

Tentamen TENB i kurs
SF1630(/SF1631), DISKRET MATEMATIK för D m.fl.
torsdagen den 12 januari 2017, 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 ht16 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 **ordningen** (eng. order) $o(g)$ för elementet g i en grupp?

c) (1p) Vad säger **Lagranges sats** om delgruppers storlek i en ändlig grupp?

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

c) (1p) För vilka $m \in \mathbb{Z}$, $m \geq 2$, är $(\mathbb{Z}_m, +, \cdot)$ en **ring**?

3a) (1p) $(F, +, \cdot)$ är en ändlig kropp av karakteristisk 7. Vad kan $|F|$ vara?

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) En linjär, binär kod $\mathcal{C}$ har längd n och dimension k . Vad är $|\mathcal{C}|$?

b) (1p) Om p och q är olika primtal, vad krävs av e för att (n, e) (där $n = p \cdot q$) skall kunna vara en offentlig nyckel för ett RSA-system?

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

DEL P1

Godkänd uppgift 2 på lsB ht16 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) Låt $(G, *)$ vara en grupp, X en mängd och $f: G \rightarrow X$ en funktion. Vi kallar $p \in G$ en **period för f** om det för alla $g \in G$ gäller att $f(p * g) = f(g)$. Visa att $P_f = \{p \in G \mid p \text{ är en period för } f\}$ är en delgrupp till G .

6) Låt $G = U_{12}$, gruppen (med operation $\cdot$) av inverterbara (under $\cdot$) element i $\mathbb{Z}_{12}$.

a) (1p) Finn alla element i G .

b) (2p) G verkar på $X = \mathbb{Z}_{12} \times \mathbb{Z}_{12}$ med komponentvis multiplikation (dvs $g(x, y) = (g \cdot x, g \cdot y)$). Finn banan och stabilisatorn för elementet $(4, 5) \in X$.

7) (3p) Låt $f(x) = x^3 + 3 \in \mathbb{Z}_7[x]$. Visa att för alla $g(x), h(x) \in \mathbb{Z}_7[x]$:

$$f(x) \mid g(x)h(x) \Rightarrow (f(x) \mid g(x) \text{ eller } f(x) \mid h(x)).$$

($f(x) \mid g(x)$ (t.ex.) betyder förstås att det finns $\varphi(x) \in \mathbb{Z}_7[x]$ med $g(x) = f(x)\varphi(x)$.)

8) (3p) Förklara varför ingen binär kod $\mathcal{C}$ (linjär eller ej) av längd 20 och med $|\mathcal{C}| = 50\,000$ (säkert) kan rätta ett fel.

DEL P2

9) Låt $(G, \cdot)$ vara en grupp. Vi söker $a, b, c \in G$ med $a = b^2$, $b = c^2$, $c = a^2$.

a) (2p) Finn alla sådana $a, b, c \in G$ med minst två av dem lika.

b) (2p) Visa att om $|G| = 1467$ finns inga sådana $a, b, c \in G$ som alla är olika.

10) Låt $k(x) = x^4 + 8x^2 + 4 \in \mathbb{Z}_{11}[x]$ och $R = \mathbb{Z}_{11}[x]/(k(x))$ vara ringen av restklasser i $\mathbb{Z}_{11}[x]$ mod $k(x)$. Kalla restklassen med polynomet x för α .

(Så $R = \{b_3\alpha^3 + b_2\alpha^2 + b_1\alpha + b_0 \mid b_3, \dots, b_0 \in \mathbb{Z}_{11}\}$ med $k(\alpha) = 0$.)

a) (2p) Finn α^{-1} i R (dvs $r \in R$ med $r\alpha = 1$ i R).

b) (2p) Finn ett $s \in R$, $s \neq 0$, sådant att $rs \neq 1$ för alla $r \in R$.

11) Låt $A \subseteq G$, $A \neq \emptyset$, där $(G, *)$ är en grupp.

a) (3p) Visa att om $G_A = \{g \in G \mid a \in A \Rightarrow g * a \in A\}$ så är $|G_A| \leq |A|$.

b) (1p) Visa att om A är ändlig är G_A en delgrupp till G .

(Resultatet i a) får användas i b), även om a) inte gjorts.)

DEL P3

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

12) (5p) Man vill färga en kubs sidoytor (en färg per sida, förstås) och har rött, blått och k st andra färger att tillgå.

På hur många väsentligt olika sätt (dvs så att de blir olika även om man roterar dem) kan det ske, om det skall vara lika många röda som blå sidor?

13) Låt $g(x), h(x) \in \mathbb{Z}_5[x]$ ges av $g(x) = x^3 + 4x + 1$, $h(x) = x^4 + 3x^2 + 3x + 2$. Vi vill finna $f(x) \in \mathbb{Z}_5[x]$ som ger rest $r(x) = 2x^2 + 3$ vid division med $g(x)$ och rest $s(x) = 3x^3 + x^2 + 4x + 3$ vid division med $h(x)$.

a) (3p) Finn $f_0(x)$, en lösning med minimal grad.

b) (2p) Finn alla lösningar $f(x)$. ("f₀(x)" från a) får ingå i svaret, även om a) inte gjorts.)

Lycka till!

Lösningar kommer att läggas ut på kurssidan.