Matematiska Institutionen
KTH

Tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 1 juni 2011 kl 08.00-13.00.

Examinator: Olof Heden, tel. 0730547891.

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

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

DEL I

1. (3p) Ett RSA-krypto har parametrarna $n = 57$ och $e = 31$. Dekryptera meddelandet 3, dvs bestäm $D(3)$.

2. Nedanstående matris är en check-(kontroll-)matris till en 1-felsrättande kod C

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

   (a) (1p) Undersök om koden C kan rätta ordet 01111011, och rätta ordet i så fall.

   (b) (1p) Bestäm tre olika ord i C.

   (c) (1p) Bestäm antalet ord som koden C inte kan rätta.

3. Antag gruppen G har delgrupper med 2, 3, resp 5 element samt eventuellt också delgrupper med ett annat antal element.

   (a) (2p) Vilket är det minsta antal element en sådan grupp G kan ha? Ange detta antal och en grupp med delgrupper med 2, 3 och resp 5 element och med detta minimala antal element.

(b) (1p) Ange en grupp G' med samma antal element som den grupp G du angav ovan, som inte är isomorf med G, men som också har delgrupper med 2, 3 och resp 5 element.

4. (3p) Betrakta gruppen $G = (Z_{18}, +)$. Bestäm den till antalet minsta mängd, som innehåller elementen 3 och 5, och som är en sidoklass till någon delgrupp till G.

5. (3p) Låt F_{16} beteckna den kropp med 16 element som består av elementen i mängden $\{ a_0 + a_1x + a_2x^2 + a_3x^3 \mid a_0, a_1, a_2, a_3 \in Z_2 \}$ och där man räknar som om $1 + x + x^2 + x^3 + x^4 = 0$. Lös ekvationen

$$z(x + 1) + x^2 = 1 ,$$

i denna kropp.

DEL II

6. (3p) Låt $\mathcal{M}$ beteckna mängden av binära 2×2-matriser (a_{ij}), dvs med $a_{ij} \in Z_2$ för $i = 1, 2$ och $j = 1, 2$. Mängden $\mathcal{M}$ utgör med de vanliga matrisoperationerna en ring (om vi räknar modulo 2). Låt $U(\mathcal{M})$ beteckna mängden av multiplikativt inverterbara element i ringen $\mathcal{M}$. Denna mängd utgör en grupp. Avgör om denna grupp är en cyklisk grupp.

7. (4p) Låt H vara en delgrupp till gruppen G med gruppoperationen $\circ$. Visa att för varje element g i G så är mängden $gHg^{-1} = \{ g \circ h \circ g^{-1} \mid h \in H \}$ också en delgrupp till G. Om H är en cyklisk delgrupp till G kommer då också gHg^{-1} att vara en cyklisk delgrupp till G? Motivera ditt svar.

8. (4p) Låt K beteckna den ändliga kroppen med 97 element. Bestäm samtliga lösningar till ekvationen $z^7 = 1$ i K.

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. (4p) Beskriv på ett ”lämpligt sätt” en 2-felsrättande linjär kod med 64 element.

10. (6p) Antag den ändliga abelska gruppen G har de k delgrupperna H_1, H_2, ..., H_k, där $k > 1$, sådana att $H_i \cap H_j = \{0\}$ för $i \neq j$, och med

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

Visa att det finns ett primtal p sådant att alla element i G utom nollelementet har ordning p. Bestäm också en sådan så kallad grupppartition till en grupp G med 25 element (och med $k > 1$).

.