

Tentamen i kurs
SF1688, 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 kontrollskrivning i ht17 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) Hur definieras att graferna $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ är **isomorfa**?

b) (1p) Vad menas med det **kromatiska talet**, $\chi(G)$, för en graf $G = (V, E)$?

c) (1p) Formulera **Eulers polyederformel** för en plan sammanhängande graf. Förklara införda beteckningar.

2a) (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 många delgrupper av ordning m har en **cyklisk** grupp av ordning n (för olika $m, n \in \mathbb{Z}_+$)?

c) (1p) Hur avgör man lätt om $\pi, \sigma \in S_n$ (givna på cykelform) är **konjugerade**?

3a) (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) Vad krävs för att en **ring** $(R, +, \cdot)$ skall vara en **kropp** (eng. field)?

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 kontrollskrivning i ht17 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) Då $G = (V, E)$ är en enkel (dvs inga öglor, inga multipla kanter) graf, låt **komplementgraf** $\overline{G}$ till G vara (den enkla) grafen med samma hörn (eng. vertices) som G , där $x, y \in V$, $x \neq y$ är grannar i $\overline{G}$ om de inte är grannar i G . Visa att om G är isomorf med $\overline{G}$ är $|V| \equiv 0$ eller $1 \pmod{4}$.

Tips: betrakta summan av valenserna (eng. degrees) i G och i $\overline{G}$.

6) (3p) Elementet g i gruppen G har ordningen 60. Vilken ordning har g^{78} ?
Glöm inte att motivera svaret.

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 högsta gradskoefficienten 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) Grafen $G = (V, E)$ är inte tom (dvs $V \neq \emptyset$) och antalet hörn med valens 3 är lika med antalet hörn med valens någon av 0 och 1.

Visa att G innehåller minst en cykel.

11a) (2p) Vilka cykelstrukturer (typer) är möjliga för udda permutationer i S_{10} (alla permutationer av $\{1, 2, \dots, 10\}$) som har ordning 12 (dvs $\pi^{12} = id$ och $\pi^k \neq id$ för $1 \leq k < 12$). Cykelstrukturen anges som $[k_1^{\alpha_1} \dots k_m^{\alpha_m}]$ då π har α_i cykler av längd k_i , $k_1 < \dots < k_m$.

b) (2p) Hur många udda permutationer av ordning 12 finns det totalt i S_{10} ?

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 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, faktulteter, potenser och de fyra enkla räknesätten.)

Lycka till!

Lösningar kommer att läggas ut på kurssidan.