

Matematik, KTH

B.Ek

**Tentamen TENB i kurs SF1630(/5B1203), SF1631(/5B1204),
DISKRET MATEMATIK för D (m.fl.)
fredagen den 31 maj 2013, klockan 8.00–13.00.**

Examinator: Bengt Ek, tel 7906951.

Tillåtna hjälpmedel: Inga, inte ens räknedosa.

Högsta möjliga poäng på skrivningen är 37p. Till poängen från skrivningen läggs bonus från lappskrivningarna 1B, 2B och 3B ht 2012, högst 6p.

Betygsgränser:

För betyg	A	B	C	D	E
krävs	32	27	22	18	15

poäng (inklusive bonus)

13–14 poäng ger omdömet Fx och rätt att delta i en komplettering för betyg E.

För att ge full poäng måste lösningarna vara ordentligt motiverade.

Satser från kursen får (utom då annat sägs) användas utan bevis, om det klart anges vad de säger.

DEL I

1) (3p) Låt G vara en grupp och H en delgrupp till G .

Visa att $K = \{g \in G \mid gH = Hg\}$ är en delgrupp till G och att H är en delgrupp till K . (gH , Hg betecknar sidoklasser till H .)

2) (3p) Låt G vara en grupp som verkar på en mängd X .

Om $|G| = 77$ och $|X| = 24$, visa att G :s verkan har minst två fixpunkter, dvs det finns minst två $x \in X$ sådana att $g(x) = x$ för alla $g \in G$.

3) (3p) Kontrollmatrisen ("checkmatrisen") för en linjär, binär 1-felsrättande kod har råkat bli fel. I stället för H används

$$H' = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Korrigera H' (till H) genom att ändra ett element, då vi vet att ordet (110110) är ett kodord.

4a) (1p) Visa att $f(x) = x^2 + x + 2$ är irreducibelt i $\mathbb{Z}_5[x]$.

b) (1p) Med $\mathbb{Z}_5[x]$ och $f(x)$ konstrueras en ändlig kropp F . Vad är $|F|$?

c) (1p) Beskriv klart elementen i F och hur de adderas och multipliceras.

5) (3p) Finn alla lösningar till ekvationen $x^2 = x$, dels i $\mathbb{Z}_{341}$ och dels i $\mathbb{Z}_{431}$. [341 = 11 · 31, 431 är primtal.]

Vänd!

DEL II

6) (4p) Låt $\oplus$ och $\odot$ definieras för $a, b \in \mathbb{Q}$ (de rationella talen) enligt

$$a \oplus b = a + b + 1, \quad a \odot b = ab + a + b.$$

Visa att $(\mathbb{Q}, \oplus, \odot)$ är en kropp.

Vilka element i $\mathbb{Q}$ är identitetslement för $\oplus$ respektive $\odot$?

7) (4p) Låt $(G, \cdot)$ vara en ändlig grupp och p ett primtal.

Visa att antalet element av ordning p i G är en multipel av $p - 1$, dvs

$$(p - 1) \mid |\{g \in G \mid o(g) = p\}|.$$

8) (4p) På hur många väsentligt olika sätt (dvs så att de inte blir lika hur man än vrider kuben i rummet) kan kanterna i en kub färgas, om det skall vara precis 6 vita kanter och 6 svarta?

DEL III

För full poäng på dessa uppgifter krävs särskilt väl strukturerade och presenterade lösningar.

9) (5p) Låt $(F, +, \cdot)$ vara en ändlig kropp av karakteristik p , ett primtal.

Visa att varje element i F har en entydig p :e rot, dvs för varje $a \in F$ finns precis ett $b \in F$ sådant att $a = b^p$.

10a) (2p) Låt $g(x), h(x) \in \mathbb{Z}[x]$. Visa att om varje koefficient i produkten $g(x)h(x)$ är delbar med ett primtal p , så är alla koefficienterna i minst en av $g(x)$ och $h(x)$ delbara med p .

b) (3p) Visa att om $f(x) \in \mathbb{Z}[x]$ är reducibel i $\mathbb{Q}[x]$ (dvs om $f(x)$ betraktad som element i $\mathbb{Q}[x]$ är reducibel), så är $f(x)$ reducibel i $\mathbb{Z}[x]$.

Resultatet i a) får användas i b), även om man inte gjort a).

Lösningar kommer att läggas ut på kurssidan.