Matematiska Institutionen
KTH

Lösning tentamensskrivning i Diskret Matematik för CINTE, CL och CMETE, SF1610 och 5B1118, lördagen den 28 januari 2012, kl 09.00-14.00.

Examinator: Olof Heden

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

Betygsgränser: (Totalsumma poäng 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

För ett godkänt resultat krävs också minst 12 poäng på del I.

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

DEL I

Var och en av nedanstående fem uppgifter på del I svarar mot en kontrollskrivning. Godkänt resultat på kontrollskrivning nr i under 2011 ger automatiskt full poäng på uppgift nr i nedan. Att lösa en uppgift som man på detta sätt redan har till godo ger inga extra poäng.

1. (3p) Bestäm samtliga lösningar till den diofantiska ekvationen

$$59x + 73y = 2.$$

Lösning: Euklides algoritm ger

$$\begin{array}{rcrcr} 73 & = & 59 & + & 24 \\ 59 & = & 2 \cdot 24 & + & 11 \\ 24 & = & 2 \cdot 11 & + & 2 \\ 11 & = & 5 \cdot 2 & + & 1 \end{array}$$

varur vi finner att

$$1 = 11 - 5 \cdot 2 = 11 - 5(24 - 2 \cdot 11) = 11 \cdot 11 - 5 \cdot 24 = 11(59 - 2 \cdot 24) - 5 \cdot 24 =$$

$$= 11 \cdot 59 - 27 \cdot 24 = 11 \cdot 59 - 27(73 - 59) = 38 \cdot 59 - 27 \cdot 73.$$

Efter multiplikation med 2 finner vi att

$$76 \cdot 59 - 54 \cdot 73 = 2.$$

På sedvanligt sätt, eller enligt formel i läroboken, emedan 59 och 73 är relativt prima, får vi

SVAR: $x = 76 + 73n$ och $y = -54 - 59n$ där $n = 0, \pm 1, \pm 2, \ldots$

2. (3p) I en klass med 10 flickor och 12 pojkar skall man utse ett klassråd med fem barn. Hur många möjligheter finns det för ett sådant klassråd om det måste finnas med minst en flicka och minst en pojke i klassrådet. För full poäng krävs att svaret ges som ett heltal, men glöm ej att motivera din lösning.

   Lösning: Utan kravet att klassrådet skall innehålla minst en pojke och en flicka blir antalet olika klassråd

   $$\binom{22}{5} = \frac{22 \cdot 21 \cdot 20 \cdot 19 \cdot 18}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 22 \cdot 21 \cdot 19 \cdot 3 = 22 \cdot 133 \cdot 9$$

   Antalet klassråd utan pojke är

   $$\binom{10}{5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 28 \cdot 9$$

   och utan flicka är

   $$\binom{12}{5} = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 88 \cdot 9.$$

   SVAR: $22 \cdot 133 \cdot 9 - 9 \cdot 28 - 9 \cdot 88 = 25290$

3. (3p) Undersök om gruppen $G = (Z_{13} \setminus \{0\}, \cdot)$ är en cyklisk grupp.

   Lösning: Antalet element i G är 12. Varje element i G har en ordning som delar 12. Vidare är G cyklisk om det finns ett element av ordning 12 i G. Vi testar om elementet 2 har ordning 12:

   $$2^2 = 4 \neq 1, \quad 2^3 = 8 \neq 1, \quad 2^4 = 3 \neq 1, \quad 2^6 = 12 \neq 1.$$

   Eftersom elementet 2 varken har ordning 1, 2, 3, 4 eller 6 så måste detta element ha ordning 12, så

   SVAR: Ja, gruppen är cyklisk.

4. (3p) Ett RSA-krypto har parametrarna $n = 91$ och $e = 29$. Dekryptera meddelandet 3, dvs bestäm $D(3)$.

