Matematiska Institutionen
KTH

Tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 13 januari 2011 kl 14.00-19.00.

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 $n = 85$ och $e = 55$. Dekryptera meddelandet 2, dvs bestäm $D(2)$.

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

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

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

   (b) (1p) Bestäm två olika ord i C.

   (c) (1p) Bestäm antalet ord i C.

3. (3p) Kroppen F består av de 25 elementen $ax + b$ där a och b tillhör kroppen Z_5, och där man vid multiplikation av de 25 elementen kan ersätta x^2 med elementet 2. Bestäm ett element z i kroppen F sådant att

$$(x + 1)^2 z = 3x + 2.$$

4. (3p) Låt p vara ett primtal och $\mathcal{Q}$ mängden av alla kvadrater skilda från noll i ringen Z_p. Visa, genom att verifiera de fyra axiomen för en grupp, att $\mathcal{Q}$ utgör en grupp under operationen multiplikation.

5. (3p) Betrakta gruppen $G = (Z_{18}, +)$ och bestäm en sidoklass S till någon delgrupp H till G sådan att elementen 3 och 7 tillhör S men 5 inte tillhör S.

DEL II

6. (3p) Hur många halsband med fem pärlor kan man skapa om det finns q stycken olika färger att välja bland till pärlorna.

7. (4p) Bestäm samtliga delgrupper till gruppen $(Z_{29} \setminus \{0\}, \cdot)$.

8. (4p) Undersök om polynomet
$$x^6 + 3x^5 + 6x^4 + 7x^3 + 6x^4 + 3x + 1$$
är irreducibelt i polynomringen $Z_2[x]$.

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. Mängden av permutationer på mängden $\{1, 2, 3, 4\}$ bildar en grupp med 24 element, och som brukar betecknas $\mathcal{S}_4$.
   (a) (1p) Bestäm en delgrupp H_1 med 8 element till gruppen $\mathcal{S}_4$.
   (b) (2p) Det finns ytterligare två delgrupper H_2 och H_3 till $\mathcal{S}_4$ och som har 8 element. Bestäm H_2 och H_3.
   (c) (2p) Undersök om några av grupperna H_1, H_2 och H_3 är isomorfa med varandra.

10. (5p) En felrättande kod C över ett alfabete med fyra symboler, och där orden har längd 5 kan konstrueras enligt följande recept:

    Betrakta kroppen GF(16) med 16 element och vars multiplikativa grupp genereras av elementet ϑ. Låt K_0 vara delmängden
    $$K_0 = \{0, 1, \vartheta^5, \vartheta^{10}\} ,$$
    till GF(16), samt låt $K_i = \vartheta^i K_0$ för $i = 1, 2, 3, 4$. Vi definerar nu C som mängden av alla de 5-tiplar $(c_0, c_1, c_2, c_3, c_4)$ som är sådana att
    $$c_0 + c_1 + c_2 + c_3 + c_4 = 0 ,$$
    där $c_i \in K_i$, för $i = 0, 1, 2, 3, 4$.

    Diskutera vilka egenskaper koden C har och om denna konstruktion går att generalisera.