Matematiska Institutionen
KTH

Lösning till tentamensskrivning i Diskret Matematik för CINTE och CMETE, m fl, SF1610, tisdagen den 2 juni 2015, 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 fem uppgifter svarar mot en kontrollskrivning. Godkänt resultat på kontrollskrivning nr. i under vårterminen 2015 ger automatiskt full poäng på uppgift nr. i. Att lösa en uppgift som man på detta sätt redan har till godo ger inga extra poäng.

1. (a) (1p) Bestäm $53^{100} (\text{mod } 101)$.

   Lösning. Talet $p = 101$ är ett primtal och $a = 53$ är relativt primt till p så vi kan använda Fermats lilla sats och får då
   $$1 \equiv_p a^{p-1} \equiv_{101} 53^{100}.$$
   Så
   SVAR: 1.

   (b) (2p) Lös ekvationen $43x + 12 = 53$ i ringen Z_{97}.

   Lösning. Vi får till en början att $43x = 41$. Söker inversen till 43 i ringen Z_{97}. Ur Euklides algoritm får vi
   $$97 = 2 \cdot 43 + 11, \qquad 43 = 4 \cdot 11 - 1,$$
   och vidare
   $$1 = 4 \cdot 11 - 43 = 4(97 - 2 \cdot 43) - 43 = 4 \cdot 97 - 9 \cdot 43.$$
   Så $43^{-1} = -9$. Till slut
   $$43x = 41 \quad \Longrightarrow \quad x = 43^{-1} \cdot 41 = -9 \cdot 41 \equiv_{97} -369 \equiv_{97} 19.$$
   SVAR: $x = 19$.

2. (3p) Ange nedanstående binomialkoefficient, multinomialkoefficient respektive Stirlingtal som hela tal:
   $$\binom{45}{42}, \qquad \binom{20}{14, 2, 2, 2}, \qquad S(8, 7).$$

   Lösning. Svar och uträkningar nedan:
   $$\binom{45}{42} = \binom{45}{3} = \frac{45 \cdot 44 \cdot 43}{1 \cdot 2 \cdot 3} = 15 \cdot 22 \cdot 43 = 30 \cdot 473 = 14190.$$

$$\binom{20}{14,2,2,2} = \frac{20!}{14!2!2!2!} = \frac{20\cdot 19\cdot 18\cdot 17\cdot 16\cdot 15}{2\cdot 2\cdot 2} = 10\cdot 19\cdot 18\cdot 17\cdot 60 = 3488400.$$

När man delar in en mängd med 8 element i 7 icketomma delmängder kommer precis en av delmängderna A att innehålla precis två element, och de övriga sex delmängderna vardera precis ett element. Antalet sätt att välja element till mängden A är alltså lika med

$$\mathrm{S}(8,7) = \binom{8}{2} = \frac{8\cdot 7}{2!} = 28.$$

3. Betrakta gruppen $G = (Z_{21}, +)$

   (a) (1p) Bestäm ett element av ordning 7 i G.

   Lösning. Elementet 3 har ordning 7 ty $k\cdot 7 \neq 0$ för $1 \leq k \leq 6$ men $7\cdot 3 = 0$.

   (b) (1p) Bestäm en cykliska delgrupp till G med sju element.

   Lösning. Den delgrupp som genereras av elementet 3 har sju element:

   $$\langle 3\rangle = \{3, 6, 9, 12, 15, 18, 21 = 0\}.$$

   (c) (1p) Finns det någon sidoklass S till en delgrupp till G sådan att S har fem element?

   Lösning. Nej, antalet element i en sidoklass till en delgrupp H till en grupp G är detsamma som antalet element i H. Enligt Lagranges sats har en grupp med 21 element ingen delgrupp med fem element.

4. (3p) Ett RSA-krypto har de offentliga nycklarna $n = 187$ och $e = 89$. Dekryptera meddelandet 2, dvs bestäm $\mathrm{D}(2)$.

