

Matematik, KTH

B.Ek

Tentamen TENB i kurs

SF1630(/SF1631), DISKRET MATEMATIK för D m.fl.

onsdagen den 14 januari 2015, 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 ls1B 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) Hur definieras att grupperna $(G_1, *)$ och $(G_2, \circ)$ är **isomorfa**?

c) (1p) Vad menas med att en grupp är **cyklisk**?

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) Om en ändlig grupp G verkar på mängden X , vilket samband finns mellan storlekarna för **banan** och **stabilisatorn** för $x \in X$?

c) (1p) Finns det **ringar** som också är **kroppar**?

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

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

c) (1p) Vad säger **faktorsatsen** (eng. factor theorem) i $F[x]$, F en kropp?

4a) (1p) Vad menas med att en binär kod är **linjär**?

b) (1p) Vad krävs av **kontrollmatrisen** (eng. check matrix) H för att dess linjära kod skall rätta minst ett fel?

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

DEL P1

Godkänd uppgift 2 på ls1B 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) Gruppen G har två delgrupper H och K med $|H| = 21$ och $|K| = 91$. Vilka värden är möjliga för g 's ordning $o(g)$ då $g \in H \cap K$?

Vänd!

6) (3p) Låt $G = \{1, 3, 5, 7\}$. Gruppen $(G, \cdot)$, med $\cdot$ multiplikation mod 8, verkar på $X = \mathbb{Z}_{15}$ enligt $g(x) = x^g$. (Så t.ex. $3(7) = 13$, ty $7^3 = 343 = 13 \text{ i } \mathbb{Z}_{15}$.)
(Du behöver inte visa att detta definierar en gruppverkan.)

Finn dels alla banor för G 's verkan på X och dels stabilisatorerna G_6 och G_7 .

7) (3p) Finn den moniska (dvs med högstgradskoefficient 1) största gemensamma delaren till $f(x) = x^5 + 2x^3 + x^2 + x + 3$ och $g(x) = x^6 + x^5 + x^2 + 3x + 2$ i $\mathbb{Z}_5[x]$.

8) Ett RSA-system för kryptering har de offentliga parametrarna (n, e) där $n = 4331 [= 61 \cdot 71]$.

a) (1p) Vilket/vilka av 205, 206, 207, 208 och 209 är möjliga värden för e ?

b) (2p) Finn ett motsvarande d -värde för ett möjligt e från uppgift a.

DEL P2

9) Låt $(G, \cdot)$ vara $(U(\mathbb{Z}_{36}), \cdot)$, de inverterbara elementen i $\mathbb{Z}_{36}$, med multiplikation som operation, och H den minsta delgruppen till G med $5 \in H$.

a) (2p) Finn alla G 's element.

b) (2p) Finn alla H 's element och alla H 's sidoklasser.

10a) (2p) Beskriv en kropp $(F, +, \cdot)$ med $|F| = 49$ som innehåller ett nollställe α till polynomet $x^2 + 3x + 5$. Uttryck F 's element med α och element i $\mathbb{Z}_7$ och förklara hur man finner $a + b$ och $a \cdot b$ för givna $a, b \in F$.

b) (2p) Finn ett $k \in F$ med $k^2 + 1 = 0$.

11) 9431 är primtal, så $(\mathbb{Z}_{9431} \setminus \{0\}, \cdot)$ är en grupp (det behöver du inte visa).

a) (2p) Hur många element i den gruppen har ordning (eng. order) 114?

b) (2p) Hur många element i gruppen har ordning 115?

DEL P3

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

12) Låt $(R, +, \cdot)$ vara en ring. Vi definierar att $J \subseteq R$ är ett **ideal** i R om $(J, +)$ är en delgrupp till $(R, +)$ och för alla $r \in R$, $a \in J$ gäller att $a \cdot r$, $r \cdot a \in J$.

a) (2p) Visa att om $m \in \mathbb{Z}$ är $J_m = \{k \cdot m \mid k \in \mathbb{Z}\}$ ett ideal i ringen $(\mathbb{Z}, +, \cdot)$.

b) (3p) Låt $\sim$ vara en ekvivalensrelation i ringen R , sådan att $\sim$ respekterar $+$ och $\cdot$ (dvs om $r, x, y \in R$ och $x \sim y$ gäller $r + x \sim r + y$, $r \cdot x \sim r \cdot y$, $x \cdot r \sim y \cdot r$).

Visa att $J_\sim = \{x \in R \mid x \sim 0\}$ är ett ideal i R .

13) 120 identiska kulor placeras i 4 särskiljbara lådor, utan någon tom låda.

Kalla antalet kulor i låda i för n_i , $i = 1, 2, 3, 4$, så $n_i \in \mathbb{Z}_+$ för $i = 1, 2, 3, 4$.

a) (2p) Bestäm a_4 , a_{31} , a_{22} , a_{211} , a_{1111} . a_4 är antalet fördelningar av kulorna med $n_1 = n_2 = n_3 = n_4$, a_{31} är antalet med $n_1 = n_2 = n_3$, a_{22} antalet med $n_1 = n_2$ och $n_3 = n_4$, a_{211} antalet med $n_1 = n_2$ och a_{1111} det totala antalet.

b) (3p) Vad är $p_4(120)$, antalet partitioner av 120 i precis 4 delar? (Dvs på hur många sätt kan 120 identiska kulor fördelas på 4 **identiska** lådor utan någon tom låda?)

Svaren får innehålla heltal, faktulteter, potenser och de fyra enkla räknesätten.

Svaret i uppgift b får också innehålla a_4 , a_{31} , $\dots$, a_{1111} (även om uppgift a inte lösts).

Lycka till!

Lösningar kommer att läggas ut på kurssidan.