

Matematik, KTH

B.Ek

Tentamen TENB i kurs
SF1630(/SF1631), DISKRET MATEMATIK för D, F
torsdagen den 13 mars 2014, 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 lsiB 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 $G \times G \rightarrow G$). Ange vad som krävs för att $(G, \circ)$ skall vara en **grupp**.

b) (1p) Om G är en grupp, hur definieras $Z(G)$, G 's **centrum**?

c) (1p) Om G är en grupp och H en delgrupp till G , vad menas med en **högersidoklass** (eng. right coset) till H (i 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) Finn alla element i $U(\mathbb{Z}_{20})$, de inverterbara elementen i $\mathbb{Z}_{20}$.

3a) (1p) För vilka $k \in \{2, 3, \dots, 20\}$ finns en **kropp** (eng. field) F med $|F| = k$?

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

c) (1p) Om F är en kropp och $k(x) \in F[x]$, låt $F[x]/(k(x))$ vara ringen av restklasser i $F[x]$ (mod $k(x)$). För vilka $k(x)$ är $F[x]/(k(x))$ en kropp?

4a) (1p) Låt $\mathcal{C}$ vara en binär kod. Definiera **minimiavståndet** δ för $\mathcal{C}$.

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

c) (1p) Är för alla $x, N \in \mathbb{N}$ med $\text{sgd}(x, N) = 1$ N ett primtal omm $x^{N-1} \equiv_N 1$?

DEL P1

Godkänd uppgift 2 på lsiB 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.

Vänd!

5) (3p) Finn en delgrupp till S_4 (gruppen av permutationer av $\{1, 2, 3, 4\}$) som är isomorf med $G_{\square}$ (symmetrigruppen för en kvadrat).

6) (3p) Låt gruppen $G = U(\mathbb{Z}_{18})$, de inverterbara elementen i ringen $(\mathbb{Z}_{18}, +, \cdot)$, verka på mängden $X = \mathbb{Z}_{18}$ med ringens multiplikation. Finn alla banor för G 's verkan på X .

7) (3p) Finn $\text{sgd}(f(x), g(x))$ (eng. gcd) i $\mathbb{Z}_5[x]$, då

$$f(x) = x^4 + x^3 + 4x^2 + 3x + 4 \text{ och } g(x) = x^4 + x^2 + 3x + 1.$$

8) (3p) En linjär, binär kod har kontrollmatrisen (eng. check matrix)

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Orden 11001, 01010, 10101 har mottagits. Vilka kodord måste ha sänts, förutsatt att högst ett fel har uppstått i överföringen av varje ord?

DEL P2

9) (4p) Låt G vara en grupp och $A \subseteq G$, $A \neq \emptyset$.

Visa att om $G_A = \{g \in G \mid ga \in A \text{ för alla } a \in A\}$ måste $|G_A| \leq |A|$.

10) Man tillverkar brickor i form av liksidiga trianglar. I varje hörn sitter en kula som kan vara röd, gul eller blå och även brickans båda ytor färgas, var och en antingen vit eller svart. Hur många väsentligt olika brickor (dvs som inte kan vridas så att de sammanfaller) finns det om

a) (3p) man bara kan vrida så att ytorna inte byter plats.

b) (1p) man också kan vrida så att ytorna byter plats.

11) (4p) Låt p och q vara olika primtal. Finn alla $k \in \mathbb{N}$ sådana att

$$x^k \equiv x \pmod{p \cdot q} \text{ för alla } x \in \mathbb{Z}.$$

För full poäng krävs att man både visar att kongruensen med de funna k gäller för alla x och att det för alla andra k finns x så att den inte gäller.

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 $(\text{mod } x^2 + 1)$ och beteckna 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 $t^2 + 7t + 9 = 0$.

13a) (1p) Hur många inverterbara element finns det i $\mathbb{Z}_{299}$, dvs vad är $|U(\mathbb{Z}_{299})|$?

b) (4p) Finn ett element av ordning 33 i gruppen $(U(\mathbb{Z}_{299}), \cdot)$. [$299 = 13 \cdot 23$]

Lycka till!

Lösningar kommer att läggas ut på kurssidan.