   Lösning. Vi faktoriserar $n = 11\cdot 17$ varur $m = (11-1)(17-1) = 160$. Den dekryperande nyckeln d satisfierar $d\cdot e = 1$ i ringen Z_m. Vi beräknar nu 89^{-1} i ringen Z_{160}:

   $$160 = 2\cdot 89 - 18, \qquad 89 = 5\cdot 18 - 1$$

   så

   $$1 = 5\cdot 18 - 89 = 5(2\cdot 89 - 160) - 18 = 9\cdot 89 - 5\cdot 160.$$

   Alltså $d = e^{-1} = 9$. Vi kan nu dekryptera:

   $$\mathrm{D}(2) = 2^9 (\mathrm{mod}\ 187) = 512 (\mathrm{mod}\ 187) = (138 + 2\cdot 187)(\mathrm{mod}\ 187) = 138.$$

   SVAR: 138.

5. Den planära och sammanhängande grafen G har noder med valenserna (graderna)

   $$1,\ 2,\ 2,\ 2,\ 3,\ 3,\ 3,\ 3,\ 4,\ 4,\ 5,\ 5,\ 7.$$

   (a) (2p) Bestäm antalet områden (regioner) som uppstår när grafen G ritas plant.

   Lösning. Antalet kanter e fås ur sambandet summa valenserna är lika med tvaa gånger antalet kanter:

   $$e = \frac{1+2+2+2+3+3+3+3+3+4+4+5+5+7}{2} = \frac{44}{2} = 22.$$

   Eulers formel ger nu antalet områden till

   $$r = e + 2 - v = 22 + 2 - 13 = 11.$$

   (b) (1p) Vilket är det minsta antal kanter som behöver läggas till för att grafen G skall få en Eulerkrets.

   Lösning. En sammanhängade graf har en Eulerkrets om och endast om alla noder har en jämn valens. Vi förbinder par av noder med udda valens med en ny kant. Det finns 8 noder med udda valens och därför fyra par av noder med udda valens, så
   SVAR: 4

VGV

DEL II

6. (3p) Bestäm antalet ord av längd 7 som man kan bilda med hjälp de sju bokstäverna A, B, C, D, E, F och G (varje bokstav skall förekomma precis en gångi ordet) och som är sådana att inget av orden EFGA, ABC och BEF får finnas med som delord i ordet. (T ex så är ordet ABCEDFG ett förbjudet ord, eftersom ABC är ett delord, DFAE är för kort och ordet AAABBBB innehåller inte samtiga sju bokstäver.)

   Lösning. Vi använder principen om inklusion exklusion. Låt $\mathcal{A}$ beteckna mängden av ord som har ordet EFGA som delord, $\mathcal{B}$ mängden av ord som innehåkller ordet ABC som delord och $\mathcal{C}$ mängden av ord som innehåller ordet BEF. Vi beräknar nu storleken på dessa mängder samt storleken på alla snitt av dessa mängder. T ex ett ord i mängden $\mathcal{A}$ består av kombinationer av "bokstäverna" B, C, D och EFGA och innehåller alltså totalt 4! olika ord. Så vi får

   $$|\mathcal{A}| = 4!, \quad |\mathcal{B}| = |\mathcal{C}| = 5!, \quad |\mathcal{A} \cap \mathcal{B}| = 2!, \quad |\mathcal{A} \cap \mathcal{C}| = 3!,$$

   Vidare ser vi att

   $$\mathcal{B} \cap \mathcal{C} = \emptyset, \quad \mathcal{A} \cap \mathcal{B} \cap \mathcal{C} = \emptyset$$

   Formeln för inklusion exklusion ger nu

   SVAR: $7! - 4! - 5! - 5! + 2! + 3! + (0 - 0)$.

7. (4p) Bestäm en 1-felsrättande kod C av längd 12 sådan att C innehåller 128 ord varav ordet 111111111111 är ett av kodens ord samt sådan att ordet 111000000000 rättas till ordet 111100000000.

   Lösning. Vi bestämmer kodens kontrollmatris $\mathbf{H}$. Antalet kolonner är 12 och antalet rader skall då vara 5 eftersom då blir antalet ord i koden lika med $2^{12-5} = 2^7 = 128$. Kolonnerna i $\mathbf{H}$ skall vara olika och ingen nollkolonn får finnas med. Vi arrangerar nu kolonner så att de specificerade orden finns med. Helt enkelt, om 111100000000 finns med i C så rättas ordet 111000000000 till detta ord, eftersom ordens avstånd är ett.

   Lite trial end error ger nu

   SVAR:

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

8. (4p) Betrakta gruppen $\mathcal{S}_8$ som består av alla permutationer av elementen i mängden $\{1, 2, \ldots, 8\}$. Bestäm antalet permutationer i $\mathcal{S}_8$ som har ordning 4.

