Matematiska Institutionen
KTH

**Lösning av tentamensskrivning i Diskret Matematik för CINTE och CMETE, SF1610, tisdagen den 27 maj 2014, kl 14.00-19.00.**

**Examinator:** Olof Heden

**Hjälpmedel:** Inga hjälpmedel är tillåtna på tentamensskrivningen.

**Betygsgränser:** (**OBS:** Totalsumma poäng vid denna tentamensskrivning är 36p.)

| | | |
|---|---|---|
| 13 | 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 |

**Observera:** 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) Bestäm samtliga lösningar i ringen $Z_{102}$ till ekvationen

$$43x + 37 = 50.$$

**Lösning.** Eftersom $\text{sgd}(102, 43) = 1$ så är elementet 43 inverterbart i ringen $Z_{102}$ och lösningen till ekvationen ges av

$$x = 43^{-1}(50 - 37).$$

Vi söker inversen till 43 m hj a Euklides algoritm:

$$102 = 2 \cdot 43 + 16, \qquad 43 = 3 \cdot 16 - 5, \qquad 16 = 3 \cdot 5 + 1,$$

vilket ger

$$1 = 16 - 3 \cdot 5 = 16 - 3(3 \cdot 16 - 43) = -8 \cdot 16 + 3 \cdot 43 = -8(102 - 2 \cdot 43) + 3 \cdot 43 = 19 \cdot 43 - 8 \cdot 102,$$

så $19 \cdot 43 \equiv 1 (\text{mod } 102)$. Vi får alltså, med räkningar i ringen $Z_{102}$

$$x = 19 \cdot 13 = \{19 \cdot 13 = 247 = 2 \cdot 102 + 43\} = 43$$

**SVAR:** 43.

2. (a) (1p) Tio indetiska objekt skall placeras i fem etiketterade lådor. På hur många olka sätt kan objekten fördelas i lådorna, om vi tillåter att lådor blir tomma? Svaret skall ges i formen av ett heltal.

**Lösning.** Enligt känd formel

$$\binom{10+5-1}{5-1} = \frac{14 \cdot 13 \cdot 12 \cdot 11}{1 \cdot 2 \cdot 3 \cdot 4} = 7 \cdot 13 \cdot 11 = 91 \cdot 11 = 1001$$

**SVAR:** 1001.

(b) (1p) Tio olika objekt skall placeras i fem etiketterade lådor med två objekt i varje låda. På hur många olika sätt kan detta ske? Svaret skall ges i formen av ett heltal.

**Lösning.** Enligt känd formel

$$\binom{10}{2,2,2,2,2} = \frac{10 \cdot 9 \cdot \dots \cdot 2 \cdot 1}{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2} = 10 \cdot 9 \cdot 7 \cdot 6 \cdot 5 \cdot 3 \cdot 2 = 10 \cdot 81 \cdot 7 \cdot 20 = 10 \cdot 567 \cdot 20 = 113400.$$

**SVAR:** 113400.

(c) (1p) Tio olika objekt skall placeras i fem oetiketterade lådor med två objekt i varje låda. På hur många olika sätt kan detta ske? Svaret skall ges i formen av ett heltal.

**Lösning.** Antag svaret på frågan är $x$. Eftersom det finns 5! sätt att etikettera fem oetiketterade lådor får vi från föregående deluppgift att

$$x = \frac{1}{5!} \cdot \binom{10}{2,2,2,2,2} = \frac{10 \cdot 9 \cdot 7 \cdot 6 \cdot 5 \cdot 3 \cdot 2}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 5 \cdot 9 \cdot 7 \cdot 3 = 45 \cdot 21 = 945.$$

**SVAR:** 945.

3. (3p) Gruppen $G$ har en delgrupp $H$ med 7 element och en delgrupp $K$ med 5 element samt eventuellt också delgrupper av andra storlekar. Förklara varför antalet sidoklasser i $G$ till delgruppen $K$ är delbart med 7.

**Lösning.** Enligt Lagranges sats så gäller att antal element i gruppen $G$ delas av antalet element i sina delgrupper. Vi har alltså att $5 \mid |G|$ och $7 \mid |G|$ och därmed att

$$|G| = k \cdot 35.$$

Vet vidare också att sidoklasserna till en delgrupp $K$ partitionerar $G$ i lika stora parvis disjunkta delmängder. Så om $t$ är antalet sidoklasser får vi likheten

$$t \cdot |K| = |G| = k \cdot 35$$

Då $|K| = 5$ får vi $t = 7k$, vilket skulle visas.

