Matematiska Institutionen
KTH

Tentamensskrivning på kursen Algebra och kombinatorik för F3, 5B1302, 22 augusti 2001 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) I ett RSA-krypto är $n = 65$ och $e = 17$. Meddelandet 3 skall sändas. Bestäm det chiffrerade meddelandet $E(3)$ och visa hur mottagaren skall göra för att dechiffrera meddelandet.

2. Betrakta den symmetriska gruppen S_5. Låt $\sigma = (1 \quad 2 \quad 3 \quad 4)$ och $\phi = (2 \quad 3 \quad 4 \quad 5)$.

a) (1p) Bestäm en permutation χ sådan att $\sigma\chi\phi = \sigma\phi\sigma$.

b) (1p) Bestäm ordningen av elementet $\sigma\phi$.

c) (1p) Har S_5 någon cyklisk delgrupp med sex element?

3. (2p) Antag att varje nod i en graf G har valensen p, där p är ett udda tal. Visa att antalet kanter i G är en multipel av p.

4. (3p) Bestäm den genererande funktionen till talföljden $a_n = 2n^2$.

5. a) (2p) Bestäm samtliga maximalideal i ringen Z_{12}.

b) (2p) Mängden S är en delring till ringen R om S är en delmängd till R och S utgör en ring under samma operationer som i R. Avgör om Z_{12} har några delringar som också är kroppar.

6. En perfekt 1-felsrättande kod C har alltid längden $n = 2^m - 1$ för något naturligt tal m. Om ordet 00...0 tillhör C så kan man visa att också ordet 11...1 tillhör C.

a) (2p) Låt C vara som ovan och antag att ordet 00...0 tillhör C. Bestäm antalet ord av vikt tre i C.

b) (3p) Bestäm antalet olika perfekta 1-felsrättande koder av längd 7 som innehåller ordet 0000000.

7. Bokstäverna i ordet INTELLIGENT används för att bilda nya ord. De nya ord som bildas skall innehålla precis samma bokstäver som detta ord, dvs två stycken N, två stycken T osv. Om två identiska bokstäver står bredvid varandra säger man att ordet innehåller ett konsekutivt par av likadana bokstäver. Till exempel så innehåller ordet INTELLIGENT precis ett konsekutivt par av likadana bokstäver.

a) (2p) Hur många ord med minst ett konsekutivt par av likadana bokstäver kan man bilda?

b) (2p) Hur många ord med minst två konsekutiva par av likadana bokstäver kan man bilda?