Matematiska Institutionen
KTH

Lösning till tentamensskrivning i Diskret Matematik för CINTE, CL2 och Media 1, SF1610 och 5B1118, tisdagen den 21 oktober 2008, kl 08.00-13.00.

Examinator: Olof Heden.

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

Betygsgränser: (Totalsumma poäng är 36p.)

12	poäng totalt eller mer ger minst omdömet	Fx
15	poäng totalt eller mer ger minst betyget	E
18	poäng totalt eller mer ger minst betyget	D
22	poäng totalt eller mer ger minst betyget	C
28	poäng totalt eller mer ger minst betyget	B
32	poäng totalt eller mer ger minst betyget	A

Generellt gäller att för full poäng krävs korrekta och väl presenterade resonemang.

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) Lös ekvationen $14x = 17$ i ringen Z_{27}.

   Lösning: I ringen Z_{27} gäller att $2 \cdot 14 = 1$ eftersom $2 \cdot 14 = 28 \equiv 1 \pmod{27}$. Så multiplicera bägge leden i ekvationen med 2 och vi får, emedan $2 \cdot 17 = 34 \equiv 7 \pmod{27}$, att

   $$14x = 17 \quad \Leftrightarrow \quad 2 \cdot 14x = 2 \cdot 17 \quad \Leftrightarrow \quad x = 7.$$

   Svar $x = 7$.

2. (3p) En skola med 30 flickor, 40 pojkar och 10 lärare skall utse en arbetsgrupp bestående av fyra pojkar, fyra flickor och tre lärare. På hur många sätt kan detta ske om lärana herr A och fru B inte kan vara med i samma arbetsgrupp.

   Lösning: De fyra flickorna kan väljas på $\binom{30}{4}$ olika sätt, de fyra pojkarna kan väljas på $\binom{40}{4}$ olika sätt och tre lärare kan väljas på $\binom{10}{3}$ olika sätt. Vissa lärarkombinationer får ju inte förekomma. Antalet otillåtna lärarkombinationer ges av de kombinationer när herr A och fru B båda ingår i gruppen och en övrig lärare väljs bland de åtta resterande lärarna vilket kan göras på $\binom{8}{1}$ olika sätt. Antalet sätt att välja lärarna på är alltså $\binom{10}{3} - \binom{8}{1}$.

   Multiplikationsprincipen ger nu vårt

   Svar $\binom{30}{4}\binom{40}{4}(\binom{10}{3} - \binom{8}{1})$.

3. (3p) Vilket är det minsta antal element en grupp G måste ha om G skall ha en delgrupp H_1 med 2 element, en delgrupp H_2 med 4 element och en delgrupp H_3 med 5 element. Ge också ett exempel på en sådan grupp G.

   Lösning: Enligt Lagranges sats delar antalet element i en delgrupp H till en grupp G antalet element i gruppen G dvs
   $$|H| \mid |G|.$$
   Antalet element i G måste alltså delas av talen 2, 4, och 5, dvs
   $$20 \mid |G|.$$
   Med $G = (Z_{20}, +)$ har vi en grupp med 20 element, (som har delgrupperna
   $$H_1 = \{0, 10\}, \qquad H_2 = \{0, 5, 10, 15\}, \qquad H_3 = \{0, 4, 8, 12, 16\}).$$

   Svar Minsta antalet element är 20 och $(Z_{20}, +)$ är exempel på en grupp med de givna egenskaperna.

4. (3p) Konstruera ett RSA-krypto, dvs ange parametrar n, e och d. Dekryptera därefter meddelandet 2, dvs bestäm $D(2)$.

   Lösning: Vi låter $n = 3 \cdot 5$, ty kravet på n är att n skall vara en produkt av olika primtal. Då blir $m = (3-1)(5-1) = 8$. Av e och d krävs att $e \cdot d = 1$ i ringen Z_m, och vi kan välja $e = 3$ och $d = 3$. Regeln för dekryptering ger att
   $$D(2) = 2^d \pmod n = 2^3 \pmod{15} = 8.$$

   Svar Till exempel $n = 15$, $e = 3$, $d = 3$ och $D(2) = 8$.

5. (3p) För vilka värden på talet n har den kompletta grafen K_n en Eulerkrets.

   Lösning: En graf G har en Eulerkrets precis då G är sammanhängande och alla noder i G har en jämn valens. Den kompletta grafen K_n är sammanhängande och det går en kant från var och en av de n noderna till grafens övriga $n-1$ noder. Detta ger att valensen hos varje nod i K_n är $n-1$. Så precis när talet $n-1$ är ett jämnt tal så har K_n en Eulerkrets.

