FX-SKRIVNING 1 – JANUARI 2022

Tillåtna hjälpmedel är ett A4-ark med egna anteckningar från kursen, ingen miniräknare. Anteckningar får finnas på båda sidor av arket. Inlämning sker i form av fotograferade handskrivna lösningar i aktuell Quiz på kurswebben. Om ni av någon anledning inte kan scanna in en fil och måste mejla den till mig, ladda istället upp en platsmarkörsfil och mejla er lösning till mig. Jag kan inte rätta uppgifter som inte har uppladdade bildfiler och observera att om ni trycker på "skicka in"/"submit" så kan ni inte längre lämna in några lösningar. Om ni mejlar en lösning till mig *måste* också detta föregås av en diskussion med mig (ansvarig lärare) på skrivningens zoommöte under skrivtiden, eller ett telefonsamtal: 08-7909473.

Skrivtiden är de normala 2 timmarna för en fx-skrivning plus 30 minuter extra tid för bildhantering & upp-laddning, skrivningen tillgängligörs några minuter innan 14.45 på kurswebben och sista (ordinarie) inlämningstid blir alltså 17.00. Observera att all behandling av alla uppgifter och all hantering med inlämning ska ske under denna tid. Annars rättas inte lösningarna. Det är Canvas tidsstämplar som gäller. (Några har förlängd skrivtid och motsvarande klockslag för dem är 18.00.)

Till denna skrivning hör en muntlig tentamen (för några) och de uppgifter som kan användas för muntlig tentamen är **2**, **3**, **5** och **6**.

Fullständiga och korrekta motiveringar krävs för alla uppgifter.

1. Logik. Visa att följande slutledning är riktig genom att ange en detaljerad redogörelse för hur slutsatsen följer av premisserna med angivande av alla regler som behövs användas (*Modus Ponens*, *Modus Tollens* etc.)

1. $p \to (q \to r)$
2. $(p \to q) \to r$
3. $r \to \neg t$ (Uppgiften kan alltså *inte* lösas bara med hjälp av en sanningstabell.)
4. $\neg t \to \neg r$

$\therefore$ $\neg q$

2. Mängdlära. Låt A, B, C beteckna mängder vilka som helst. Betrakta nedanstående två påståenden. Det ena är sant och det andra är falskt. Ange vilket som är sant och vilket som är falskt och bevisa det sanna och motbevisa det falska.

$$A \subset B \cap C \wedge B \subset A \cap C \wedge C \subset A \cap B \Rightarrow A = B = C$$
$$A \subset B \cup C \wedge B \subset A \cup C \wedge C \subset A \cup B \Rightarrow A = B = C$$

Som ett undantag är det nu tillåtet att använda Venndiagram, men om du gör det *måste* de vara mycket tydliga, rita dem hellre för stora än för små. Du behöver också motivera *ordentligt* med text. Bara Venndiagram med bristfällig text är underkänt. För det påstående som ska motbevisas måste tre exempelmängder, A, B, C hittas som uppfyller förledet i implikationen men inte efterledet.

3. Funktioner. Vi låter P vara en funktion från $\mathbb{R}^n$ till $\mathbb{R}^n$ som uppfyller följande två krav:

1. P är *linjär*, det vill säga för alla $x, y \in \mathbb{R}^n$ och alla $a, b \in \mathbb{R}$ gäller $P(ax + by) = aP(x) + bP(y)$.
2. P är en *projektion*, det vill säga $P \circ P = P$.

Visa att om $P \neq \iota$ så är P inte injektiv.

4. Inledande talteori. I den mycket viktiga RSA-algoritmen används så kallade krypterings- och dekrypteringstal som vi kallar e respektive d. Dessa är positiva heltal som vi tar fram baserat på ett par av hemliga primtal p och q på följande sätt:

Steg 1. Välj två primtal p, q.
Steg 2. Bilda talet $\phi = (p-1)(q-1)$.
Steg 3. Välj e, d sådana att $ed \equiv 1 \pmod{\phi}$

Ange det minsta $d > 1$ som uppfyller kraven i de olika stegen ovan om $p = 5$, $q = 11$ och $e = 7$.

5. Relationer. Beteckna med A mängden av alla positiva heltal ($\{1, 2, 3, \ldots\}$). Definiera relationen $\mathcal{R}$ på A genom

$$a\mathcal{R}b \Leftrightarrow a|b^2 \wedge b|a^2.$$

Bevisa att $\mathcal{R}$ *inte* är en ekvivalensrelation.

6. Fördjupad talteori. Studera följande identiteter

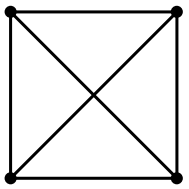
$$1 \cdot 2 = \frac{1}{3} \cdot 1 \cdot 2 \cdot 3,$$

$$1 \cdot 2 + 2 \cdot 3 = \frac{1}{3} \cdot 2 \cdot 3 \cdot 4,$$

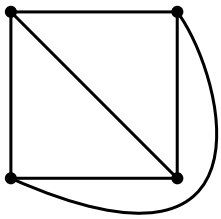
$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 = \frac{1}{3} \cdot 3 \cdot 4 \cdot 5.$$

Baserat på dessa likheter, formulera en hypotes (i form av en formel) med ett summatecken och bevisa sedan formeln med matematisk induktion.

