Matematiska Institutionen
KTH

Lösning till tentamensskrivning i Diskret Matematik för CINTE, CL2 och Media 1, SF1610 och 5B1118, fredagen den 23 oktober 2009, kl 08.00-13.00.

1. (3p) Lös ekvationen $5(7x+3) = 1$ i ringen Z_9.

   Lösning: Eftersom inversen till 5 i den givna ringen är 2 så kan ekvationen uttryckas $7x + 3 = 2$. Vidare är inversen till 7 lika med 4. Alltså

   $$x = 4(2-3) = -4 = 5.$$

   SVAR: $x = 5$.

2. (3p) En klass med 15 elever skall delas in i fem grupper med vardera 1, 2, 3, 4 resp 5 elever. Hur många möjliga indelningar finns för detta. (För full poäng räcker det att svara med ett uttryck som innehåller de fyra räknesätten.)

   Lösning: Vi skall dela in den givna mängden i etiketterade delmängder av storlekarna 1, 2, 3, 4 respektive 5 element. Antalet möjligheter ges då av en multinomialkoefficient

   $$\binom{15}{1,2,3,4,5} = \frac{15!}{1! \cdot 2! \cdot 3! \cdot 4! \cdot 5!},$$

   vilket är det svar vi ger på uppgiften

3. (3p) Nedan finner du en tabell som är en delvis ifylld multiplikationstabell till en grupp G med elementen e, a, b, c, d. Bestäm ett element x i gruppen sådant att $axb^{-1} = c$.

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a				
b	b			e	a
c	c		e	a	
d	d	e	a	b	

   Lösning: Vi börjar med att komplettera tabellen till en grupptabell, och får då

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

   Räkningar i gruppen ger att

   $$x = a^{-1}cb = dcb = de = d.$$

   SVAR: $x = d$.

4. (3p) Konstruera ett RSA-krypto, dvs ange parametrar n, e och d och som har $e = 7$. Dekryptera därefter meddelandet 2, dvs bestäm $D(2)$.

   Lösning: Vi finner att $7 \cdot 3 \equiv 1 \pmod{20}$ samt att $20 = (3-1)(11-1)$. Eftersom 3 och 11 är primtal väljer vi nu $n = 33$ och har då ett RSA-krypto med $e = 7$ och $d = 3$. Dekryptering av meddelandet 2 blir då
   $$D(2) = 2^3 \pmod{33} = 8,$$
   vilket blir det svar vi avger.

5. (3p) För vilka värden på talet n och m har den kompletta bipartita grafen $K_{n,m}$ en Eulerkrets.

   (Glöm ej att motivera ditt svar.)

   Lösning: En graf har en Eulerkrets precis då alla noder har en jämn valens. I grafen $K_{n,m}$ har noderna antingen valensen n eller m. Således precis då de bägge talen n och m är jämna har grafen ifråga en Eulerkrets.

DEL II

6. Du har 8 identiska röda bollar och 4 identiska blå bollar som skall placeras efter varandra i olika rader. På hur många sätt kan detta ske om

   (a) (1p) bollarna skall placeras i en rad.

   Lösning: Bollarna skall placeras ut i 12 olika positioner i raden, varav fyra skall väljas till de blå bollarna. Så
   SVAR: $\binom{12}{4}$.

   (b) (1p) bollarna placeras i två lika långa rader, rad 1 och rad 2.

   Lösning: Ställ raderna efter varandra, rad 1 först, och vi får precis samma antal möjligheter som i föregående uppgift.

   (c) (2p) i tre icketomma rader, rad 1, rad 2 och rad 3.

   Lösning: Placera rad 1 först, sen rad 2 och sist rad tre. Lägg ut bollarna på en rad, antal möjligheter se ovan. Placera sedan ut två radavskiljare i de 11 olika mellanrummen mellan bollarna. Detta går på $\binom{11}{2}$ olika sätt.
   SVAR:
   $$\binom{12}{4} \cdot \binom{11}{2}.$$

7. (3p) Ge kontrollmatrisen H till en 1-felsrättande kod C, vars ord har längd 7, och som har så många ord som möjligt, och som uppfyller följande tre krav:

   (i) ordet 0111000 tillhör C.

   (ii) ordet 1111100 tillhör inte C men ordet går att rätta på sedvanligt sätt med hjälp av H.

   (iii) ordet 1111111 går inte att rätta.

   (**Anm.** Poäng sätts bl a efter hur stor kod C man lyckas konstruera.)

   Lösning: Vi provar först med att hitta en kod med maximalt antal ord 16, vilket kräver en kontrollmatris med sju olika kolonner, varav ingen är nollkolonnen. Då kommer varje rad att inehålla precis

fyra stycken ettor, vilket medför att ordet 1111111 blir ett kodord. Så vi kan utesluta en kod med 16 ord.

Vi provar nu om vi kan finna kontrollmatrisen till en kod med 8 ord. Den skall då ha fyra rader. Vi börjar med att se till att villkor (i) blir uppfyllt:

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

Sen lägger vi till två kolonner som gör att (ii) blir uppfyllt:

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

Nu till de sista två kolonnerna. För att ordet 1111111 inte skall gå att rätta måste summan av alla kolonner bli en kolonn som inte finns med i koden.