   Svar Svar när n är ett udda tal.

DEL II

6. (3p) Visa att det inte finns något träd med 30 noder varav tretton noder har valens 1, tolv noder har valens 2 och fem noder har valens 3.

   Lösning: Vi beräknar först antalet kanter $|E|$ i grafen genom att beräkna summan av alla valenser och sedan dela med två.
   $$|E| = \frac{1}{2}(13 \cdot 1 + 12 \cdot 2 + 5 \cdot 3) = \frac{1}{2}52 = 26.$$
   I varje träd gäller att antalet kanter är ett mindre än antalet noder. Det kan alltså inte finnas något träd med 30 noder och 26 kanter och vårt bevis är klart.

7. Låt $\varphi = (1\ 2\ 3\ 4\ 5\ 6)$ och $\psi = (7\ 8\ 9\ 10)$ vara permutationer av elementen i mängden $\{1, 2, 3, \ldots, 10\}$

(a) (1p) Bestäm två naturliga tal n och m sådana att permutationen $\varphi^n\psi^m$ har ordning 3.

Lösning: Vi minns att ordningen av en permutation är minsta gemensamma multipeln av längden av permutationens cykler, under förutsättning att cyklerna är disjunkta, (inte innehåller några gemensamma element).

Vi observerar först att

$$\varphi^2 = (1\ 3\ 5)(2\ 4\ 6) \qquad \text{och} \qquad \psi^4 = id.$$

Då φ^2 är en produkt av två 3-cykler så har φ^2 ordning 3. Permutationen ψ^4 har ordning 1.

Alltså gäller att permutation $\varphi^2\psi^4$ har ordning 3.

Svar Till exempel $n = 2$ och $m = 4$.

(b) (2p) Bestäm samtliga naturliga tal n och m sådana att permutationen $\varphi^n\psi^m$ har ordning 6.

Lösning: Vi använder att en permutations ordning är minsta gemensamma multiplen av längderna av de cykler som uppstår när man skriver permuationen som en produkt av disjunkta cykler.

Vi listar upp de olika cykler som uppstår hos φ^n och ψ^m för olika värden på n och m:

$$\begin{array}{lllll} n \equiv 0 \pmod 6 & \Rightarrow & \varphi^n = (1)(2)(3)(4)(5)(6) \\ n \equiv 1 \pmod 6 & \Rightarrow & \varphi^n = (1\ 2\ 3\ 4\ 5\ 6) \\ n \equiv 2 \pmod 6 & \Rightarrow & \varphi^n = (1\ 3\ 5)(2\ 4\ 6) \\ n \equiv 3 \pmod 6 & \Rightarrow & \varphi^n = (1\ 4)(2\ 5)(3\ 6) \\ n \equiv 4 \pmod 6 & \Rightarrow & \varphi^n = (1\ 5\ 3)(2\ 6\ 4) \\ n \equiv 5 \pmod 6 & \Rightarrow & \varphi^n = (1\ 6\ 5\ 4\ 3\ 2) \end{array},$$

resp

$$\begin{array}{lllll} m \equiv 0 \pmod 4 & \Rightarrow & \psi^m = (7)(8)(9)(10) \\ m \equiv 1 \pmod 4 & \Rightarrow & \psi^m = (7\ 8\ 9\ 10) \\ m \equiv 2 \pmod 4 & \Rightarrow & \psi^m = (7\ 9)(8\ 10) \\ m \equiv 3 \pmod 4 & \Rightarrow & \psi^m = (7\ 10\ 9\ 8) \end{array}.$$

Vi ser att minsta gemensamma multiplen hos längderna hos de disjunkta cyklerna av $\varphi^n\psi^m$ blir 6 när

Fall 1: $n \equiv 1 \pmod 6$ eller $n \equiv 5 \pmod 6$ och $m \equiv 2 \pmod 4$ eller $m \equiv 0 \pmod 4$.

eller

Fall 2: $n \equiv 2 \pmod 6$ eller $n \equiv 4 \pmod 6$ och $m \equiv 2 \pmod 4$.

Detta kan också sammanfattas i ett

Svar Om $m \equiv 2 \pmod 4$ och n ger någon av resterna 1, 2, 4 eller 5 vid division med 6, eller om m är delbart med 4 så skall $n \equiv 1 \pmod 6$ eller $n \equiv 5 \pmod 6$.

(c) (1p) Beskriv samtliga naturliga tal n och m sådana att permutationen $\varphi^n\psi^m$ är en jämmn permutation.

Lösning: En produkt av två permutationer $\gamma = \varphi^n$ och $\delta = \psi^m$ är en jämn permutation om och endast om antingen både γ och δ är jämna permutationer eller båda är udda permutationer.

