LÖSNINGAR TILL ÖVNINGSTENTA DISKRET MATEMATIK FÖR IT2 ht08

DEL I

Var och en av nedanstående uppgifter svarar mot en kontrollskrivning. Godkänt resultat på en kontrollskrivning ger automatiskt full poäng på motsvarande uppgift. Att lösa en uppgift som man på detta sätt redan har till godo ger inga extra poäng.

1. (3p) Bestäm den minsta positiva resten som erhålls när talet 53^{36} delas med talet 37.

   Lösning: Vi använder Fermats lilla sats. Eftersom 37 är ett primtal och talet 37 inte delar talet 53 gäller att
   $$53^{37-1} \equiv 1 \pmod{37}.$$
   Därmed har vi omedelbart vårt

   SVAR: Talet 1.

2. (3p) Bestäm antalet binära ord av längd 15 som innehåller precis 3 stycket ettor. Svaret skall ges i formen av ett heltal.

   Lösning: Bland 15 möjliga positioner för ettorna i ordet skall tre positioner väljas. Detta kan ske på
   $$\binom{15}{3} = \frac{15 \cdot 14 \cdot 13}{1 \cdot 2 \cdot 3} = 5 \cdot 7 \cdot 13 = 455,$$
   olika sätt.

   SVAR: 455.

3. (3p) Gruppen $(Z_{20}, +)$ har ett antal delgrupper och en samling av olika sidoklasser till dessa delgrupper. En av dessa sidoklasser innehåller precis fem element varav elementet 3 är ett av dessa fem element. Ange samtliga element i denna sidoklass.

   Lösning: Gruppen $(Z_{20}, +)$ har precis en delgrupp med fem element nämligen mängden
   $$H = \{0, 4, 8, 12, 16\}.$$
   Sidoklassen
   $$3 + H = \{3, 7, 11, 15, 19\},$$
   är den sökta sidoklassen.

4. (3p) Den e-felsrättande koden C har kontrollmatrisen (eng: (parity) check matrix)
   $$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

   (a) Bestäm e. (**OBS:** Glöm ej att ge en kortfattad motivering!)

   Lösning: Kodens minimiavstånd är tre eftersom, dels kolonnerna är olika och dels både nollordet 000000 och ordet 000111 (se nedan) tillhör koden C. Koden kan då rätta högst ett fel och därmed är $e = 1$.
   SVAR: $e = 1$.

(b) Bestäm ett ord $\bar{c} \in C$ sådant att $\bar{c} \neq \bar{0}$.

Lösning: Ordet $\bar{c} = 000111$ tillhör koden eftersom summan av de tre sista kolonnerna i H är lika med nollkolonnen, eller ekvivalent:

$$H \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

(c) Går ordet 111001 att rätta.

Lösning: Då

$$H \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix},$$

vilket är den första kolonnen i matrisen H så gäller att om ändrar vi ettan i ordets första position till en nolla får vi ordet 011001 och

$$H \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix},$$

dvs ordet 011001 tillhör C och ligger på avståndet ett från det givna ordet.

SVAR: Ordet 111001 kunde rättas till ordet 011001.

5. (3p) Den planära sammanhängande grafen G har nio noder varav en har valensen (degree) två, en har valensen tre, en har valensen fem och resterande sex noder har valensen fyra. Bestäm antalet områden som uppstår när grafen ritas plant.

Lösning: Vi bestämmer först antalet kanter med hjälp av sambandet $\sum_{v \in V} \delta(v) = 2|E|$, där V och E betecknar mängden av noder respektive kanter och $\delta(v)$ betecknar valensen hos noden v. Vi får alltså att

$$2|E| = 2 + 3 + 5 + 6 \cdot 4 = 34,$$

så antalet kanter är 17. Nu använder vi Eulers formel $v + r = e + 2$ för planära grafer där v, r och e betecknar antalet noder, områden resp kanter som uppstår vid en plan ritning av en planär graf:

$$r = e + 2 - v = 17 + 2 - 9 = 10.$$

SVAR: Antalet områden är 10.

DEL II

6. (3p) Visa att $4^n - 3n - 1$ är delbart med talet 9 för alla naturliga tal $n \geq 2$.

   Lösning: Påståendet sant för $n = 2$ ty $4^2 - 3 \cdot 2 - 1 = 9$ som ju uppenbarligen är delbart med nio.
   Vi visar nu att implikationen

   $$9 \mid 4^n - 3n - 1 \qquad \Longrightarrow \qquad 9 \mid 4^{n+1} - 3(n+1) - 1$$

   är giltig för alla naturliga tal $n \geq 2$. Vi finner att

   $$4^{n+1} - 3(n+1) - 1 = 4 \cdot 4^n - 3(n+1) - 1,$$

   som om $4^n - 3n - 1 = 9k$ ger att

   $$4^{n+1} - 3(n+1) - 1 = 4 \cdot 4^n - 3(n+1) - 1 = 4(9k + 3n + 1) - 3(n+1) - 1 = 36k + 9n = 9(4k + n),$$

   dvs att $4^{n+1} - 3(n+1) - 1$ är delbart med 9.
   Enligt induktionsprincipen är nu $4^n - 3n - 1$ är delbart med talet 9 för alla naturliga tal $n \geq 2$.

