Matematiska Institutionen
KTH

Tentamensskrivning på kursen Algebra och Kombinatorik för F3, 5B1302, onsdagen den 8 januari 2003 kl 14.00-19.00.

Examinator: Olof Heden.

Tillåtna hjälpmedel: Inga hjälpmedel är tillåtna.

Gräns för godkänt resultat: 10 poäng.

1. a) (2p) Bestäm ett tal x sådant att 27 delar $x-4$, 35 delar $x+7$ och 61 delar $x-1$.

b) (2p) Bestäm ett tal z, $0 \leq z \leq 1010$, sådant att

$$408^{2004} \equiv z \pmod{1010}$$

2. (3p) Vi har ett RSA-system med $n = 143$ och $e = 11$. En användare A har lösenordet k (ett tal mindre än n) till en dator. I datorn lagras $E(k)$. Antag att du tar dig in i datorn och finner att $E(k) = 2$. Beräkna k.

3. (3p) Visa, utan att hänvisa till en figur du ritat, att det inte finns något träd med 10 noder sådant att fem av noderna har valensen 1, en har valensen 3, två har valensen 2 och de resterande två noderna har valensen 4.

4. a) (1p) Bestäm antalet olika ord med precis åtta bokstäver som man kan bilda med hjälp av bokstäverna a, a, b, b, c, c, d och d.

b) (2p) Hur många av orden ovan innehåller inte någon av kombinationerna aa, bb, cc eller dd.
Anm: ordet caabddebce t ex innehåller kombinationerna aa och dd.

5. (3p) Betrakta mängden av uppåt triangulära 2×2-matriser R med element från Z_3:

$$A \in R \quad \text{precis då} \quad A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad \text{där} \quad a, b, c \in Z_3.$$

Motivera varför R är en ring. Är ringen kommutativ. Ange samtliga vänsterideal. Har R några tvåsidiga ideal?

6. (3p) Man klistrar ihop nio små genomskinliga kvadrater till ett större kvadratiskt bräde bestående av nio rutor. De små kvadraterna är genomskinliga och färgade röda eller blå. Hur många olika bräden kan man klistra ihop.

7. (3p) Låt G beteckna den cykliska gruppen $G = \{a, a^2, a^3, ..., a^{24} = e\}$ och låt H beteckna den cykliska gruppen $= \{b, b^2, b^3, ..., b^{30} = e\}$ där e betecknar identitetselementet. Både G och H är delgrupper till en och samma cykliska grupp. Undersök om denna information räcker för att avgöra om det finns några element i $G \cap H$ och ange i så fall de gemensamma elementen till G och H. Motivera väl.

8. (3p) Låt F beteckna den ändliga kropp med 16 element som man på sedvanligt sätt erhåller genom att betrakta de 16 polynomen i $Z_2[x]$ vars grad är högst tre och räkna modulo ett fjärdegradspolynom $p(x)$ som är irreducibelt i $Z_2[x]$. Vi väljer $p(x) = x^4 + x + 1$. Bestäm samtliga element z i F sådana att $z^5 = 1$. De element du svarar med skall anges som polynom av grad högst tre.