

Matematik, KTH

B.Ek

Tentamen TENB i kurs
SF1630(/SF1631), DISKRET MATEMATIK för D, F
torsdagen den 16 januari 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) Vad säger **Lagranges sats** om delgruppers storlek i en ändlig grupp?

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

2a) (1p) Vad menas med **banan** (eng. orbit) 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) Om $(R, +, \cdot)$ är en **ring**, vad kan sägas om strukturen $(R, +)$?

3a) (1p) Vad menas med **karakteristiken** för en kropp (eng. field)?

b) (1p) Hur definieras att ett polynom i $F[x]$ är **irreducibelt**, F en kropp?

c) (1p) Vad säger satsen om **entydig faktorisering** i $F[x]$, F en kropp?

4a) (1p) Kodet $\mathcal{C}$ skall rätta e fel. Vad krävs för **minimiavståndet** δ i $\mathcal{C}$?

b) (1p) Man har RSA-parametrar $(n = p \cdot q, e)$ (p, q primtal). Hur bestäms d ?

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

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.

5) (3p) Elementet g i gruppen G har ordningen 10. Vilken ordning har g^6 ? Motivera svaret.

Vänd!

6) (3p) $G = \{id, \pi, \sigma, \pi\sigma, \sigma\pi, \pi\sigma\pi, \sigma\pi\sigma, \pi\sigma\pi\sigma\}$ är en delgrupp till S_6 då $\pi = (1\ 2)(3\ 4)(5\ 6)$, $\sigma = (2\ 3)$ (det behöver du inte visa).

Finn banor och stabilisatorer för 1 och 5 då G verkar på $\{1, 2, 3, 4, 5, 6\}$.

7) (3p) Faktorisera i irreducibla faktorer polynomet i $\mathbb{Z}_3[x]$

$$f(x) = x^4 + x^3 + x^2 + 2.$$

Skriv koefficienterna i faktorerna som element i $\mathbb{Z}_3$, dvs utan t.ex. minustecken.

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

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

Orden 110100, 101001, 010100 har mottagits. Vilka kodord måste ha sänts, förutsatt att högst ett fel har uppstått i överföringen av varje ord?

DEL P2

9) (4p) Är $(\{\ln x \mid x \in \mathbb{Q}, x > 0\}, +)$ en delgrupp till gruppen $(\mathbb{R}, +)$?

$\mathbb{R}$ är de reella talen, $\mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{Z}_+\}$ de rationella. Motivera svaret.

10) Låt U_{99} vara mängden av inverterbara element i ringen $(\mathbb{Z}_{99}, +, \cdot)$.

a) (1p) Finn inversen till elementet 2 i gruppen $(U_{99}, \cdot)$.

b) (3p) Finn ordningen för elementet 2 i gruppen $(U_{99}, \cdot)$.

11) Låt R vara ringen $\mathbb{Z}_7[x]/(f(x))$ (alla ekvivalensklasser i $\mathbb{Z}_7[x] \pmod{f(x)}$), där

$$f(x) = x^3 + 5x^2 + 4x + 4.$$

x :s ekvivalensklass kallas α .

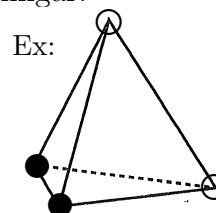
a) (2p) Uttryck α^4 som en linjärkombination av $1, \alpha, \alpha^2$ (med koefficienter i $\mathbb{Z}_7$).

b) (2p) Finn nolldelare i R , dvs $r, s \in R \setminus \{0\}$ med $r \cdot s = 0$.

DEL P3

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

12) Genom att foga samman sex cylindriska pinnar som kanter och fyra sfäriska kulor som hörn skapar man små maskotar i form av tetraedrar. Pinnarna och kulorna kan vara antingen svarta eller vita, men bortsett från det är alla pinnar identiska och kulorna likaså.



a) (1p) Hur många olika rotationssymmetrier har en regelbunden tetraeder?

b) (4p) Hur många väsentligt olika (dvs sådana att ingen kan vridas så att den blir identisk med någon annan) maskotar enligt ovan kan man skapa, om kanter av båda färgerna och hörn av båda färgerna måste vara med i varje maskot?

13) Ett RSA-system har offentlig nyckel $n = 1147$, $e = 271$. [$1147 = 31 \cdot 37$]

a) (1p) Bestäm motsvarande dekrypteringsparameter d .

b) (4p) Hur många meddelanden krypteras som sig själva, dvs för hur många heltal x , $0 \leq x \leq 1146$, gäller $E(x) = x$?

Lycka till!

Lösningar kommer att läggas ut på kurssidan.