7. (5p) Man skall utse precis nio personer ur de tre mängderna $\mathcal{A} = \{A_1, A_2, \ldots, A_6\}, \mathcal{B} = \{B_1, B_2, \ldots, B_6\}$ och $\mathcal{C} = \{C_1, C_2, \ldots, C_6\}$. (Mängderna är disjunkta så ingen person finns med i fler än i en av mängderna $\mathcal{A}$, $\mathcal{B}$ och $\mathcal{C}$.) På hur många sätt kan detta ske om

   (a) (1p) Inga restriktioner finns.

   Lösning: Av totalt 18 personer skall nio väljas Antalet sätt detta kan ske på är vårt
   SVAR:

   $$\binom{18}{9}.$$

   (b) (2p) Minst en person från varje mängd skall finnas med i urvalet.

   Lösning: Vi använder oss av inklusion exklusion och låter A beteckna de urval där ingen från $\mathcal{A}$ kommer med, B beteckna de urval där ingen från $\mathcal{B}$ kommer med och C beteckna de urval där ingen från $\mathcal{C}$ kommer med. Svaret ges då av

   $$\binom{18}{9} - |A \cup B \cup C|,$$

   där formeln för inklusion exklusion ger att

   $$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|.$$

   Man ser omdelbart att $A \cap B = A \cap C = B \cap C = A \cap B \cap C = \emptyset$ och att

   $$|A| = |B| = |C| = \binom{12}{9}.$$

   Således får vi
   SVAR

   $$\binom{18}{9} - 3\binom{12}{9}.$$

(c) (2p) Precis tre personer från varje mängd skall ingå och högst en person från mängden $\{A_1, B_1, C_1\}$ får finnas med bland de nio utvalda personerna.

Lösning: Vi gör en indelning i fall:
Fall 1: Ingen av A_1, B_1, C_1 ingår och vi väljer tre av de övriga fem i varje grupp vilket går på

$$\binom{5}{3}^3,$$

olika sätt.
Fall 2: Precis en av A_1, B_1, C_1 ingår. Först väljer vi vilken sen utser vi de övriga vilket enligt multiplikationsprincipen går på

$$\binom{3}{1} \cdot \binom{5}{2} \cdot \binom{5}{3} \cdot \binom{5}{3}$$

olika sätt. Summerar vi antalet möjligheter får vi
SVAR:

$$\binom{5}{3}^3 + \binom{3}{1} \cdot \binom{5}{2} \cdot \binom{5}{3} \cdot \binom{5}{3}.$$

8. (4p) Låt $\mathcal{S}_5$ beteckna mängden av permutationer på en mängd med fem element. Bestäm en delgrupp till $\mathcal{S}_5$ med 12 element.

Lösning: Vi använder att mängden av jämna permutationer i gruppen $\mathcal{S}_4$ bildar en delgrupp $\mathcal{A}_4$ till $\mathcal{S}_4$ och att denna delgrupp $\mathcal{A}_4$ innehåller precis 12 element. Vidare kan vi uppfatta $\mathcal{S}_4$ some en delgrupp till $\mathcal{S}_5$, nämlgen de permutationer φ i $\mathcal{S}_5$ för vilka elementet 5 fixeras, dvs $\varphi(5) = 5$.

SVAR De permutationer $\varphi \in \mathcal{S}_4$ som är jämna och sådana att $\varphi(5) = 5$.

Anm. Det finns givetvis många andra delgrupper till $\mathcal{S}_5$ som har 12 element.

DEL III

Om du i denna del använder eller hänvisar till satser från läroboken skall dessa citeras, ej nödvändigvis ordagrant, där de används i beviset.

9. En felkorrigerande kod C säges vara linjär om för varja par av ord c och c' som finns i C också deras skillnad $c - c'$ tillhör C. Till varje linjär kod C finns en kontrollmatris H sådan att $C = \{c \mid Hc^T = 0\}$ och omvänt är är varje kod som definieras på detta sätt med hjälp av en kontrollmatris en linjär kod. (Detta är information inför upppgifterna (a) och (b) nedan och du behöver inte visa att denna information är sann.)

   (a) (2p) Visa att det inte finns någon 1-felsrättande linjär kod C med 32 ord och som innehåller de tre orden

   $$c_1 = 111100000, \quad c_2 = 011001100, \quad c_3 = 100101010.$$

   Lösning: Då C är linjär så kommer varje linjärkombination

   $$\lambda_1 c_1 + \lambda_2 c_2 + \lambda_3 c_3$$

   att tillhöra C. T ex kommer ordet

   $$c_1 + c_2 + c_3 = 000000110,$$

   att tillhöra C. Men eftersom nollordet tillhör C och ordet ovan har avstånd två till nollordet så skulle inte koden vara 1-felsrättande om detta ord tillhörde C.