Eftersom φ är en cykel av jämn längd så är φ en udda permutation och likadant för ψ. Så för att $\varphi^n\psi^m$ skall vara en jämmn permutation krävs att antingen är båda talen n och m udda tal eller så är både n och m jämna tal, eller ekvivalent

Svar $n \equiv m \pmod 2$.

8. (4p) Låt $n = 2^5 3^{10} 5^8$ och låt $m = 8000 \cdot 1377$. Bestäm antalet positiva heltal q som delar både n och m.

Lösning: Vi söker gemensamma primfaktorer till talen n och m, och eftersom vi vet primfaktoriseringen av n är detta inte något större bekymmer. Vi får med räkningar exempelvis som nedan, primfaktoriseringen av m till

$$m = 8000 \cdot 1377 = 16 \cdot 500 \cdot 9 \cdot 153 = 16 \cdot 4 \cdot 125 \cdot 9 \cdot 9 \cdot 17 = 2^6 \cdot 5^3 \cdot 3^4 \cdot 17.$$

Från talens primfaktorisering ser vi att den största gemensamma delaren till talen n och m är

$$D = 2^5 \cdot 3^4 \cdot 5^3.$$

Alla gemensamma delare till n och m delar den största gemensamma delaren D och alla delare till den största gemnsamma delaren D delar både n och m. Vidare har vi att

$$d \mid D \qquad \Longleftrightarrow \qquad d = 2^a \cdot 3^b \cdot 5^c \quad \text{där} \quad 0 \le a \le 5, \;\; 0 \le b \le 4, \;\; 0 \le c \le 3.$$

Det finns alltså 6 olika användbara val av talet a, 5 val av b och 4 val av talet c. Totalt enligt multiplikationsprincipen

Svar Totalt $6 \cdot 5 \cdot 4 = 120$ olika positiva gemensamma delare.

DEL III

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

9. Låt C vara en 1-felsrättande kod som erhålles på sedvanligt sätt ur en kontrollmatris H. Koden C innehåller bland annat orden 11111100000 och 11100001100.

   (a) (1p) Bestäm det största antalet ord koden C kan ha.

   Lösning: Ordlängden är lika med 11, så antalet kolonner i kodens kontrollmatris H är 11. Antal ord koden har är 2^{11-m} där m är antalet rader i H. Så flest ord får vi när vi har ett minimalt antal rader. För att H skall vara en kontrollmtaris till en 1-felsrättande kod måste matrisens kolonner vara olika och ingen kolonn får vara lika med nollkolonnen. Det finns bara sju olika möjliga sådana kolonner om antalet rader är tre, men med fyra rader kan vi välja bland 15 olika kolonner som inte är nollkolonnen. Dessutom skall gälla, eftersom de givna orden skall tillhöra koden, att

   $$H(1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0)^T = (0\,0\,0\,0)^T \quad \text{och} \quad H(1\,1\,1\,0\,0\,0\,0\,1\,1\,0\,0)^T = (0\,0\,0\,0)^T,$$

   dvs summan av de sex första kolonnerna skall vara nollkolonnen och summan av de tre första kolonnerna och kolonn 8 och 9 skall vara nollkolonnen. Lite trial and error ger matrisen

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

   som uppfyller alla de givna kraven.

   Svar Maximalt antal ord är $2^{11-4} = 2^7 = 128$.

   (b) (2p) Bestäm det minsta antalet ord koden C kan ha och beskriv samtliga koder C som har detta minsta antal ord.

   Lösning: Antalet ord i en kod med en kontrollmatris är 2^{n-m} där n är antalet kolonner och m antalet rader, dessutom så tillhör alltid nollordet C eftersom $H\bar{0}^T = \bar{0}^T$ får alla kontrollmatriser

H. Om koden innehåller de givna två orden samt nollordet så måste koden innehålla minst fyra ord, och motsvarande kontrollmatris precis $m = 9$ rader. Vi bygger nu ut matrisen ovan med ytterligare fem rader:

$$H = \left[\begin{array}{cccccccccc|c} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right],$$

så att de givna orden fortfarande tillhör koden. (Egentligen krävs också att ingen icketrivial linjärkombination av raderna blir nollraden, vilket ju matrisen ovan uppfyller.)

Svar Fyra ord.

(c) (2p) För vilka tal k finns en kod C med k stycken ord och som uppfyller de givna förutsättningarna ovan.

