Matematiska Institutionen
KTH

Tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 20 maj 2009 kl 08.00-13.00.

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

Bonuspoäng: Bonuspoäng erhållna från lappskrivningar till kursen under vt09 adderas till skrivningspoängen.

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

DEL I

1. (3p) Ett RSA-krypto har parametrarna $n = 77$ och $e = 37$. Dekryptera meddelandet 3, dvs bestäm $D(3)$.

2. (3p) Tabellen nedan är multiplikationstabellen till en grupp G.

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

   Bestäm ett element x i G som löser ekvationen
$$a^2bx = cd.$$

3. (a) (1p) Bestäm a och b så att nedanstående matris blir en parity-check (kontroll-) matris till en 1-felsrättande kod C
$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ a & 1 & 0 & 1 & 0 & b \end{bmatrix}$$
   (b) (1p) Undersök om koden C kan rätta ordet 011110, och rätta ordet i så fall.
   (c) (1p) Bestäm två olika kodord, dvs bestäm c och c' sådana att $c \neq c'$ och $c, c' \in C$.

4. (3p) Är polynomet $x^3 + 2x + 1$ irreducibelt i polynomringen $Z_5[x]$.

5. Betrakta gruppen $G = (Z_{12}, +)$.
   (a) (1p) Bestäm en delgrupp H till G sådan att H har fyra element.
   (b) (1p) Bestäm en vänster sidoklass S till H som innehåller elementet 2.
   (c) (1p) Förklara varför G saknar en sidoklass S till en delgrupp K med fyra element sådan att både 2 och 4 tillhör S.

DEL II

6. (3p) Kroppen $GF(16)$ med 16 element definieras av att kroppen består av elementen
$$GF(16) = \{a + bx + cx^2 + dx^3 \mid a, b, c, d \in Z_2\}.$$
och av att man räknar som om $x^4 + x + 1 = 0$. Lös, i den givna kroppen, ekvationen
$$(x^2 + 1)^2 z = x + 1.$$

7. Betrakta den direkta produkten R av ringarna Z_{10} och Z_{14}, dvs
$$R = Z_{10} \times Z_{14} = \{(a, b) \mid a \in Z_{10}, b \in Z_{14}\},$$
och där addition och multiplikation sker komponentvis.
   (a) (2p) Visa att (a, b) är inverterbar, m a p multiplikationen i R, om och endast om a är inverterbar i Z_{10} och b är inverterbar i Z_{14}.
   (b) (2p) Mängden av inverterbara element i en ring R bildar en grupp, ringens så kallade multiplikativa grupp $U(R)$. Avgör om $U(R)$, för den givna ringen $R = Z_{10} \times Z_{14}$, är en cyklisk grupp.

8. (4p) Går tabellen nedan att fylla i så att den blir multiplikationstabellen till en grupp

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

.

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) Låt G vara en abelsk, dvs kommutativ, grupp. Visa att om gruppen G har två olika delgrupper H_1 och H_2, som bägge har 7 element så består snittet av H_1 och H_2, dvs $H_1 \cap H_2$, endast av gruppen G:s identitetselement, med andra ord att det enda element i G som tillhör både H_1 och H_2 är G:s identitetselement. (Utan att behöva bevisa det, får man använda att $H_1 \cap H_2$ också är en delgrupp till G.)
   (b) (1p) Låt G, H_1 och H_2 vara som ovan. Antag $h_1, h_1' \in H_1$ och $h_2, h_2' \in H_2$. Visa att om $h_1 + h_2 = h_1' + h_2'$ så är $h_1 = h_1'$ och $h_2 = h_2'$.
   (c) (1p) Låt G, H_1 och H_2 vara som ovan. Visa att G har minst 49 element.
   (d) (1p) Vilka av påståendena ovan är sanna i det fall förutsättningarna ändras och kravet G abelsk inte finns med.
   (e) (2p) Formulera en allmän sats som har ovanstående resultat som ett specialfall. (Du behöver inte ge ett bevis för satsen, men poäng på denna deluppgift sätts efter kvalite'n på den sats du formulerar.)

10. (4p) Betrakta en ändlig kropp F. Låt $p(x)$ vara ett irreducibelt tredjegradspolynom i polynomringen $F[x]$. Låt K vara kroppen
$$K = \{a + bx + cx^2 \mid a, b, c \in F\},$$
där man räknar som om $p(x) = 0$. Om polynomet $q(z)$ har grad två och är irreducibelt i polynomringen $F[z]$ under vilka förutsättningar kommer då $q(z)$ också att vara irreducibelt i polynomringen $K[z]$.