Matematiska Institutionen
KTH

Tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 19 augusti 2009 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 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 $n = 65$ och $e = 7$. Dekryptera meddelandet 2, dvs bestäm $D(2)$.

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

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

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

   (b) (1p) Bestäm antalet ord i C.

   (c) (1p) Bestäm antalet ord som inte ”kan rättas” av C.

3. (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

   Visa att elementet a genererar gruppen och bestäm samtliga delgrupper till G.

4. (3p) Bestäm ett irreducibelt andragradspolynom i polynomringen $Z_{11}[x]$.

5. (3p) Går det att bestämma a och b och n så att nedanstående mängd H blir en sidoklass till en delgrupp till $(Z_n, +)$,

$$H = \{1, 6, 16, a, b\}$$

DEL II

6. Betrakta den ändliga kropp F som på sedvanligt sätt konstrueras med hjälp av det irreducibla polynomet $p(x) = x^3 + x + 1$ i polynomringen $Z_2[x]$.

   (a) (1p) Ange antalet element i F.

   (b) (1p) Visa att elementet x genererar kroppens multiplikativa grupp.

   (c) (2p) Bestäm n så att $x^n = x^3 + x^2$.

7. Betrakta ringen R bestående av elementen

$$R = \{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in Z_3 \},$$

   och där addition och multipliktion är sedvanlig matrisaddition resp matrismultiplikation fast räkningarna sker modulo 3.

   (a) (1p) Bestäm antalet element i R.

   (b) (1p) Är ringen kommutativ.

   (c) (2p) Bestäm de element i R som är inverterbara.

8. (3p) Visa att till varje ändlig grupp G med gruppoperationen $\circ$ och identitetselement e finns minst ett primtal p och minst ett element $a \in G \setminus \{e\}$ sådant att $a^p = a \circ a \circ \cdots \circ a = e$

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) För vilka naturliga tal n gäller att mängden $Z_n \setminus \{0\}$ under operationen multiplikation i Z_n bildar en grupp $G = (Z_n \setminus \{0\}, \cdot)$. (Motivera ditt svar).

   (b) (2p) Visa att när den algebraiska strukturen G ovan bildar en grupp så kommer antalet element i snittet $H \cap K$ av två delgrupper H och K till G enbart att bero på antalet element i H och K.

   (c) (2p) Gäller det generellt för varje grupp G att antalet element i ett snitt $H \cap K$ av två delgrupper H och K till G enbart beror på antalet element i H och K. (Motivera ditt svar på lämligt sätt.)

10. (a) (1p) Ge en lämplig definition av vad som menas med att K är en delkropp till kroppen F.

    (b) (1p) Betrakta kroppen $F = \{a + b\sqrt{3} \mid a, b \in Q\}$, där Q betecknar de rationella talen. Ange en kropp $K \neq F$ som är en delkropp till F.

    (c) (3p) Bestäm en kropp F som uppfyller följande krav

        i. Q är innehållet i F.

        ii. Ekvationerna $x^2 = 2$ och $x^2 = 3$ är lösbara i F.

    och som är sådan att det inte finns någon kropp $K \subseteq F$ och $K \neq F$ som uppfyller ovanstående två krav.

    Anmärkning. Det räcker med en kortfattad motivering för svaret på denna deluppgift, så inget stringent bevis krävs.