)$

Så $8^{1903} \equiv (27)(47)(11) - (32)(43)(12) \equiv \underline{1489} \pmod{2021}$

5) Lös ekvationen $a_n - 4a_{n-1} + 4a_{n-2} = n-4$, $a_0 = 2$
$a_1 = 5$

Lösning $a_n = a_n^{(h)} + a_n^{(p)}$ där
$a_n^{(h)}$ löser en homogen ekvation med <u>K.E</u> $r^2 - 4r + 4 = 0$
$r_{1,2} = 2$ (dubbel); $a_n^{(h)} = (A_1 + A_2 n)(2)^n$
För att hitta <u>en</u> partikulärlösning vi noterar att högerleden $f(n) = (n-4)(1)^n$ är ett polynom av grad 1 (och $1 \neq 2$) Gissa $a_n^{(p)} = B_1 n + B$. Sätt in i ekv

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

$n(B_1 - 4B_1 + 4B_1) + B_2 + 4B_1 - 8B_1 = n - 4$ $\begin{cases} \underline{B_1 = 1} \\ B_2 = -4 + 4B_1 = \underline{0} \end{cases}$

$a_n = n + (A_1 + A_2 n)(2)^n$

Med BV $\begin{cases} a_0 = 2 = A_1 \\ a_1 = 5 = 1 + 2A_1 + 2A_2 \end{cases}$ $\underline{A_1 = 2}$ $A_2 = 0$

$$\boxed{a_n = n + (2)^{n+1}}$$

6) För att räkna total antal sätt, vi använder MP och ser att total antal sätt $a = a_k \cdot a_m$ där a_k är alla sätt där klockor lämnas "felaktigt" och a_m är alla sätt där mobiler lämnas "felaktigt"
Vi vet att vi har permuterat alla sex studenter och ingen har kommit till dess ursprungliga position (där föremål fanns) för både a_k och a_m, så
$a_k = a_m = d_6$ $\therefore$ d_6 = Antal derangemang av 6 (föremål)

$a = (d_6)^2$

$$d_6 = \sum_{k=2}^{6} \frac{6!\,(-1)^k}{k!} = \frac{720}{2} - \frac{720}{6} + \frac{720}{24} - \frac{720}{120} + 1 = \underline{265}$$

$$\boxed{a = (265)^2}$$

7) $A = \{$ delmängder till $\{1,2,3,4,5\}\}$ $|A| = 32$, $F = \{1,5\}$

Vi definierar $\mathcal{R}$ på A genom $X \mathcal{R} Y$ om $X \cup F = Y \cup F$

(a) $\mathcal{R}$ ekvivalens relation ty

i) $\mathcal{R}$ reflexiv: $\forall X \in A$ $X \cup F = X \cup F$

ii) $\mathcal{R}$ symmetrisk; om $X \mathcal{R} Y$ dvs $X \cup F = Y \cup F \Leftrightarrow$
$Y \cup F = X \cup F \Leftrightarrow Y \mathcal{R} X$

iii) $\mathcal{R}$ transitiv: om $X \mathcal{R} Y$ och $Y \mathcal{R} Z \Leftrightarrow$
$X \cup F = Y \cup F = Z \cup F$, så $X \cup F = Z \cup F \Leftrightarrow X \mathcal{R} Z$

(b) Vi ser att $\emptyset \cup \{1,5\} = \{1\} \cup \{1,5\} = \{5\} \cup \{1,5\} = \{1,5\} \cup \{1,5\}$

så $[\emptyset] = \{\emptyset, \{1\}, \{5\}, \{1,5\}\}$

Likadant

$[\{2\}] = \{\{2\}, \{1,2\}, \{2,5\}, \{1,2,5\}\}$

$[\{3\}] = \{\{3\}, \{1,3\}, \{3,5\}, \{1,3,5\}\}$

$[\{4\}] = \{\{4\}, \{1,4\}, \{4,5\}, \{1,4,5\}\}$

$[\{2,3\}] = \{\{2,3\}, \{1,2,3\}, \{2,3,5\}, \{1,2,3,5\}\}$

$[\{2,4\}] = \{\{2,4\}, \{1,2,4\}, \{2,4,5\}, \{1,2,4,5\}\}$

$[\{3,4\}] = \{\{3,4\}, \{1,3,4\}, \{3,4,5\}, \{1,3,4,5\}\}$

$[\{2,3,4\}] = \{\{2,3,4\}, \{1,2,3,4\}, \{2,3,4,5\}, \{1,2,3,4,5\}\}$

Partitionen på A är

$A = [\emptyset] \cup [\{2\}] \cup [\{3\}] \cup [\{4\}] \cup [\{2,3\}] \cup [\{2,4\}] \cup$
$\cup [\{3,4\}] \cup [\{2,3,4\}]$

8)