4. (a) (2p) Bestäm kontrollmatrisen (parity-checkmatrisen) till en 1-felsrättande kod $C$ med 256 ord av minsta möjliga längd $n$.

**Lösning.** Antal ord i koden är $2^{n-r}$ där $r$ är antalet rader i den sökta kontrollmatrisen $\mathbf{H}$ och $n$ antalet kolonner i $\mathbf{H}$. Talet $n$ är också ordlängden. Antalet ord är 256 ger då att $n - r = 8$. Men villkoret att kontrollmatrisens kolonner är olika, och skilda från nollkolonnen ger då att $r > 3$, ty om $r = 3$ skulle $n = 11$ men det finns i så fall bara 7 möjliga kolonner att placera i matrisen $\mathbf{H}$. Minsta möjliga $n$ fås då när $n = 12$. T ex kan vi låta

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

(b) (1p) Bestäm antalet ord av längd $n$ som inte tillhör koden $C$ ovan och ej heller kan rättas till ett ord i $C$.

**Lösning.** Ord på avstånd ett från kodord kan rättas. Det finns 12 ord på avstånd ett från varje kodord. Totala antalet ord som ligger på avstånd ett från ett kodord är eller är ett kodord är då

$$2^8 \cdot 12 + 2^8,$$

eftersom varje ord ligger på avstånd ett eller mindre från högst ett kodord. Totalt finns $2^{12}$ ord av längd 12 så

**SVAR:** $2^{12} - 13 \cdot 2^8$, dvs 768.

5. (3p) I den planära och sammanhängande grafen $G$ har alla noder valensen 3. Antalet kanter (inklusive eventuella multipelkanter) är 186. Bestäm antalet områden, ytterområdet medräknat, som uppstår vid en plan ritning av grafen.

**Lösning.** Vi kommer att använda Eulers formel $r = e + 2 - v$ för sammanhängande planära grafer, där $r$ betecknar antalet områden som bildas vid en plan ritning, $e$ antalet kanter och $v$ antalet noder. Sambandet mellan nodernas valenser och antalet kanter ger

$$3v = 2 \cdot 186.$$

Alltså $v = 124$. Då $186 + 2 - 124 = 64$ så

**SVAR:** Antalet områden är 64.

**DEL II**

6. (3p) Den oändliga talföljden $a_0$, $a_1$, ... definieras rekursivt genom sambandet

$$a_n = -a_{n-1} + 4a_{n-2} + 4a_{n-3}\,, \qquad \text{för} \qquad n = 3, 4, \ldots$$

samt av att $a_0 = 3$, $a_1 = -1$ och $a_2 = 9$. Visa med ett induktionsbevis att

$$a_n = (-1)^n + 2^n + (-2)^n$$

för $n = 0, 1, 2, 3, \ldots$ .

**Lösning.** Sätt $b_n = (-1)^n + 2^n + (-2)^n$. Vi skall visa att $a_n = b_n$ för $n = 0, 1, 2, \ldots$.
Vi konstaterar först att

$$b_0 = 1 + 1 + 1 = a_0 \qquad , b_1 = -1 + 2 - 2 = a_1 \text{och} \qquad b_2 = 1 + 4 + 4 = a_2.$$

Återstår att verifiera det så kallade induktionssteget, dvs implikationen

$$\left\{ \begin{array}{lcl} a_{n-3} & = & b_{n-3} \\ a_{n-2} & = & b_{n-2} \\ a_{n-1} & = & b_{n-1} \end{array} \right. \qquad \Longrightarrow \qquad a_n = b_n.$$

Vi får nu

$$a_n = -a_{n-1} + 4a_{n-2} + 4a_{n-3} = \{\text{om } a_{n-1} = b_{n-1}, a_{n-2} = b_{n-2} \text{ och } a_{n-3} = b_{n-3}\} =$$
$$= -b_{n-1} + 4b_{n-2} + 4b_{n-3} =$$
$$= -((-1)^{n-1} + 2^{n-1} + (-2)^{n-1}) + 4((-1)^{n-2} + 2^{n-2} + (-2)^{n-2}) + 4((-1)^{n-3} + 2^{n-3} + (-2)^{n-3}) =$$
$$= (-1)^{n-3}(-1 - 4 + 4) + 2^{n-3}(-2^2 + 4 \cdot 2 + 4) + (-2)^{n-3}(-(-2)^2 + 4(-2) + 4) =$$
$$= (-1)^n + 8 \cdot 2^{n-3} + (-8)(-2)^{n-3} = (-1)^n + 2^n + (-2)^n = b_n$$

