

Tentamen TENB i kurs
SF1630(/SF1631), DISKRET MATEMATIK för D m.fl.
onsdagen den 20 december 2017, klockan 8.00–13.00.

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 *lsB 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) Låt H vara en delgrupp till G och $|G| = 45$. Vilka värden är möjliga för antalet olika högersidoklasser till H ?

c) (1p) Låt $(G, \circ)$ och $(H, *)$ vara grupper.

Beskriv elementen och operationen i den direkta produktgruppen $(G \times H, \cdot)$.

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 ett (användbart) uttryck för **antalet banor** då en grupp G verkar på en mängd X (G, X ändliga).

c) (1p) Vad skiljer i definitionerna av begreppen **ring** och **kropp**?

3a) (1p) Beskriv strukturen för gruppen $(F, +)$, då $(F, +, \cdot)$ är en ändlig kropp.

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

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

4a) (1p) Koden med **kontrollmatris** H skall rätta ett fel. Vad krävs av H ?

b) (1p) Vilken sats om potenser (mod $p \cdot q$) ligger till grund för RSA-kryptering?

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) Elementet g i gruppen G har ordningen 60. Vilken ordning har g^{78} ?
Glöm inte att motivera svaret.

6) (3p) Låt $G = A_4$, gruppen av jämna permutationer av $\{1, 2, 3, 4\}$.
 G verkar elementvis på delmängderna till $\{1, 2, 3, 4\}$ (dvs på elementen i $\mathcal{P}(\{1, 2, 3, 4\})$).
T.ex. är $\pi\{3, 4\} = \{\pi(3), \pi(4)\}$.
Finn banorna $G\{1\}$ och $G\{2, 3\}$ och stabilisatorerna $G_{\{1\}}$ och $G_{\{2, 3\}}$ för denna verkan. Det skall tydligt framgå vilka elementen i de sökta mängderna är.

7) (3p) Låt $f(x) = x^4 + x^3 + 3x^2 + x + 1$ och $g(x) = x^5 + 3x^4 + 3x^3 + 3x + 4$ och finn den moniska (dvs med högstgradskoefficienten 1) största gemensamma delaren (eng. greatest common divisor) till $f(x)$ och $g(x)$ i $\mathbb{Z}_5[x]$.

8) Beräkna följande potenser i $\mathbb{Z}_{1547}$ ($1547 = 7 \cdot 13 \cdot 17$)

a) (1p) 55^{1153} , b) (1p) 10^{100} , c) (1p) 26^{224} .

DEL P2

9) (4p) Låt G vara en grupp, H en delgrupp till G och N en normal delgrupp till G (dvs en delgrupp vars vänster- och högersidoklasser är lika ($gN = Ng$ för alla $g \in G$)).
Visa att $HN (= \{hn \mid h \in H, n \in N\})$ är en delgrupp till G .

10) (4p) Låt $(G, +)$ vara en abelsk grupp. En **endomorf**i av G är en homomorf*i* $f: G \rightarrow G$ (dvs $f(x + y) = f(x) + f(y)$ för alla $x, y \in G$).
Låt $\text{End}(G)$ vara mängden av endomorfier av G och definiera för $f, g \in \text{End}(G)$ $f + g$ enligt $(f + g)(x) = f(x) + g(x)$, för alla $x \in G$.
Visa att $(\text{End}(G), +, \circ)$ är en ring (med etta). ($\circ$ är sammansättning av funktioner).

11) Låt X vara en mängd och G mängden av alla bijektioner $f: X \rightarrow X$.

a) (2p) Visa att $(G, \circ)$ är en grupp (där $\circ$ är sammansättning av funktioner).

b) (2p) Om $Y \subseteq X$ och $H = \{f \in G \mid f(y) \in Y \text{ för alla } y \in Y\}$, är H säkert (dvs för alla sådana X och Y) en delgrupp till G ?

DEL P3

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

12) Betrakta ringen $R = \mathbb{Z}_{11}[x]/(x^2 + 1)$ av restklasser (mod $x^2 + 1$) och kalla restklassen som innehåller x för α .

a) (1p) Hur många element finns det i R , dvs vad är $|R|$?

b) (4p) Finn alla $t \in R$ som uppfyller $t^2 + 3t + 3 = 0$.

13) (5p) Man vill färga en kubs kanter (samma färg på hela kanterna) med (en del eller alla av) färgerna rött, blått, grönt och gult.

På hur många väsentligt olika sätt (dvs så att de förblir olika då kuben roteras) kan det ske, om totalt 6 kanter skall vara röda eller blå?

(Svaret får innehålla heltal, faktorer, potenser och de fyra enkla räknesätten.)

Lycka till!

Lösningar kommer att läggas ut på kurssidan.