Lösning: Vi konstaterar att $n = 7 \cdot 13$ och alltså är parametern $m = (7-1)(13-1) = 72$. För den dekrypterande nyckeln d gäller att $d \cdot e = 1$ i ringen Z_m. Euklides algoritm ger nu

$$\begin{array}{rcrcr} 72 & = & 3 \cdot 29 & - & 15 \\ 29 & = & 2 \cdot 15 & - & 1 \end{array}$$

och därmed

$$1 = 2 \cdot 15 - 29 = 2(3 \cdot 29 - 72) - 29 = 5 \cdot 29 - 2 \cdot 72.$$

dvs i ringen Z_{72} gäller att $5 \cdot 19 = 1$ och vi har att $d = 5$. Nu dekrypterar vi elementet 3:

$$D(3) = 3^5 \pmod{91} = 243 \pmod{91} = 61$$

SVAR: 61.

5. (3p) En sammanhängade planär graf har totalt nio noder varav fyra noder med valensen 2, två noder med valensen 3, en nod med valensen 4 och två noder med valensen 5. Vilka möjligheter finns det för antalet områden som uppstår vid en plan ritning av grafen, om ytterområdet skall räknas med.

Lösning: Summan av nodernas valenser är

$$4 \cdot 2 + 2 \cdot 3 + 1 \cdot 4 + 2 \cdot 5 = 28,$$

så antalet kanter i grafen är 14. Eulers polyederformel ger nu att antalet områden r satisfierar

$$9 + r = 14 + 2,$$

så

SVAR: Antalet områden är $r = 7$.

DEL II

6. (3p) Bestäm antalet funktioner f från mängden $\{1, 2, 3, 4, 5, 6\}$ till mängden $\{1, 2, 3, 4, 5\}$ som är sådana att $|\{f(1), f(2), f(3)\}| = 3$. För full poäng krävs att svaret ges som ett heltal, men glöm ej att motivera din lösning.

Lösning: Det finns $5 \cdot 4 \cdot 3 = 60$ olika möjligheter att välja tre olika värden till $f(1), f(2)$ och respektive $f(3)$. Funktionsvärdena $f(4)$, $f(5)$ och $f(6)$ kan sen väljas godtyckligt bland elementen i mängden $\{1, 2, 3, 4, 5\}$, dvs på totalt $5^3 = 125$ olika sätt. Multiplikationsprincipen ger nu

SVAR: $125 \cdot 60$, dvs 750, olika funktioner som satisfierar de givna villkoren.

7. (4p) Antag att skogen T har 100 noder varav minst 27 av noderna har valensen (graden) 3. Bestäm det maximala antalet träd som kan finnas i denna skog.

Lösning: Antag att antalet träd i en skog är t, och att träden är T_1, T_2, ..., T_t, var och en med v_i noder, och därför med $e_i = v_i - 1$ kanter. Givna indata ger då att

$$v_1 + v_2 + \ldots + v_t = 100$$

och då $e_i = v_i - 1$, att

$$t + e_1 + e_2 + \ldots + e_t = 100,$$

dvs antalet träd är

$$t = 100 - |E|,$$

där $|E|$ är antalet kanter i skogen. Så för att få så många träd som möjligt så skall vi minimera antalet kanter i en acyklisk graf där minst 27 av noderna har valens 3.

Eftersom

$$\sum_{v \in V} \delta(v) = 2|E| \tag{1}$$

får vi minst antal kanter när vi har 27 noder med valens 3 och så få antal noder med valens 1 eller 2 som möjligt (och inga noder med valens större än 3).

Varje träd har löv. Ett träd med fyra noder varav en har valens 3 har tre löv. Om vi lägger till två grenar till ett av löven så får vi ett träd med två noder med valensen 3 och fyra löv. Så antalet löv ökar med ett varje gång vi låter ett träd växa på detta sätt. Detta ger ett bidrag med 1 till summan i ekvation T (1), förutom bidraget 3 från noden med valens 3. Om vi bara lägger till en gren vid ett löv så har vi kvar samma antal löv som tidigare men får en nod med valensen 2, vilket adderar 2 till summan i ekvation (1). Så för varje träd, det mest ekonomiska sättet, ekonomiskt i den meningen att använda så få kanter som möjligt, är att lägga till två grenar vid varje nod när trädet växer. Ett så konstruerat träd med k noder av grad 3 kommer att ha $2 + k$ löv.