7. Grafteori. I denna uppgift angvänds ordet ”graf” för både pseudografer och vanliga grafer. En graf kallas *plan* om den kan ritas utan överkorsande kanter. Det är inte alltid lätt att se om en graf är plan eller inte. K_5 respektive $K_{3,3}$ är inte plana. K_4 är dock plan. Nedan visas en figur där vi kan se varför K_4 är plan.



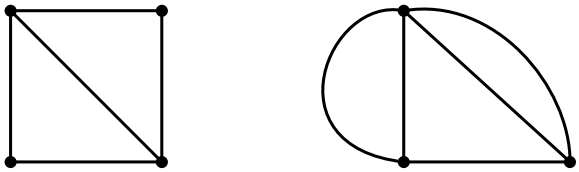
K_4



K_4 *ritad plant*

Till vänster är K_4 ritad, inte plant, en kant korsar en annan. Till höger ges en framställning av K_4 som är ritad plant, inga kanter korsar någon annan. Med detta har vi visat att K_4 är plan. Läsaren uppmuntras att försöka rita K_5 respektive $K_{3,3}$ plant för att få en känsla för vad en plan graf är. (Det kommer inte att lyckas eftersom K_5 och $K_{3,3}$ som sagt *inte* är plana.)

En plan graf delar upp den plana yta som den är ritad på i ett antal delytor. Om dessa är F till antalet så har en plan graf tre tal: V = antalet hörn, E = antalet kanter och F = antalet delytor som grafen delar upp planet i. Nedan illustreras detta begrepp för två plana (pseudo)grafer:



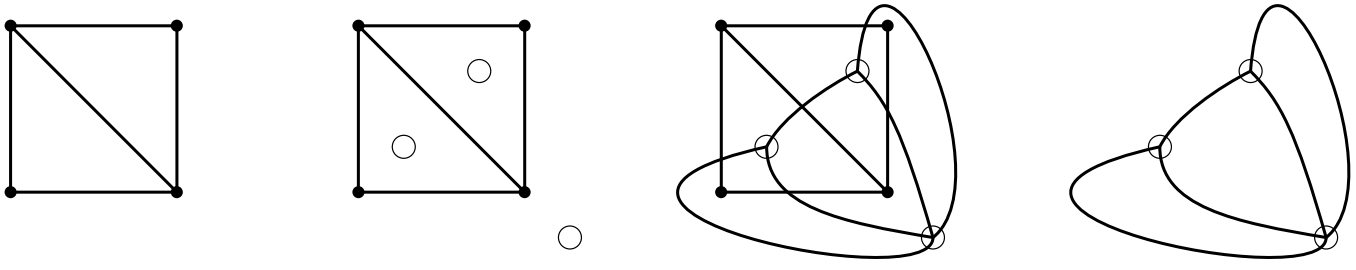
Till vänster ser vi en plan graf med $V_1 = 4$, $E_1 = 5$ och $F_1 = 3$, till höger ser vi en pseudograf med $V_2 = 3$, $E_2 = 5$ och $F_2 = 4$.

Vi låter nu $G = (\mathcal{V}_1, \mathcal{E}_1)$ vara en plan graf med $V_1 = |\mathcal{V}_1|$ hörn, $E_1 = |\mathcal{E}_1|$ kanter och f delytor. Vi skapar nu en ny graf G' genom följande procedur:

Steg 1. Placera ett nytt hörn i varje delyta.

Steg 2. För varje kant e i G inför en kant e' i G' på följande sätt: förbind de två isolerade noderna som ligger i delytorna som avgränsas av e så att e' korsar e.

Dessa steg finns illustrerade i nedanstående figur:



Längst till vänster ser vi ursprungsgrafen, G, i mitten till vänster ser vi de införda nya hörnen som ska höra till den nya grafen. Vi illustrerar de nya hörnen med större prickar som inte är ifyllda. I mitten till höger har dessa nya hörn förbundits med de nya kanterna enligt steg 2 i proceduren ovan. Längst till höger ser vi den nya grafen G'.

Vi kallar en graf G' som är skapad på detta sätt utgående från en given plan graf G för *den duala grafen till* G.

Visa att summan av gradtalen av alla hörn i G' och summan av alla gradtalen av alla hörn i G alltid är lika.

8. Kombinatorik. Låt $n > 0$ vara ett godtyckligt heltal. Visa algebraiskt (alltså inte genom att hänvisa till ett kombinatoriskt resonemang) att för alla heltal $0 \leq k < n$ gäller olikheten

$$\binom{2n}{k} < \binom{2n}{n}.$$

Ledning: Du kan försöka visa att $\binom{2n}{k} < \binom{2n}{k+1}$ för alla $k = 0, 1, \ldots, n-1$. Då följer $\binom{2n}{k} < \binom{2n}{n}$ om $k < n$.

9. Sannolikhetslära. Antag att A, B, C är tre händelser som uppfyller följande krav:

1. $P(A \cap (B \cup C)^c) = P(B \cap (A \cup C)^c) = P(C \cap (A \cup B)^c) = 0.3$
2. Alla tre kan inte inträffa samtidigt men någon av dem inträffar säkert.

Beräkna sannolikheten av att precis två av dem inträffar.

Ledning: Du får motivera med ett Venndiagram hur den sökta sannolikheten är fördelad. Vi gör alltså ett undantag till här gällande Venndiagram och här gäller återigen att du måste motivera noggrannt med text varför Venndiagrammet ser ut som det gör.