Matematik, KTH
B.Ek

Tentamen TENB i kurs
SF1630(/SF1631), DISKRET MATEMATIK för D (m.fl.)
onsdagen den 20 augusti 2014, klockan 14.00–19.00.

Examinator: Bengt Ek, tel 790 6951.
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 ls*i*B ht13 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 $G \times G \to G$). Ange vad som krävs för att $(G, \circ)$ skall vara en **grupp**.
b) (1p) Vad menas med att en grupp är **abelsk**?
c) (1p) Hur många delgrupper av ordning m har en **cyklisk** grupp av ordning n (för olika m, n)?

2a) (1p) Vad menas med **stabilisatorn** (eng. stabilizer) för $x \in X$ då gruppen G verkar på mängden X (dvs G är en grupp av permutationer av X)?
b) (1p) Om en ändlig grupp G verkar på mängden X, vilket samband finns mellan storlekarna för **banan** och **stabilisatorn** för $x \in X$?
c) (1p) Vad krävs för att en **ring** $(R, +, \cdot)$ skall vara en **kropp** (eng. field)?

3a) (1p) Vilka värden är möjliga för en kropps **karakteristik**?
b) (1p) Hur definieras att ett polynom i $F[x]$ är **irreducibelt**, F en kropp?
c) (1p) Vad säger **faktorsatsen** (eng. factor theorem) i $F[x]$, F en kropp?

4a) (1p) Koden med **kontrollmatris** H skall rätta ett fel. Vad krävs av H?
b) (1p) Man har RSA-parametrar $(n = p \cdot q, e)$ (p, q primtal). Hur bestäms d?
c) (1p) Vilken sats om potenser (mod $p \cdot q$) ligger till grund för RSA-kryptering?

DEL P1

Godkänd uppgift 2 på ls*i*B ht13 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) $ax^2 = b$ och $x^5 = c$, där $a, b, c, x \in G$, en grupp. Uttryck x i a, b, c.

Vänd!

6) Låt $(H, *)$ vara en delgrupp till gruppen $(G, *)$. H verkar på mängden G med gruppens operation, $h(g) = h * g$ för $h \in H$, $g \in G$.
a) (1p) Bestäm stabilisatorn H_g för $g \in G$.
b) (2p) Bestäm banan $H(g)$ för $g \in G$.

7) (3p) Faktorisera polynomet $f(x) \in \mathbb{Z}_5[x]$ i irreducibla faktorer,

$$f(x) = x^4 + x^3 + x + 4.$$

Skriv koefficienterna i faktorerna som element i $\mathbb{Z}_5$, dvs utan t.ex. minustecken.

8) (3p) Finn det minsta talet $e \geq 10$ sådant att $(391, e)$ kan användas som krypteringsnyckel i ett RSA-system. Finn också ett tal d, så att $(391, d)$ är en motsvarande dekrypteringsnyckel. [$391 = 17 \cdot 23$]

DEL P2

9) Låt $(U_{21}, \cdot)$ vara gruppen av inverterbara element i $(\mathbb{Z}_{21}, \cdot)$.
a) (1p) Ange alla element i U_{21}.
b) (3p) Avgör (med motivering) om $(U_{21}, \cdot)$ är en cyklisk grupp.

10) Låt F vara ringen $\mathbb{Z}_3[x]/(f(x))$ (alla ekvivalensklasser i $\mathbb{Z}_3[x]$ (mod $f(x)$)), där

$$f(x) = x^2 + 2x + 2.$$

x:s ekvivalensklass kallas α.
a) (1p) Visa att F är en kropp.
b) (1p) Uttryck α^2 som en linjärkombination av 1 och α (med koefficienter i $\mathbb{Z}_3$).
c) (2p) Faktorisera $g(x) = x^2 + x + 2 \in F[x]$ i irreducibla faktorer.

11) Låt $S_\mathbb{Z}$ vara mängden av bijektioner från $\mathbb{Z}$ till $\mathbb{Z}$, heltalen. $(S_\mathbb{Z}, \circ)$ är då en grupp, (med $\circ$ sammansättning av funktioner). Det behöver du inte visa.
a) (1p) Vilket element i $S_\mathbb{Z}$ är identitetselement och vilket är invers till $f \in S_\mathbb{Z}$?
b) (3p) För $A \subseteq \mathbb{Z}$, låt $K_A = \{f \in S_\mathbb{Z} \mid f(x) \in A \text{ för alla } x \in A\}$.
Är $(K_A, \circ)$ säkert (dvs för alla A) en delgrupp till $(S_\mathbb{Z}, \circ)$? Visa eller ge motexempel.

DEL P3

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

12) (5p) Ett enkelt men smakfullt armband består av 5 svarta, 2 röda och 2 vita pärlor uppträdda på en ögla av snöre.
Hur många väsentligt olika sådana armband finns det?
Pärlorna ser likadana ut från båda håll och armbanden kan vändas och vridas.

13) $\psi : G \to G$ kallas en **automorfi** för gruppen G omm den är en isomorfi.
a) (1p) Visa att $\mathrm{Aut}(G)$, mängden av G:s automorfier, är en grupp (med sammansättning av funktioner som operation).
b) (1p) Visa att om $a \in G$ och $\phi_a(g) = aga^{-1}$, så $\phi_a \in \mathrm{Aut}(G)$.
c) (3p) Låt $\mathrm{I}(G) = \{\phi_a \mid a \in G\}$ (G:s **inre** automorfier). Visa att $\mathrm{I}(G)$ är en **normal delgrupp** till $\mathrm{Aut}(G)$ (dvs en delgrupp vars vänster- och högersidoklasser är lika).

Lycka till!

Lösningar kommer att läggas ut på kurssidan.