Induktionsprincipen ger nu att $a_n = b_n$ för $n = 0, 1, 2, \ldots$

7. (4p) Bestäm antalet Booleska funktioner $g$ i de fyra variablerna $x$, $y$, $z$ och $w$, dvs $g = g(x, y, z, w)$, som satisfierar bägge ekvationerna i ekvationssystemet

$$\left\{ \begin{array}{rcccl} (x+y)z & + & g(x,y,z,w) & = & 1 \\ (z + w\bar{z})\bar{y} & + & g(x,y,z,w) & = & 1 \end{array} \right.$$

**Lösning.** I de punkter där minst en av de Booleska funktionerna $(x+y)z$ och $(z+w\bar{z})\bar{y}$ tar värdet 0 måste $g$ ha värdet 1 för att satisfiera ekvationssystemet. I övriga punkter kan, eftersom $1 + g = 1$

i varje Boolesk algera, funktionen $g$ tilldelas godtyckligt värdet 0 eller 1. Vi söker allså de punkter där både $(x+y)z$ och $(z+w\bar{z})\bar{y}$ antar värdet 1. De är de enda punkter där produkten av dessa Booleska uttryck är lika med ett. Vi skriver produkten av uttrycken på en disjunktiv normalform:

$$(x+y)z\cdot(z+w\bar{z})\bar{y} = xzz\bar{y}+yzz\bar{y}+xzw\bar{z}y+yzw\bar{z}\bar{y} = xz\bar{y} = xz\bar{y}(w+\bar{w}) = x\bar{y}zw+x\bar{y}z\bar{w}.$$

De fundamentala konjunktionerna ovan tar värdet 1 i punkterna $(1,0,1,1)$ och $(1,0,1,0)$. Så, $2\cdot 2$ möjliga funktioner.

**SVAR:** Antalet lösningar till det givna systemet är 4.

8. (4p) Sju flickor och åtta pojkar skall delas in i fyra grupper. På hur många sätt kan detta ske om varje grupp skall innehålla minst en flicka, och exakt en grupp skall sakna pojkar. Svaret får ges som summor och produkter av hela tal, (och lösningen skall motiveras).

**Lösning.** Flickorna kan delas in i fyra icketomma grupper på $\mathrm{S}(7,4)$ olika sätt. Efter varje genomförd sådan uppdelning kan grupperna betraktas som etiketterade, namngivna av sina medlemmar. En av dessa grupper skall sakna pojkar. Det finns fyra val av en sådan grupp. Resterande tre grupper skall innehålla minst en pojke. Antalet uppdelningar av de åtta pojkarna i tre icketomma etiketterade delgrupper beräknas nog enklast med hjälp av inklusion exklusion, på sedvanligt sätt. Detta antal blir

$$3^8-3\cdot 2^8+3\cdot 1^8 = 81\cdot 81-3\cdot 256+3.$$

Så svaret fås av multiplikationsprincipen till

$$\mathrm{S}(7,4)\cdot 4\cdot(81\cdot 81-3\cdot 256+3).$$

För att beräkna Stirlingtalet $\mathrm{S}(7,4)$ använder vi rekursionen $\mathrm{S}(n,k)=\mathrm{S}(n-1,k-1)+k\mathrm{S}(n-1,k)$ och får

$$\mathrm{S}(7,4)=\mathrm{S}(6,3)+4\mathrm{S}(6,4),\quad \mathrm{S}(6,3)=\mathrm{S}(5,2)+3\mathrm{S}(5,3),\quad \mathrm{S}(6,4)=\mathrm{S}(5,3)+4\mathrm{S}(5,4).$$

Vidare

$$\mathrm{S}(5,3)=\mathrm{S}(4,2)+3\mathrm{S}(4,3),\qquad \mathrm{S}(5,2)=\mathrm{S}(4,1)+2\mathrm{S}(4,2)$$

Vi minns kanske att $\mathrm{S}(4,1)=1$, $\mathrm{S}(4,2)=7$ och att $\mathrm{S}(n,n-1)=\binom{n}{2}$, Så

$$\mathrm{S}(5,2)=1+2\cdot 7=15,\quad \mathrm{S}(5,3)=7+3\cdot 6=25,\quad \mathrm{S}(5,4)=10$$

och sen

$$\mathrm{S}(6,3)=15+3\cdot 25=90,\qquad \mathrm{S}(6,4)=25+4\cdot 10=65.$$

Tillslut

$$\mathrm{S}(7,4)=90+4\cdot 65=350.$$

**SVAR:** $350\cdot 4\cdot(81\cdot 81-3\cdot 256+3)$.

## 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. (a) (1p) Förklara varför mängden av element i en cyklisk grupp $G$ aldrig är en union av mängderna av element i en samling icketriviala delgrupper till $G$, dvs visa att

$$G \neq H_1\cup H_2\cup\ldots\cup H_k,$$

för varje uppsättning icketriviala delgrupper $H_1, H_2\ldots, H_k$ till $G$ om $G$ är en cyklisk grupp.