   Lösning. Ordningen hos en permutation är minsta gemensamma multipeln av cykellängderna när permutationen är skriven som en produkt av disjunkta cykler. Om en permutation skall ha ordning 4 måste den ha minst en cykel av längd 4 samt cykler av längd 2 förutom 1-cykler.

   1. Vi beräknar antalet permutationer som har precis en 4-cykel: Vi skall först välja ut de fyra element av de åtta som skall ingå i cykeln. Sen skall dessa fyra valda element ordnas i en cykel $(a_1\ a_2\ a_3\ a_4)$ vilket går på 3! olika sätt, eftersom vi kan välja a_1 som vilket som helst av de fyra valda elementen. Så antal möjligheter i detta fall är

   $$\binom{8}{4} \cdot 3! = 8 \cdot 7 \cdot 6 \cdot 5/4 = 420.$$

   2. Vi beräknar antalet permutationer som har precis två 4-cykler: Vi skall först välja ut två delmängder med vardera fyra element. Dessa delmängder är oetiketterade så antalet sätt att göra detta urval på är

   $$\frac{1}{2!}\binom{8}{4, 4}$$

Sen skall respektive delmängd med fyra element ordnas i cykler $(a_1\ a_2\ a_3\ a_4)$ resp $(b_1\ b_2\ b_3\ b_4)$ vilket går på $3! \cdot 3!$ olika sätt, eftersom vi kan välja a_1 resp b_1 som vilket som helst av de fyra valda elementen. Så antal möjligheter i detta fall är

$$\frac{1}{2!}\binom{8}{4,4} \cdot 3! \cdot 3! = \frac{1}{2}8 \cdot 7 \cdot 6 \cdot 5/4 \cdot 3! = 1260.$$

3. Vi beräknar antalet permutationer som har en 4-cykel och en 2-cykel: Med resonemang liknande de ovan får vi att antalet möjligheter i detta fall är

$$\binom{8}{4} \cdot 3! \cdot \binom{4}{2} \cdot 1! = 420 \cdot 6 = 2520$$

4. Vi beräknar antalet permutationer som har en 4-cykel och två 2-cykler: Med resonemang liknande de ovan får vi att antalet möjligheter i detta fall är

$$\binom{8}{4} \cdot 3!\frac{1}{2} \cdot \binom{4}{2} \cdot 1! \cdot \binom{2}{2} \cdot 1! = 1260$$

Eftersom det inte finns fler möjligheter att skapa permutationer av ordning fyra får vi

SVAR:

$$\binom{8}{4} \cdot 3! + \frac{1}{2!}\binom{8}{4,4} \cdot 3! \cdot 3! + \binom{8}{4} \cdot 3! \cdot \binom{4}{2} \cdot 1! + \binom{8}{4} \cdot 3! \cdot \binom{4}{2} \cdot 1! \cdot \binom{2}{2} \cdot 1! = 5460.$$

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 $\text{sgd}(a, b)$ och $\text{mgm}(a, b)$ beteckna den största gemensamma delaren respektive den minsta gemensamma multipeln till heltalen a och b.

   (a) (1p) Förklara varför det inte finns några hela tal a och b som uppfyller

   $$\text{sgd}(a, b) = 96, \qquad \text{mgm}(a, b) = 492.$$

   Lösning. Allmänt gäller att $\text{sgd}(a, b)$ delar både a och b och att dessa bägge tal delar $\text{mgm}(a, b)$. Härav följer att $\text{sgd}(a, b)$ delar $\text{mgm}(a, b)$. Men 96 delar inte 492.

   (b) (1p) Låt p vara ett primtal och n ett positivt heltal. Bestäm samtliga positiva heltal a och b sådana att

   $$\text{sgd}(a, b) \cdot \text{mgm}(a, b) = p^n.$$

   Lösning. Varje primtal som delar något av talen a och b delar den minsta gemensamma multipeln av a och b. Det givna villkoret ger alltså att det enda primtal som delar a och/eller b är primtalet p. Så $a = p^s$ och $b = p^t$, där $0 \leq s \leq n$ och $0 \leq t \leq n$, och