(b) (2p) Undersök om en sådan kod C kan finnas om bara två av de tre givna orden ovan skall finnas med bland de 32 orden i C.

Lösning: Vi konstruerar en kontrollmatris H med 4 rader och 9 kolonner. Den 1-felsrättande kod C som denna matris då definierar kommer att ha $2^{9-4} = 32$ stycken ord. Matrisen H kommer att bestå av nio olika kolonner. Ordet c_1 finns med i C precis då summan av de fyra första kolonnerna blir noll, och en motsvarande reltion mellan andra kolonner skall gälla för att ordet c_2 skall finnas med i C. Lite trial and error ger följande matris (observera att matrisens kolonner också måste vara olika):

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

V hittade en kontrollmatris som ger en 1-felsrättande kod med 32 ord och som innehåller orden c_1 och c_2. Så svaret är JA.

10. För grupper G_1 och G_2 med gruppoperationerna $\circ_1$ respektive $\circ_2$ så definieras den direkta produkten av dessa grupper som mängden

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, \quad g_2 \in G_2\}$$

med gruppoperationen $\circ$ definierad av

$$(g_1, g_2) \circ (h_1, h_2) = (g_1 \circ_1 h_1, g_2 \circ_2 h_2).$$

(a) (2p) Under vilka förutsättningar gäller att om $G_1 \times G_2$ är en ändlig cyklisk grupp så är både G_1 och G_2 cykliska grupper.

Lösning: (Vi skriver $g_1 \circ_1 h_1 = g_1 h_1$ och $g_2 \circ_2 h_2 = g_2 h_2$.) Vi visar att om $G_1 \times G_2$ är cyklisk så är både G_1 och G_2 cykliska. Antag att $G_1 \times G_2$ är cyklisk och låt (g, h) vara en generator till $G_1 \times G_2$. Låt x och y vara godtyckliga element i G_1 resp G_2. Då gäller att $(x, y) \in G_1 \times G_2$ och alltså, eftersom (g, h) genererar $G_1 \times G_2$, att för något tal k

$$(x, y) = (g, h)^k = (g^k, h^k),$$

vilket ger att $x = g^k$ och $y = h^k$. Varje element x i G_1 är alltså en potens $x = g^k$ av g och varje element y i G_2 är en potens $y = h^k$ av h, dvs G_1 är cyklisk med generator g och G_2 cyklisk med generator G_2.

(b) (3p) Under vilka förutsättningar gäller att om G_1 och G_2 är ändliga cykliska grupper så är $G_1 \times G_2$ en cyklisk grupp.

Lösning: Vi visar att $G_1 \times G_2$ är en cyklisk grupp precis då antalet element i G_1 och G_2 är relativt prima. Enligt förutsättningarna är G_1 cyklisk med en generator g och ordningen av g är lika med $n = |G_1|$, och G_2 cyklisk med en generator h och ordningen av h är lika med $m = |G_1|$.
Vi kommer att använda följande sats

Sats. *Låt g vara ett element i en grupp G och antag att ordningen av g är k. Då gäller att om $g^t = e$ så måste k delat talet t.*

Bevis. Om $g^t = e$ och vi delar t med k får vi en rest r som är mindre än k: $t = d \cdot k + r$, och då skulle vi ha

$$e = g^t = g^{d \cdot k + r} = (g^k)^d \cdot g^r = e^d \cdot g^r = g^r,$$

men $r < k$ och detta strider mot att ordningen av g var k, dvs k är det minsta tal sådant att $g^k = e$.

Antag $sgd(n, m) = 1$. Vi visar att då är ordningen av $(g, h) = n \cdot m$.
Om $(g, h)^k = (e, e)$ så gäller att $g^k = e$ och $h^k = e$. Enligt satsen måste då n dela k och m dela k och alltså att $mgm(n, m)$ delar k. Eftersom talen n och m är relativt prima så gäller att $mgm(n, m) = nm$ och alltså att $n \cdot m$ delar k.
Vi ser också att

$$(g, h)^{nm} = ((g^n)^m, (h^m)^n) = (e^m, e^n) = (e, e).$$

Det minsta heltal k sådant att $(g, h)^k = (e, e)$ är alltså $k = nm$. Alltså gäller att elementet (g, h) har ordning $n \cdot m$ om $sgd(n, m) = 1$ och att $G_1 \times G_2$ genereras av (g, h) (eftersom $G_1 \times G_2$ har nm stycken element.)
Antag nu att $sgd(n, m) = D \neq 1$. Då gäller för varje element (g, h) i gruppen $G_1 \times G_2$ att $(g, h)^{nm/D} = (e, e)$, ty om talet D delar både n och m så har vi att

$$(g, h)^{nm/D} = (g^{n \cdot \frac{m}{D}}, g^{m \cdot \frac{n}{D}}) = (e^{\frac{m}{D}}, e^{\frac{n}{D}}) = (e, e).$$

Inget element i $G_1 \times G_2$ kan alltså ha ordning nm, och $G_1 \times G_2$ kan då ej vara cyklisk.