Summan av de fem första kolonnerna är kolonn nummer två. Så lite trial and error ger kontrollmatrisen

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

8. (4p) Betrakta gruppen $G = (Z_{29} \setminus \{0\}, \cdot)$. Denna grupp har precis en delgrupp H med fyra element och en delgrupp K med 14 element. Bestäm $H \cap K$. (Du får om du vill, och utan att behöva bevisa det, använda att också $H \cap K$ kommer att vara en delgrupp till G med mer än ett element.)

Lösning: Antalet element i $H \cap K$ är enligt Lagranges sats en delare till antalet element i H resp. antalet element i K, så

$$|H \cap K| \mid \mathrm{sgd}(|H|, |K|).$$

Således $|H \cap K|$ är lika med ett eller två. Givet var att det inte var lika med ett.

Nu vet vi att $H \cap K$ består av två element, varav det ena är identiteten. Det andra elementet har en ordning som delar antalet element i gruppen. Eftersom ordningen inte kan vara ett så måste elementets ordning vara två och elementet måste vara en lösning till ekvationen $x^2 - 1 = 0$. En faktorisering ger

$$(x - 1)(x + 1) = 0.$$

Vi befinner oss i kroppen Z_{29} och där blir produkter bara noll om en av faktorerna är noll. Så antingen är $x - 1 = 0$ eller $x + 1 = 0$ och endast elementen $x = 1$ och $x = -1$ uppfyller $x^2 = 1$.

SVAR: $H \cap K = \{1, -1\} = \{1, 28\}$.

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. Ett spännande träd till en graf G är en delgraf T till G sådan att T är ett träd och T och G har samma mängd av noder. Vidare gäller att en graf G är sammanhängande precis då G har ett spännande delträd.

(a) (1p) Rita två olika, dvs ickeisomorfa, grafer som har precis tre spännade träd vardera.

Lösning: Rita först en cykel med tre noder och tre kanter. Den har precis tre spännande träd. Häng sedan på en kant med en nod på cykeln. Fortfarande har du en graf med precis tre spännade träd.

(b) (2p) Är det sant att om en graf G bara har ett spännade träd så måste G vara ett träd. Svaret skall givetvis motiveras. En resonerande motivering är OK.

Lösning: Om grafen inte är ett träd och är sammanhängande finns minst en cykel i grafen, men med minst lika många kanter som noder. Ta bort kanter så att grafen förblir sammanhängande och har lika många kanter som noder. Nu finns en cykel, tag bort en av cykelns kanter, fortfarande hänger grafen ihop, men det som återstår är ett träd, ett spännande träd till grafen. Cykeln har flera kanter så vi kan hitta fler och olika spännade träd med denna metod.

(c) (2p) Kan en sammanhängande graf ha 75 kanter och 63 noder varav två av noderna har valens 9 vardera.

Lösning: Rita en sammanhängande graf med 47 noder som samtliga utom två har valens två och två av noderna har valens ett. Denna graf är ett träd. Rita till 8 kanter och 8 noder i vardera av de två noder som har valens ett. Grafen är fortfarande ett träd men med 63 noder och 62 kanter. Rita nu ytterligare 13 kanter i grafen utan att tillföra några ytterligare noder. Grafen fanns så svaret är ja.

10. (a) (1p) Ge en lämplig definition av vad som menas med minsta gemensamma multipeln, $\mathrm{mgm}(a, b, c)$, av tre tal a, b och c.

Lösning: Ett tal M med egenskapen att a, b och c är delare till M och om talen a, b och c delar m så gäller att M delar m.

(b) (1p) Bestäm $\mathrm{mgm}(124, 45, 50)$.

Lösning: Vi primfaktoriserar talen i fråga och finner att

$$124 = 2^2 \cdot 31, \qquad 45 = 3^2 \cdot 5, \qquad 50 = 2 \cdot 5^2,$$

så

$$\mathrm{mgm}(124, 45, 50) = 2^2 \cdot 3^2 \cdot 5^2 \cdot 31 = 27900,$$

eftersom minimikravet på ett tal M som skall delas av de tre givna talen är att faktorerna ovan finns med i primfaktoruppdelningen av M.

(c) (3p) Antag att du har en metod att beräkna största gemensamma delaren, $\mathrm{sgd}(x, y)$, till två tal x och y. Utred om du kan finna en formel, eller metod, som ger den minsta gemensamma multipeln av tre tal a, b och c, uttryckt i, eller med hjälp av, en eller flera beräkningar av största gemensamma delaren av två olika tal.

Lösning: Vi använder sambanden

$$\mathrm{mgm}(a, b, c) = \mathrm{mgm}(\mathrm{mgm}(a, b), c), \qquad \mathrm{mgm}(x, y) = \frac{x \cdot y}{\mathrm{sgd}(x, y)},$$

och finner att

$$\mathrm{mgm}(a, b, c) = \mathrm{mgm}(\frac{a \cdot b}{\mathrm{sgd}(a, b)}, c) = \frac{\frac{a \cdot b \cdot c}{\mathrm{sgd}(a,b)}}{\mathrm{sgd}(\frac{a \cdot b}{\mathrm{sgd}(a,b)}, c)},$$

eller med $D = \mathrm{sgd}(a, b)$, så

$$\mathrm{mgm}(a, b, c) = \frac{\frac{a \cdot b \cdot c}{D}}{\mathrm{sgd}(\frac{a \cdot b}{D}, c)} = \frac{a \cdot b \cdot c}{D \cdot \mathrm{sgd}(\frac{a \cdot b}{D}, c)},$$