

Matematiska Institutionen  
KTH

**Tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 18 augusti 2010 kl 14.00-19.00.**

**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 vt10 adderas till skrivningspoängen.

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

## DEL I

- (3p) Ett RSA-krypto har  $n = 143$  och  $e = 103$ . Dekryptera meddelandet 3, dvs bestäm  $D(3)$ .
- (3p) Låt  $G$  beteckna gruppen  $(Z_{15}, +)$ . Vilka av följande delmängder kan vara sidoklasser till en delgrupp till  $G$ :

$$L_1 = \{2, 6, 11\}, \quad L_2 = \{2, 4, 6, 8\}, \quad L_3 = \{0, 3, 6, 9, 12\}.$$

- Låt  $F$  vara kroppen med de 8 elementen

$$F = \{a_0 + a_1x + a_2x^2 \mid a_0, a_1, a_2 \in Z_2\},$$

och där man räknar som om  $x^3 + x^2 + 1 = 0$ .

- (1p)  $F$ 's multiplikativa grupp, dvs för  $(F \setminus \{0\}, \cdot)$  är ju cyklisk. Ange, med en motivering, en generator för denna grupp (utan en korrekt motivering blir det inget poäng på denna uppgift).
  - (2p) Bestäm ett element  $w$  i  $F$  sådant att  $x \cdot w = x + 1$ .
- (3p) Gruppen  $G$  är cyklisk med 24 element, dvs det finns ett element  $a \in G$  sådant att

$$G = \langle a \rangle = \{a, a^2, a^3, \dots, a^{24} = e\},$$

där  $e$  är gruppens identitets-element.

- (1p) Ange en icke-trivial cyklisk delgrupp till  $G$ .
  - (2p) Bestäm totala antalet delgrupper som  $G$  har.
- (3p) Bestäm antalet sätt att färga hörnen i en regelbunden tetraeder i sju olika färger.

## DEL II

6. (a) (1p) Varför finns det ingen 1-felsrättande kod  $C$  med egenskapen att den rättar orden 111001010 och 110101011 till samma kodord  $c \in C$ .
- (b) (2p) Beskriv, t ex genom att ge en kontrollmatrix (check-matrix), en linjär 1-felsrättande kod  $C$  med så många ord som möjligt och som har egenskapen att orden 111001010, 110101010 och 110001011 rättas till samma kodord  $c \in C$ . Ange också antalet ord i  $C$ , samt minst tre olika ord i  $C$ .
7. (4p) Bestäm ett primitivt tredjegradspolynom i polynomringen  $Z_3[x]$ ?
8. (a) (2p) Visa att det finns en grupp  $G$  med åtta element som har icke-triviala delgrupper  $H$ ,  $K$  och  $L$  sådana att  $H \not\subseteq K$ ,  $K \not\subseteq H$  med egenskapen att  $H \cup K \cup L$  är en delgrupp till  $G$ .
- (b) (2p) Visa att gruppen  $G$  ovan inte kan ha nio element om förutsättningarna ovan skall vara uppfyllda.  
(Man får använda, utan att bevisa det, att  $H \cup K$  aldrig kan vara en delgrupp till  $G$ , jfr årets maj-tenta på detta kursmoment.)

## DEL III

Om du i denna del använder eller hänvisar till satser från läroboken skall dessa citeras, ej nödvändigtvis ordagrant, där de används i lösningen.

9. I denna uppgift antar vi att ringar inte nödvändigtvis har en så kallad "etta".
  - (a) (2p) Bestäm, och beskriv på lämpligt sätt, samtliga ringar med precis tre element. Motivera noggrant.
  - (b) (1p) Antag att både ringen  $R$  och ringen  $R'$  är kommutativa ringar med 48 element vardera. Ringen  $R$  har en delring  $S$  med fyra element som inte är en kropp och  $R'$  en delring  $S'$  med fyra element som är en kropp. Kan  $R$  och  $R'$  vara isomorfa som ringar?  
**(Motivering behövs ej för att få poäng på deluppgift b.)**
  - (c) (2p) Motivera ditt svar i uppgift b) genom ett bevis eller motsvarande.
10. (a) (2p) Bestäm den minsta kropp  $F$  som har egenskapen att  $F$  har en delkropp med fyra element och som är sådan att polynomet  $z^7 - 1$  kan faktoriseras i förstagsgradsfaktorer i polynomringen  $F[x]$ .
- (b) (3p) Bestäm den minsta kropp  $F$  som har egenskapen att  $F$  har en delkropp med fyra element och som är sådan att polynomen  $z^{14} - 1$  och  $z^{16} - 1$  kan faktoriseras i förstagsgradsfaktorer i polynomringen  $F[x]$ .