Slutsatsen blir att den optimala situationen inträder när vi har ett träd med 27 noder med valens 3 och 29 löv. Ett sådant träd har då totalt $27 + 29 = 56$ noder. Kvar blir då 44 noder som var och en kan bilda ett träd.

SVAR: Det kan finnas högst 45 träd i skogen.

8. (4p) Antag G är en abelsk grupp, dvs $ab = ba$ för alla element a och b i G. Låt $\sigma(g)$ beteckna ordningen av elementet g i G. Visa att om $\text{sgd}(\sigma(a), \sigma(b)) = 1$ så är $\sigma(ab) = \text{mgm}(\sigma(a), \sigma(b))$.

Lösning: Låt

$$H = \langle a \rangle \cap \langle b \rangle.$$

Eftersom H är en delgrupp till $\langle a \rangle$ och $\langle b \rangle$ så följer av Langranges sats att $|H|$ delar $|\langle a \rangle| = \sigma(a)$, och $|H|$ delar $\sigma(b)$. Eftersom $\gcd(\sigma(a), \sigma(b)) = 1$ så måste $|H| = 1$.

Låt $n = \sigma(ab)$, då gäller eftersom $ab = ba$, att $a^n b^n = e$. Om $a^n \neq e$ så $a^n = (b^n)^{-1}$ vilket är ett element i både $\langle a \rangle$ and $\langle b \rangle$ och därmed $a^n \in H$. Detta innebär att $a^n = e$ och $b^n = e$ eftersom $H = \{e\}$.

Vi visar nu att detta innebär att $\sigma(a)$ delar n, och likadant för b.

Om $n = k \cdot \sigma(a) + r$, där $0 \leq r < \sigma(a)$, så

$$e = a^n = (a^{\sigma(a)})^k \cdot a^r = e^k \cdot a^r = a^r,$$

vilket motsäger det faktum att $\sigma(a)$ är det minsta heltal t sådant att $a^t = e$, såvida inte $r = 0$. Alltså, $\sigma(a)$ delar n.

Vi vet nu att både $\sigma(a)$ och $\sigma(b)$ delar n. Enligt definition av minsta gemensamma multipel betyder detta att $\mathrm{lcm}(\sigma(a), \sigma(b))$ delar n.

Eftersom ordningarna av a och b är relativt prima, så är minsta gemensamma multipeln av ordningarna av a and b lika med produkten av deras ordningar. Alltså,

$$(ab)^{\mathrm{lcm}(\sigma(a),\sigma(b))} = (ab)^{\sigma(a)\sigma(b)} = (a^{\sigma(a)})^{\sigma(b)} \cdot (b^{\sigma(b)})^{\sigma(a)} = e.$$

Sammanfattningsvis: Vi har visat att $\mathrm{lcm}(\sigma(a), \sigma(b))$ delar ordningen av ab, och att $(ab)^{\mathrm{lcm}(\sigma(a),\sigma(b))} = e$. Detta betyder att ordningen av ab är den givna.

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. För en 1-felsrättande kod C av längd n så låter vi $D(C)$ beteckna mängden av ord som C inte kan rätta, dvs $D(C)$ består av de ord av längd n vars avstånd är minst två till alla kodord.

   (a) (2p) Låt C vara den 1-felsrättande kod som har nedanstående matris som kontrollmatris:

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

   Visa att orden i mängden $D(C)$ bildar en 1-felsrättande kod, som inte är linjär.

   Lösning: Se lösning av uppgift (b) nedan med $n = 6$ och $m = 3$.

(b) (3p) Låt C vara en linjär 1-felsrättande kod av längd n och med $|C| = 2^{n-m}$ ord. Gäller det generellt att om kodens kontrollmatris har m rader och $n = 2^m - 2$ kolonner så kommer orden i mängden $D(C)$ att utgöra en 1-felsrättande kod?