**Lösning.** Antag att elementet $g$ genererar $g$. Om

$$G = H_1\cup H_2\cup\ldots\cup H_k,$$

så $g \in H_i$ för någon av delgrupperna $H_i$, för $i = 1, 2, \ldots, k$. Men då gäller, eftersom $H_i$ är sluten m a p operationen i $H_i$, att

$$G = \langle g \rangle \subseteq H_i \subseteq G$$

varur $G = H_i$. Då är $H_i$ ingen icketrivial delgrupp till $G$.

(b) (2p) Bevisa att ingen grupp $G$ är en union av två icketriviala delgrupper $H_1$ och $H_2$ till $G$.

**Lösning.** Antag att $G = H_1 \cup H_2$. Om $H_2 \subseteq H_1$ så $H_1 \cup H_2 = H_1$. Vi kan anta att $H_2$ inte är innehållet i $H_1$ och vice versa. Låt $h_1 \in H_1 \setminus H_2$ och $h_2 \in H_2 \setminus H_1$. Då gäller att

$$h_1 \circ h_2 \in G = H_1 \cup H_2$$

Antag $h_1 \circ h_2 = h_1' \in H_1$. Då gäller

$$h_2 = h_1^{-1} \circ h_1' \in H_1$$

vilket motsäger antagandet $h_2 \in H_2 \setminus H_1$. På samma sätt gäller att $h_1 \circ h_2 \notin H_2$. Men $h_1 \circ h_2 \in G = H_1 \cup H_2$.

(c) (1p) Ange en grupp $G$ som är en union av tre icketriviala delgrupper $H_1, H_2$ och $H_3$ till $G$.

**Lösning.**
Låt $G$ beteckna gruppen som består av de multiplikativt inverterbara elementen i ringen $Z_{12}$, så

$$G = \{1, 5, 7, 11\},$$

som har delgrupperna

$$H_1 = \langle 5 \rangle = \{1, 5\}, \qquad H_2 = \langle 7 \rangle = \{1, 7\} \qquad H_3 = \langle 11 \rangle = \{1, 11\},$$

vars union är $G$.

(d) (1p) Finns det någon grupp $G$ som är en union av fyra icketriviala delgrupper till $G$? Motivera ditt svar.

**Lösning.** Vi låter $G$ vara gruppen $\mathcal{S}_4$, dvs mängden av permutationer av elementen i mängden $\{1, 2, 3, 4\}$. Denna grupp är följande union av fyra av sina icketriviala delgrupper:

$$\mathcal{S}_4 = \{\text{id.}, (1\,2\,3), (1\,3\,2)\} \cup \{\text{id.}, (1\,2)\} \cup \{\text{id.}, (2\,3)\} \cup \{\text{id.}, (1\,3)\}$$

10. (5p) Låt $\mathcal{S}_n$ beteckna mängden av alla permutationer av elementen i mängden $\{1, 2, \ldots, n\}$. Låt $m(k)$ beteckna det minsta heltal $m$ sådant att $\mathcal{S}_n$ har en permutation av ordning $k$ för alla hela tal $n \geq m$. Härled en formel för antalet permutationer av ordning $k$ i $\mathcal{S}_{m(k)}$.

(Kvaliteten hos dina motiveringar spelar stor roll vid poängbedömningen av denna uppgift.)

**Lösning.** Vi konstaterar först att om elementet $\varphi$ i gruppen $\mathcal{S}_n$ har ordning $k$ så finns för varje $t \geq n$ en permutation $\psi$ i $\mathcal{S}_t$ av ordning $k$, nämligen

$$\psi(i) = \begin{cases} \varphi(i) & \text{om} \quad i \leq n, \\ i & \text{om} \quad n < i \leq t. \end{cases}$$

Alltså räcker det att hitta det minsta tal $m = m(k)$ sådant att $\mathcal{S}_m$ har en permutation av ordning $k$.