Lösning: Eftersom koden skall gå att beskriva med hjälp av en kontrollmatris kommer antalet ord att var en potens av två, 2^{n-m}, där n är antalet kolonner och m antalet rader. Om vi i kontrollmatrisen H ovan tar bort en godtycklig delmängd av de rader som är under linjen får vi en kontrollmatris som uppfyller alla förutsättningar. Antalet ord i koden blir då 2^{11-r} där r är antalet kvarvarande rader i H (inklusive de ovanför linjen). Antalet möjliga ord i koden är alltså, med olika val av r,

Svar 4 ($r = 9$), 8 ($r = 8$), 16 ($r = 7$), 32 ($r = 6$), 64 ($r = 5$) eller 128 ($r = 4$).

10. Låt $\mathcal{F}(A, B)$ beteckna mängden av alla funktioner från mängden A till mängden B, och låt $\mathcal{S}(A, B)$ beteckna mängden av alla surjektioner av A på B. Låt $n = |A|$ och $m = |B|$.

(a) (1p) Det finns precis ett värde på m för vilket $\mathcal{F}(A, B) = \mathcal{S}(A, B)$ för alla mängder A. Bestäm detta värde på m.

Lösning: Om B bara innehåller ett element som måste detta vara det enda funktionsvärdet och alla element i B kommer att vara ett funktionsvärde. Då är alla funktioner också surjektioner.

Svar $m = 1$

(b) (1p) Bestäm kvoten

$$\frac{|\mathcal{S}(\{1,2,3,4\},\{a,b\})|}{|\mathcal{F}(\{1,2,3,4\},\{a,b\})|}$$

Lösning: Antalet funktioner från A till B kommer att vara $2^4 = 16$ eftersom det till vart och ett av de fyra elmenten i definitionsmängden A finns två möjliga funktionsvärden a eller b. Alltså gäller att

$$|\mathcal{F}(\{1,2,3,4\},\{a,b\})| = 2^4.$$

Om en funktion till den givna mängden B inte är en surjektion så kommer antingen alla funktionsvärden att vara a eller alla funktionsvärden att vara b. Det är alltså precis två funktioner som inte är surjektioner, och därmed

$$|\mathcal{S}(\{1,2,3,4\},\{a,b\})| = 2^4 - 2.$$

Svar $(16 - 2)/16$ dvs $7/8$.

(c) (3p) Undersök om det till varje värde på talet m finns ett tal n sådant att

$$\frac{|\mathcal{S}(A,B)|}{|\mathcal{F}(A,B)|} \geq \frac{1}{2}.$$

Lösning: Idén är att visa att för varje naturligt tal m finns ett tal n sådant att mindre än hälften av alla funktioner från A till B *inte* är surjektioner.

Låt $B = \{b_1, b_2, \ldots, b_m\}$ och låt A_i vara mängden av funktioner för vilka b_i inte är ett funktionsvärde:

$$A_i = \{f \in \mathcal{F}(A,B) \mid f(x) \neq b_i \quad \text{för alla} \quad x \in A\}.$$

Då gäller att mängden av funktioner som inte är surjektioner finns i unionen av mängderna A_1, A_2, ..., A_m och alltså att

$$\mathcal{S}(A,B) = \mathcal{F}(A,B) \setminus (A_1 \cup A_2 \cup \ldots \cup A_m).$$

Men

$$|A_1 \cup A_2 \cup \ldots \cup A_m| \leq |A_1| + |A_2| + \ldots + |A_m|$$

och för varje $1 \leq i \leq m$ gäller att

$$|A_i| = (m-1)^n,$$

eftersom mängden A_i består av samtliga funktioner från mängden A, som har n element, till mängden $B \setminus \{b_i\}$, med $m-1$ element. Detta ger nu att

$$\frac{|\mathcal{S}(A,B)|}{|\mathcal{F}(A,B)|} = \frac{|\mathcal{F}(A,B) \setminus (A_1 \cup A_2 \cup \ldots \cup A_m)|}{|\mathcal{F}(A,B)|} \geq \frac{m^n - m \cdot (m-1)^n}{m^n} = 1 - m \cdot (1 - \frac{1}{m})^n.$$

Men talet $(1-1/m)$ är strikt mindre än talet 1 och då gäller att $(1-1/m)^n$ kan bli hur litet som helst bara n är tillräckligt stort, och så litet så att $(1-1/m)^n \leq \frac{1}{2m}$ och därmed

$$1 - m \cdot (1 - \frac{1}{m})^n \geq 1 - \frac{m}{2m} = \frac{1}{2}$$

(*Detta resonemang räcker för full poäng*).

Svar Ja, i varje fall om $n \geq (\ln 2 + \ln m)/(\ln m - \ln (m-1))$ så kommer den givna kvoten att var minst $1/2$.