Lösning: Låt $\mathbf{H}$ beteckna kodens kontrollmatris. Koden C består av de ord $\mathbf{x} = (\mathbf{x_1}\ \mathbf{x_2}\ \ldots\ \mathbf{x_n})$ sådana att

$$\mathbf{H}\mathbf{x}^T = \mathbf{0}^T.$$

Låt $\mathbf{k}^T$ vara den unika kolonn som är skild från nollkolonnen och inte finns med bland matrisen $\mathbf{H}$:s kolonner. Då gäller att mängden $D(C)$ består av de ord $\mathbf{y}$ sådana att

$$\mathbf{H}\mathbf{y}^T = \mathbf{k}^T.$$

Låt $\mathbf{y}'$ vara ett annat ord i $D(C)$. Vi visar att avståndet mellan $\mathbf{y}$ och $\mathbf{y}'$ är minst tre, och betraktar för den skull $\mathbf{x} = \mathbf{y} - \mathbf{y}'$. Multiplicerar vi med $\mathbf{H}$ får vi

$$\mathbf{H}(\mathbf{y}^T - \mathbf{y}')^T = k^T - k^T = 0^T,$$

varav följer att $\mathbf{x} = \mathbf{y} - \mathbf{y}'$ tillhör den 1-felsrättande koden C. Antalet ettor i ordet $\mathbf{x}$ är då minst tre, och därmed skiljer sig orden $\mathbf{y}$ och $\mathbf{y}'$ åt i minst tre positioner. Således, koden $D(C)$ har minavstånd tre och är då 1-felsrättande.

10. (5p) Låt $\mathcal{S}_n$ beteckna mängden av alla permutationer av elementen i mängden $\{1, 2, \ldots, n\}$. Vi låter på sedvanligt sätt $\mathcal{S}_n$ utgöra en grupp. Bestäm en formel för antalet delgrupper av ordning p till $\mathcal{S}_n$ i de fall då p är ett primtal.

Lösning: Om p är ett primtal och H en delgrupp med p element, så har alla element utom identiteten en ordning som delar talet p, dvs de har ordning p och genererar H. Så har $p-1$ element av ordning p. Skärningen mellan två delgrupper H och K till en grupp är också en delgrupp $H \cap K$ till både H och K. Enligt Lagranges sats delar då antalet element i $H \cap K$ antalet element p i H, och enda möjligheten, om $H \neq K$, är då att $H \cap K = \{\text{id.}\}$.

Varje element av ordning p genererar en cyklisk delgrupp med p element, och varje sådant element tillhör, enligt resonemanget ovan, precis en sådan delgrupp, med precis $p - 1$ element av ordning p. Vi sluter att antalet delgrupper med p element är lika med antalet element av ordning p delat med $p - 1$.

Så vi bestämmer antalet element av ordning p. Ett element av ordning p i $\mathcal{S}_n$, när p är ett primtal, är en produkt av disjunkta cykler av längd p, samt 1-cykler.

Antalet olika p-cykler man kan skapa med hjälp av elementen i mängden $\{x_1, x_2, \ldots, x_p\}$ är $(p-1)!$. Eftersom dessutom de olika p-cyklerna i permutationen är oetiketterade så blir antalet element av ordning p i $\mathcal{S}_n$ lika med

$$\sum_{i=1}^{\lfloor n/p \rfloor} \frac{1}{i!} \cdot \binom{n}{p, p, \ldots, p, 1, 1, \ldots, 1} ((p-1)!)^i = \sum_{i=1}^{\lfloor n/p \rfloor} \frac{1}{i!} \cdot \frac{n!}{p^i}$$

Som vi konstaterade tidigare tillhör varje sådant element precis en delgrupp med ordning p, och varje delgrupp av ordning p, när p är ett primtal, kommer att innehålla precis $p-1$ element av ordning p, Således får vi

SVAR:

$$\frac{1}{p-1} \cdot \sum_{i=1}^{\lfloor n/p \rfloor} \frac{1}{i!} \cdot \frac{n!}{p^i}$$