Matematiska Institutionen
KTH

Tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 21 maj 2008 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 vt08 adderas till skrivningspoängen. Maximalt har man kunnat få 6 bonuspoäng.

Generellt gäller att för full poäng krävs korrekta och väl presenterade resonemang.

DEL I

1. (3p) Betrakta gruppen $G = (Z_{30}, +)$. Är mängden
$$H = \{0, 3, 7, 17, 10, 27, 2, 5, 29\},$$
en delgrupp till G?
(**OBS:** Glöm ej att motivera!)

2. (3p) Avgör om polynomet $x^2 + x + 1$ är irreducibelt i polynomringen $Z_5[x]$.

3. (3p) Mängden av enheter (eng: units) i ringen Z_{18} bildar en grupp G. Avgör om G är en cyklisk grupp.

4. (3p) Den e-felsrättande koden C har kontrollmatrisen (eng: (parity) check matrix)
$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$
   (a) Bestäm e. (**OBS:** Glöm ej att ge en kortfattad motivering!)
   (b) Bestäm ett ord $\bar{c} \in C$ sådant att $\bar{c} \neq \bar{0}$.
   (c) Går ordet 111001 att rätta.

5. (3p) Bestäm antalet olika sätt att färga kanterna i en regelbunden 6-hörning med högst k olika färger. Man kan vrida och vända på 6-hörningen, men inte flytta om kanterna genom att ha sönder 6-hörningen.

DEL II

6. (3p) Låt F beteckna den minsta ändlig kroppen med q element där $q > 3$:

$$F = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}.$$

Skriv upp additions- och multiplikationstabeller för F.

7. (4p) Låt G beteckna gruppen

$$G = (Z_2, +) \times (Z_3, +) \times (Z_4, +).$$

Bestäm samtliga delgrupper med fyra element till G och avgör vilka av dessa som är isomorfa med varandra.

8. (4p) Låt $\mathcal{S}_5$ beteckna mängden av permutationer på en mängd med fem element. Bestäm en delgrupp med 12 element till $\mathcal{S}_5$.

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) (2p) Betrakta gruppen $G = (Z_{20}, +)$. Bestäm två olika delgrupper H och K till G med sidoklasser $a + H$ och $b + K$, där $a \notin H$ och $b \notin K$, sådana att

$$|(a + H) \cap (b + K)| = 2.$$

(b) (3p) Betrakta nu en abelsk grupp G, vilken som helst. Gäller det generellt att om H_1 och K_1 är sidoklasser till delgrupper H och K till G så måste antalet element i $H_1 \cap K_1$ antingen vara noll eller dela antalet element i G, dvs

$$|H_1 \cap K_1| = m \quad \text{och} \quad |G| = n \qquad \Longrightarrow \qquad m = 0 \quad \text{eller} \quad m \mid n.$$

(Givetvis skall svaret motiveras på ett lämpligt sätt.)

10. (a) (2p) Undersök om det existerar något element α i kroppen F_{1024} med 1024 element sådant att polynomet $z^3 + \alpha$ är irreducibelt i polynomringen $F_{1024}[z]$.

(b) (3p) En kropp med p^3 stycken element skall konstrueras där p är ett stort primtal. Så du behöver ett irreducibelt polynom $p(x)$ av grad 3 i polynomringen $Z_p[x]$. Emellertid har du bara några minuter på dig så du är tvungen att gissa på ett polynom $p(x)$. Är sannolikheten för alla typer av polynom av grad tre att vara irreducibla lika stor eller beror sannolikheten för ett polynom av grad tre och av viss typ att vara irreducibelt på primtalet p?

(**Anm.** Frågan är kanske lite luddigt formulerad och kanske det inte finns något rätt svar på denna deluppgift, men antagligen mer eller mindre kloka och mer eller mindre väl motiverade strategier för att gissa på ett polynom $p(x)$.)