

Matematik, KTH

B.Ek

Tentamen TENB i kurs
SF1630(/SF1631), DISKRET MATEMATIK för D m.fl.
torsdagen den 9 april 2015, klockan 8.00–13.00.

Examinator: Bengt Ek, tel 790 6951 (under tentamen: Olof Heden, tel 790 6296).

Tillåtna hjälpmedel: Inga, inte ens räknedosa.

Maximal poäng på de olika delarna är T: 12p, P1: 12p, P2: 12p, P3: 10p.

För **godkänt** krävs minst 9p på var och en av delarna T och P1.

För betyg A–E krävs **dels** godkänt och **dels** poäng enligt:

För betyg	A	B	C	D	E	
krävs totalt	37	32	-	25	-	poäng
varav	-	12	8	-	-	på delarna P2 och P3 tillsammans
och	5	-	-	-	-	på del P3

Omdömet FX, dvs rätt att komplettera för betyg E, ges för skrivning som inte är godkänd, men nått minst 18p totalt.

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 T

Godkänd uppgift 1 på lsiB ht14 ger automatiskt full poäng på uppgift i ($i = 1, 2, 3$) och det ger då ingen ytterligare poäng att lösa den uppgiften på skrivningen.

1a) (1p) Låt $\circ$ vara en binär operation på mängden G (dvs en funktion $G \times G \rightarrow G$). Ange vad som krävs för att $(G, \circ)$ skall vara en **grupp**.

b) (1p) Låt $g \in G$, en ändlig grupp. För vilka $s \in \mathbb{Z}$ är $g^s = 1$ (identiteten i G)?

c) (1p) Vad menas med **centrum** $\mathcal{Z}(G)$ för gruppen G ?

2a) (1p) Vad menas med **stabilisatorn** för $x \in X$ då gruppen G verkar på mängden X (dvs G är en grupp av permutationer av X)?

b) (1p) Ange antalet banor då en grupp G verkar på en mängd X (G , X ändliga).

c) (1p) Vad krävs för att en **ring** $(R, +, \cdot)$ skall vara en **kropp** (eng. field)?

3a) (1p) För vilka $k \in \{10, 11, 12, \dots, 30\}$ finns en **kropp** F med $|F| = k$?

b) (1p) Beskriv strukturen för $(F \setminus \{0\}, \cdot)$, då $(F, +, \cdot)$ är en ändlig kropp.

c) (1p) Vilka värden är möjliga för en kropps **karaktistik**?

4a) (1p) Kodern $\mathcal{C}$ skall rätta e fel. Vad krävs för **minimiavståndet** δ i $\mathcal{C}$?

b) (1p) Hur krypteras $x \in \mathbb{Z}_n$, dvs hur fås $E(x)$, med RSA-parametrar (n, e) ?

c) (1p) Vad innebär **Fermattestet med bas b** för att testa primalitet?

DEL P1

Godkänd uppgift 2 på lsiB ht14 ger automatiskt full poäng på uppgift $4 + i$ ($i = 1, 2, 3$) och det ger då ingen ytterligare poäng att lösa den uppgiften på skrivningen.

5) (3p) Finn det minsta möjliga $|G|$, om gruppen G har en delgrupp H med $|H| = 51$ och ett $g \in G$ med ordning $o(g) = 39$ (dvs $g^{39} = 1$, $g^n \neq 1$ för $0 < n < 39$). Ge också exempel på sådana G , H , g som gör $|G|$ minimalt.

Vänd!

- 6) (3p) Låt X vara mängden av färgningar av elementen i $\{1, 2, 3, 4\}$ med (högst) två färger och $x \in X$ göra 1 och 3 röda och 2 och 4 blå. Gruppen $G = S_4$ verkar på X genom att permutera 1, 2, 3 och 4 (med sina färger). Finn banan Gx och stabilisatorn G_x .
- 7) (3p) Faktorisera $p(x) = x^5 + x^4 + 2x^3 + 2 \in \mathbb{Z}_3[x]$ i irreducibla faktorer.
- 8) En linjär, binär kod ges av kontrollmatrisen (eng. check matrix) $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$.
- a) (2p) Orden (01010), (10101), (11011) har mottagits. Vilka kodord har sänts, om högst ett fel har uppstått i varje ord?
- b) (1p) Finn ett ord som inte kan fås med högst ett fel i ett kodord.

DEL P2

- 9a) (1p) Hur många kvadrater finns det i $\mathbb{Z}_{13}$, dvs hur många element i $\mathbb{Z}_{13}$ är x^2 för minst ett $x \in \mathbb{Z}_{13}$?
- b) (3p) Hur många kvadrater finns det i $\mathbb{Z}_p$, då p är ett udda primtal? Motivera ordentligt!
- 10a) (1p) Finn en icke-trivial (dvs inte $\{id\}$ eller hela S_3) abelsk (dvs kommutativ) delgrupp till S_3 (gruppen av permutationer på $\{1, 2, 3\}$).
- b) (3p) Visa att varje icke-abelsk grupp G har minst två olika abelska icke-triviala delgrupper. Motivera ordentligt!
- 11) Låt R vara ringen $\mathbb{Z}_5[x]/(f(x))$ (alla ekvivalensklasser i $\mathbb{Z}_5[x]$ (mod $f(x)$)), där
- $$f(x) = x^3 + 3x^2 + 3.$$
- x :s ekvivalensklass kallas α .
- a) (1p) Hur många element har R ?
- b) (2p) Vad är $(\alpha^2 + 3\alpha + 2)(3\alpha^2 + 4)$ i R (uttryckt i 1, α , α^2 , med koefficienter i $\mathbb{Z}_5$)?
- c) (1p) Finn nolldelare i R , dvs $r, s \in R \setminus \{0\}$ med $r \cdot s = 0$.

DEL P3

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

- 12) (5p) En kub skall smyckas med en enfärgad kula i varje hörn. På hur många väsentligt olika sätt (dvs så att de inte blir lika hur man än vrider kuben i rummet) kan det göras om det skall vara precis två röda och två blå kulor och godtyckliga antal kulor med k andra färger (dvs utöver rött och blått)?
- 13) Låt $(G, \cdot) = (U(\mathbb{Z}_{589}), \cdot)$, gruppen av inverterbara (under multiplikation) element i $\mathbb{Z}_{589}$. [589 = 19 · 31]
- a) (1p) Finn G :s ordning, $|G|$.
- b) (2p) Vilken är den maximala ordningen för element i G ?
- c) (2p) Hur många element i G har den maximala ordningen?

Lycka till!

Lösningar kommer att läggas ut på kurssidan nästa vecka.