MATEMATISKA INSTITUTIONEN
KTH
Examinator: Olof Heden
Telefon: 0730 547 891

Tenta B i 5B1204 DISKRET MATEMATIK för D och 5B1203 DISKRET MATEMATIK för F3 och F1spec den 22 augusti 2007, kl 14.00-19.00.

Hjälpmedel: Inga hjälpmedel tillåtna.
Gränser: Man får en trea för minst 11 poäng, en fyra för minst 15 poäng och en femma för minst 19 poäng. OBS: Godkänt, dvs minst 4 poäng, på lappskrivningen ger 2 bonuspoäng.
Motivera dina lösningar!!!

1. Det finns en sats i boken som lyder:
   Theorem 21.4 The number of orbits of G on X is
   $$\frac{1}{|G|}\sum_{g\in G}|F(g)|.$$
   (a) (2p) Förklara vad som menas med "orbits of G on X" och $F(g)$.
   (b) (2p) Skissera ett bevis av satsen. (De lemma som föregår bokens bevis av satsen behöver du inte visa eller motivera.)

2. (3p) Ett RSA-krypto har parametrarna $n = 143$ och $e = 103$. Dekryptera meddelandet 3, dvs beräkna $D(3)$.

3. (3p) De inverterbara elementen i ringen Z_{30} bildar en grupp. (Detta behöver du ej visa.) Undersök om denna grupp är cyklisk.

4. (3p) Bstäm den största gemensamma delaren i ringen $Z_3[x]$ till de bägge polynomen
   $$p(x) = 2x^5 + x^3 + 2x + 1, \quad \text{och} \quad q(x) = x^4 + x^3 + x + 1.$$

5. (3p) Undersök om nedanstående mängd matriser med sedvanliga matrisoperationer bildar en ring utan etta:
   $$\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a+b+c+d = 0, \quad a,b,c,d \in R.\}$$

6. (3p) Beskriv en 1-felsrättande binär kod med 61 ord av längd 10 och som är sådan att följande tre villkor är uppfyllda:

   (a) Ordet 1111111111 har ett avstånd minst tre till alla kodord.
   (b) Ordet 1111000000 har avstånd två till minst ett kodord.
   (c) Ordet 0000111111 har avstånd ett till minst ett kodord.

   Anm. Delpoäng kan ges för lösningar där bara vissa eller inga av villkoren ovan är uppfyllda.

7. (3p) Konstruera en ickeabelsk grupp med 30 element.

8. Låt F_4 beteckna nedanstående kropp med fyra element
   $$F_4 = \{a + \iota b \mid a, b \in Z_2\} \quad \text{med } \iota \text{ uppfyllande ekvationen} \quad \iota^2 = \iota + 1.$$
   (a) (1p) Gör en, ur matematisk synvinkel vettig, definition av vad som menas med att en kropp F är en delkropp till en kropp K.
   (b) (2p) Visa att det inte går att konstruera en kropp med åtta element som innehåller F_4 som delkropp.
   (c) (2p) Konstruera en kropp med 16 element som innehåller F_4 som delkropp.