Matematiska Institutionen
KTH

Tentamensskrivning på kursen Algebra och kombinatorik för F3, 5B1302, 14 augusti 2002, klockan 14.00-19.00.

Examinator: Olof Heden.

Tillåtna hjälpmedel: INGA HJÄLPMEDEL ÄR TILLÅTNA.
Gränser: 10 poäng ger betyget tre, 14 poäng ger betyget fyra och 18 poäng ger betyget fem.
Lösningarna måste, såvida inget annat anges, motiveras utförligt.

PROBLEM:

1. (2p) Ett RSA-system har de offentliga nycklarna $n = 77$ och $e = 13$. Knäck kryptot, dvs bestäm d, och dechiffrera meddelandet 2, dvs bestäm $D(2)$.

2. a) (2p) En felkorrigerande kod C har kontrollmatrisen (check-matrix)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Bestäm antalet kodord och kodens minimiavstånd.

b) (1p) Undersök om det finns ett ord av längd 6 som inte ligger på avståndet ett eller noll från något ord i koden C.

3. (3p) Bestäm antalet följder av längd n som man kan bilda med hjälp av siffrorna 0, 1, 2, ..., 9 sådana att siffrorna 1, 2, och 3 finns med i följden.

4. a) (1p) Visa att mängden

$$I =< x^2 - 1 >= \{p(x)(x^2 - 1) \mid p(x) \in Z_6[x]\}$$

är ett ideal i ringen $Z_6[x]$.

b) (2p) Bestäm antalet enheter i kvotringen $Z_6[x]/I$.

c) (1p) Sant eller falskt. Om ett element i en ring inte är en nolldelare är det då en enhet. Motivera ditt svar.

Anm Elementet a är en nolldelare i ringen R om det finns $b \neq 0$, $b \in R$, så att $ab = 0$ eller $ba = 0$.

5. (3p) Visa att i varje sammanhängande planär graf med färre än 12 noder finns minst en nod med valensen högst fyra.

6. a) (2p) Bestäm en delgrupp med 24 element till den symmetriska gruppen S_5.

b) (2p) Undersök om det finns någon delgrupp H med 24 element till S_5 sådan att H enbart består av jämna permutationer.

V.G.V.

7. (3p) Konstruera en kropp med 16 element och en kropp med 64 element så att snittet av dessa två kroppar är en kropp med fyra element.

8. a) (1p) Bestäm antalet n-följder av mynt som man kan bilda med hjälp av 10-kronor, femkronor och enkronor om det finns två olika 10-kronorsmynt, tre olika femkronorsmynt och två olika enkronorsmynt.

b) (2p) Samma förutsättningar som i uppgift a) men två mynt med samma värde får inte ligga bredvid varandra.

Lösningarna anslås på adressen
http://www.math.kth.se/ tranberg/5B1302.Extentor.html
efter skrivtidens slut.