

Matematik, KTH

B.Ek

Tentamen TENB i kurs
SF1630(/SF1631), DISKRET MATEMATIK för D m.fl.
tisdagen den 24 oktober 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 lsiB 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 $g \in G$, en grupp. Om g har ordning (eng. order) m , för vilka s är $g^s = 1$, G 's identitetsselement?

c) (1p) Hur många delgrupper av ordning m har en cyklisk grupp av ordning n (för olika m, n)?

2a) (1p) Vad menas med **banan** 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) Vad krävs för att en **ring** $(R, +, \cdot)$ skall vara en **kropp** (eng. field)?

3a) (1p) Hur definieras att ett polynom i $F[x]$ är **irreducibelt**, F en kropp?

b) (1p) Ange för vart och ett av följande n hur många olika (dvs icke-isomorfa) kroppar $(F, +, \cdot)$ det finns med $|F| = n$: $n = 7, 8, 9, 10, 15, 36, 103$.

c) (1p) Vad gäller för $F[x]/(k(x))$, restklassringen modulo $k(x)$, då $k(x)$ är **irreducibelt** (F en kropp, $k(x) \in F[x]$)?

4a) (1p) Vad menas med att en binär kod är **linjär**?

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?

Vänd!

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 gruppen G ha delgrupperna H och K , med $|H| = |K| = p$, ett primtal. Visa att $H = K$ eller $H \cap K = \{1\}$ (där 1 är identitets-elementet i G).

6) (3p) Låt gruppen $G = U_{15}$, de inverterbara elementen i ringen $(\mathbb{Z}_{15}, +, \cdot)$, verka på mängden $X = \mathbb{Z}_{15}$ med ringens multiplikation.

Finn båda bana och stabilisator för vart och ett av elementen 3 och 5 i X .

7) (3p) Faktorisera polynomet $f(x) \in \mathbb{Z}_7[x]$ i irreducibla faktorer,

$$f(x) = x^5 + 3x^4 + x^3 + x^2 + 6x + 1.$$

Skriv koefficienterna i faktorerna som element i $\mathbb{Z}_7$, dvs utan t.ex. minustecken.

8) (3p) Finn ett $x \in \mathbb{Z}_+$ sådant att för alla $a, b \in \mathbb{Z}$:

$$b \equiv a^{143} \pmod{447} \text{ om och endast om } a \equiv b^x \pmod{447}.$$

DEL P2

9) (4p) Låt $(R, +, \cdot)$ vara en ring (med etta, som alla ringar enligt bokens definition) med egenskapen att $a^2 = a$ för alla $a \in R$ (en s.k. boolesk ring).

Visa att det enda inverterbara (under multiplikation) elementet i R är 1.

(Ledning: Vad följer av att $ab = 0$ i en ring och a är inverterbart? Motivera.)

10) Låt $k(x) = x^3 + 2x^2 + 4x + 4 \in \mathbb{Z}_5[x]$ och $F = \mathbb{Z}_5[x]/(k(x))$ vara ringen av restklasser i $\mathbb{Z}_5[x]$ mod $k(x)$. Kalla restklassen med polynomet x för α .

a) (2p) Finn $|F|$ (antalet element i F) och visa att $(F, +, \cdot)$ är en kropp.

b) (2p) Finn ett $t \in F$, sådant att $(\alpha^2 + 2\alpha + 2) \cdot t = 3\alpha^2 + 2\alpha + 1$.

11) Låt G vara en grupp med en delgrupp H .

a) (2p) Visa att $K = \{g \in G \mid gxg^{-1} \in H \Leftrightarrow x \in H\}$ är en delgrupp till G .

b) (2p) $G = \{(1), (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3), (2\ 4)\} \subset S_4$ är en grupp (det behöver du inte visa). Vilka K_1 och K_2 svarar mot delgrupperna $H_1 = \{(1), (1\ 3)\}$ och $H_2 = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$?

DEL P3

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

12) (5p) Ett (pytte-)RSA-system använder parametrarna $n = 899 (= 29 \cdot 31)$ och $e = 484$. Hur många $x \in \mathbb{Z}_n$ krypteras som sig själva (dvs uppfyller $E(x) = x$)?

13) (5p) Vi får veta att det kromatiska polynomet för kubgrafen (dvs antalet sätt att färga kubens hörn med högst k färger, utan att några hörn vid samma kant har samma färg) är $P_{\text{kub}}(k) = k(k-1)(k^6 - 11k^5 + 55k^4 - 159k^3 + 282k^2 - 290k + 133)$.

Finn antalet väsentligt olika (dvs som förblir olika då man vrider dem i rummet) sådana (dvs utan likfärgade grannhörn) färgningar av kubens hörn med högst k färger.

Lycka till!

Lösningar kommer att läggas ut på kurssidan.