

Matematik, KTH

B.Ek

Tentamen TENB i kurs
SF1630(/SF1631), DISKRET MATEMATIK för D m.fl.
onsdagen den 13 januari 2016, 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 lsiB ht15 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 en grupp $(G, \circ)$ är **abelsk** (eng. abelian)?

c) (1p) Låt H vara en delgrupp till gruppen $(G, *)$. Vad menas med en **högersidoklass** (eng. right coset) till H (i G)?

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) Är $(\mathbb{Q} \setminus \{0\}, +, \cdot)$ en **ring**? ($\mathbb{Q}$ betecknar de rationella talen.)

3a) (1p) För vilka $k \in \{5, 6, \dots, 30\}$ finns en **kropp** (eng. field) F med $|F| = k$?

b) (1p) Vad menas med **karakteristiken** för en (ändlig) kropp $(F, +, \cdot)$?

c) (1p) Vad menas med ett **primitivt element** i en kropp $(F, +, \cdot)$?

4a) (1p) Vad krävs av **kontrollmatrisen** (eng. check matrix) H för att dess linjära kod skall rätta minst ett fel?

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 ht15 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.

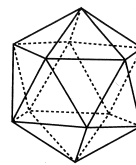
Vänd!

5) (3p) $x^2a = bxc^{-1}$ och $acx = xac$, där $a, b, c, x \in G$, en grupp.
Uttryck x i a, b, c .

6) Låt G vara gruppen av rotationssymmetrier för en ikosaeder.

a) (1p) Vad är $|G|$?

b) (2p) Finn alla storlekar på (dvs antal element i) banor för G 's verkan på punkter i rummet.



En ikosaeder

7) (3p) Faktorisera $f(x) = x^5 + x^3 + 2x^2 + x + 4 \in \mathbb{Z}_5[x]$ i irreducibla faktorer.

8) En linjär, binär kod ges av kontrollmatrisen (eng. check matrix) $H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$.

a) (2p) Hur många ord innehåller koden?

b) (1p) Hur många ord (dvs följder av längd 5 av 0:or och 1:or) kan inte rättas (genom att ändra högst en bit), dvs kan inte fås med högst ett fel i ett kodord?

DEL P2

9) $\pi, \sigma \in S_8$ (gruppen av permutationer av $\{1, 2, \dots, 8\}$) ges av $\pi = (17568)(234)$ och $\sigma = (1478653)$. Låt $H = \{id, \pi, \sigma, \pi^2, \pi\sigma, \sigma\pi, \sigma^2, \pi^3, \pi^2\sigma, \pi\sigma\pi, \dots\}$, mängden av alla produkter av π :n och σ :n.

a) (2p) Visa att H är en delgrupp till S_8 .

b) (2p) Visa att $|H| \geq 420$.

10) (4p) Låt H vara en delgrupp till gruppen G .

Om $A \subseteq G$ är en vänstersidoklass (eng. left coset) till H i G , finns det då säkert en delgrupp H' till G sådan att A är en högersidoklass till H' i G ?

Visa att H' måste finnas eller ge exempel på A, H, G sådana att H' inte finns.

11a) (2p) Visa att $k(x) = x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$ är irreducibelt i $\mathbb{Z}_2[x]$.

b) (2p) Låt (som vanligt) $F = \mathbb{Z}_2[x]/(k(x))$ vara kroppen av restklasser mod $k(x)$ (med $k(x)$ från a) och α vara restklassen som innehåller polynomet x .

Finn $(\alpha^2 + 1)^{-1}$ i F , uttryckt som en summa av vissa av $\alpha^4, \alpha^3, \alpha^2, \alpha$ och 1.

(Uppgift b får göras även om a inte lösts.)

DEL P3

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

12a) (2p) Låt p vara ett primtal, $p \equiv 3 \pmod{4}$.

Visa att för alla $x \in \mathbb{Z}$ gäller $p \nmid x^2 + 1$, dvs att $x^2 + 1$ inte är delbart med p .

b) (3p) Låt p vara ett primtal, $p \equiv 1 \pmod{4}$.

Visa att det finns ett heltal x , sådant att $p \mid x^2 + 1$.

[Ledning: Betrakta sambanden som ekvationer för x i $\mathbb{Z}_p$.]

13) Två binära relationer $\mathcal{R}$ och $\mathcal{R}'$ på en mängd X är **isomorfa** om det finns en bijektion $f: X \rightarrow X$ sådan att $a\mathcal{R}b \Leftrightarrow f(a)\mathcal{R}'f(b)$ för alla $a, b \in X$.

a) (3p) Hur många icke-isomorfa binära relationer finns det på X om $|X| = 3$?

b) (2p) Samma fråga då $|X| = 4$.

(Svaret i a) ges som ett heltal. Svaret i b) får innehålla heltal och de fyra enkla räknesätten.)

[Ledning: $\mathcal{R}$ kan beskrivas av en $|X| \times |X|$ -matris med element 0 eller 1 (för falskt och sant).]

Lycka till!

Lösningar kommer att läggas ut på kurssidan.