Vi visar att om $k = p_1^{e_1} \cdots p_r^{e_r}$, där $p_1, \ldots, p_r$ är olika primtal, och exponenterna $e_1, \ldots, e_r$ är positiva heltal, så är

$$m(k) = p_1^{e_1} + \cdots + p_r^{e_r},$$

samt att varje permutation av ordning $k$ i $\mathcal{S}_{m(k)}$ då är en produkt av $r$ disjunkta cykler av längderna $p_1^{e_1}$, $p_2^{e_2}$, ..., resp $p_r^{e_r}$. Varje element i $\mathcal{S}_{m(k)}$ finns då med i precis en cykel. Eftersom varje cykel av längd $q = p_i^{e_i}$ kan representeras på $q$ olika sätt, se nedan:

$$(a_1\, a_2\, \cdots, a_{q-1}\, a_q) = (a_2\, \cdots\, a_{q-1}\, a_q\, a_1) = \cdots = (a_q\, a_1\, a_2\, \cdots, a_{q-1}),$$

så är det sökta formeln för antalet permutationer av ordning $k$ i $\mathrm{S}_{m(k)}$, enligt multiplikationsprincipen, lika med

$$\frac{m(k)!}{p_1^{e_1}\cdots p_r^{e_r}}$$

dvs

$$\frac{(p_1^{e_1}+\cdots+p_r^{e_r})!}{p_1^{e_1}\cdots p_r^{e_r}}.$$

Nu till bevis av att $m(k)$ är som ovan angivits.

Vi kommer att använda oss av att ordningen av en permutation är minsta gemensamma multipleln av cykellängderna, utan att alltid specifikt hänvisa till detta faktum. Till exempel om $\varphi$ är en produkt av $r$ stycken disjunkta cykler av längd $p_i^{e_i}$, för $i=1,2,\ldots,r$, så har $\varphi$ ordning $k$.

Vidare kommer vi att använda att

$$\ell = m_1 m_2 \cdots m_s \qquad \Longrightarrow \qquad \ell > m_1+m_2+\cdots+m_s.$$

om $m_i \geq 2$ för $i=1,2,\ldots,s$ och minst ett av talen $m_i$ är större än 2 samt $s\geq 2$. (Bevis av detta är ej nödvändigt för full poäng men kommer här:

$$m_1m_2 > (m_1-1)(m_2-1) > 1 \quad\Longrightarrow\quad m_1m_2-m_1-m_2+1>1 \quad\Longrightarrow\quad m_1m_2>m_1+m_2,$$

om t ex $m_2-1>1$.

Fortsätt sedan med ett induktionsbevis för att uppnå den generella olikheten för en produkt av $s$ faktorer samtliga minst lika med 2.)

Antag $\varphi$ är en permutation av ordning $k$. Vi skriver $\varphi$ som en produkt av disjunkta cykler

$$\varphi = \ell_1\ell_2\cdots\ell_s$$

med längderna $m_1$, $m_2$, ..., $m_s$. Ordningen av $\varphi$ är minsta gemensamma multipeln av talen $m_1$, $m_2$, ..., $m_s$. Så samtliga primtalspotenser $p_i^{e_i}$ måste var och en dela minst ett av talen $m_i$. Antag att

$$m_i = p_{i_1}^{e_{i_1}} p_{i_2}^{e_{i_2}} \cdots p_{i_q}^{e_{i_q}} a_i.$$

för något heltal $a_i$. Då gäller från ovan att

$$m_i \geq p_{i_1}^{e_{i_1}} + p_{i_2}^{e_{i_2}} + \cdots + p_{i_q}^{e_{i_q}} + a_i. \tag{1}$$

Låt $d_i$ beteckna antalet tal $m_j$, där $j=1,2,\ldots,s$, som delas av talet $p_i^{e_i}$. Vi får då från ekvation (1) att

$$m_1+\cdots+m_s \geq d_1p_1^{e_1}+\cdots+d_rp_r^{e_r} \geq p_1^{e_1}+\cdots+p_r^{e_r} = m(k) \tag{2}$$

eftersom vi redan konstaterat att $d_i \geq 1$ för $i=1,2,\ldots,r$. Cyklerna $\ell_1$, ..., $\ell_s$ är disjunkta och minst $m(k)$ olika element permuteras. Av ekvation (2) framgår att det inte finns någon annan möjlighet att uppnå denna undre begränsning på ett annat sätt än när antalet cykler är $r$ och cyklernas längder är $p_i^{e_i}$, för $i=1,2,\ldots,r$.

**SVAR:** För $k=p_1^{e_1}\cdots p_r^{e_r}$, där $p_1,\ldots,p_r$ är olika primtal, och exponenterna $e_1,\ldots,e_r$ är positiva heltal, så är den sökta formeln

$$\frac{(p_1^{e_1}+\cdots+p_r^{e_r})!}{p_1^{e_1}\cdots p_r^{e_r}}.$$