   $$\text{sgd}(a, b) = p^{\min(s,t)} \qquad \text{mgm}(a, b) = p^{\max(s,t)}$$

   och vidare

   $$\text{sgd}(a, b)\text{mgm}(a, b) = p^{s+t}.$$

   Alltså $s + t = n$. Vi får två fall:
   Fall 1: $n = 2k + 1$. Vi får precis k möjligheter

   $$\{a, b\} = \{a = p^s, b = p^{n-s} \mid 0 \leq s \leq k, \}.$$

   dvs k olika oordnade par av tal a och b.
   Fall 2: $n = 2k$. Vi får också i detta fall precis k möjligheter

   $$\{a, b\} = \{a = p^s, b = p^{n-s} \mid 0 \leq s \leq k, \}.$$

   dvs k olika oordnade par av tal a och b, där $a = b$ ifall $s = t = k$.
   SVAR: Mängderna $\{p^s, p^{n-s}\}$ för $s = 0, 1, \ldots . \lfloor n/2 \rfloor$.

(c) (3p) Låt n och m vara två positiva hela tal. Ge en formel för antalet oordnade par av positiva hela tal $\{a, b\}$ sådana att

$$\text{sgd}(a, b) = n, \qquad \text{mgm}(a, b) = m.$$

Lösning. Antag att n och m har primtalsfaktoriseringarna

$$n = p_1^{e_1} \cdots p_t^{e_t} \qquad \text{resp} \qquad m = p_1^{f_1} \cdots p_t^{f_t}$$

där $e_i \geq 0$ och $f_i \geq 0$ för $i = 1, 2, \ldots, t$. Som i deluppgift a) får vi att talet n delar talet m. Därav följer att

$$e_i \leq f_i, \qquad i = 1, 2, \ldots, t.$$

Vidare vet vi för tal a och b som satisfierar förutsättningarna att med

$$a = p_1^{g_1} \cdots p_t^{g_t} \qquad \text{resp} \qquad b = p_1^{h_1} \cdots p_t^{h_t}$$

så

$$e_i = \min\{g_i, h_i\} \quad \text{och} \quad f_i = \max\{g_i, h_i\} \qquad i = 1, 2, \ldots, t.$$

dvs för varje index i är antingen g_i eller h_i lika med e_i och det andra av g_i och h_i lika med f_i. Vi kan anta att $g_1 = e_1$ och $h_1 = f_1$. För $i \geq 2$ och för de exponenter e_i och f_i sådana att $e_i \neq f_i$ finns två möjliga val av g_i, om $e_i = f_i$ finns bara en möjlighet för exponenten g_i. Totala antalet möjliga tal a och b som ger den givna största gemensamma delaren och minsta gemensamma multipeln är alltså lika med 2 upphöjt till ett mindre än antalet exponenter e_i och f_i som är olika.

Låt $\mathbf{n}(q)$ beteckna antalet primtal som delar talet q. Då

$$\frac{m}{n} = p_1^{f_1 - e_1} \cdots p_t^{f_t - e_t}$$

får vi alltså

SVAR: Om n delar m är antalet oordnade par av tal a och b sådana att $\text{sgd}(a, b) = n$ och $\text{mgm}(a, b) = m$ lika med $2^{\mathbf{n}(m/n)-1}$.

10. Låt $\mathcal{F}$ beteckna mängden av alla booleska funktioner i de oändligt många booleska variablerna $x_1, x_2, \ldots$. Låt N beteckna de naturliga talen, dvs 0,1,2, ... och låt 2^{N} beteckna mängden av alla delmängder till N. Låt $\mathcal{B}$ beteckna mängden av bijektioner från N till N.

(a) (2p) Har $\mathcal{F}$ samma kardinalitet som mängden av alla delmängder till 2^{N}?

Lösning. En boolesk punkt P i de oändligt många booleska variablerna kan beskrivas som ett binärt ord av oändlig längd, vilket i sin tur svarar mot en delmängd till de naturliga talen, nämligen, en etta i position i svarar mot att talet i ingår i delmängden A_P. En boolesk funktion antar antingen värdet 1 eller 0 i en punkt P, en etta svara mot att delmängden A_P ingår i den delmängd till 2^{N} som den booleska funktionen anger. Detta beskriver en bijektiv funktion Φ från mängden av delmängder av 2^{N} till $\mathcal{F}$. Så

SVAR: Ja.

(b) (3p) Utgick pga felformulering.