

**Tentamen TENB i kurs
SF1630(/SF1631), DISKRET MATEMATIK för D m.fl.
onsdagen den 16 mars 2016, klockan 8.00–13.00.**

Examinator: Bengt Ek, tel 790 6951 (inte tillgänglig under tentamen).

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) 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 **stabilisatorn** 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** (eng. orbit) och **stabilisatorn** för $x \in X$?

c) (1p) Är $(\mathbb{Z}_m, +, \cdot)$ en **ring** för något sammansatt tal (dvs $\neq 1$, inte primtal) m ?

3a) (1p) Beskriv strukturen för $(F \setminus \{0\}, \cdot)$, då $(F, +, \cdot)$ är en ändlig kropp.

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

c) (1p) Vad säger **faktorsatsen** (eng. factor theorem) i $F[x]$, F en kropp?

4a) (1p) Hur många fel kan **rättas** i en binär kod med minimala avståndet δ ?

b) (1p) I ett RSA-system med offentliga parametrar (n, e) , vad är $E(x)$, den krypterade formen av meddelandet x ?

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.

- 5) (3p) Gruppen G har ett element $g \neq 1$ med $g^{12} = 1$ (G :s identitetsselement).
Vilka av värdena 1, 2, 3, ..., 10 är möjliga för G :s ordning $|G|$?
- 6) Låt G vara gruppen U_{20} av inverterbara element i ringen $(\mathbb{Z}_{20}, +, \cdot)$.
a) (2p) Finn alla banor då G verkar på $X = \mathbb{Z}_{20}$ med multiplikation (i $\mathbb{Z}_{20}$).
b) (1p) Verifiera vår formel ("Burnsides lemma") för antalet banor i detta fall.
- 7) (3p) Finn alla moniska (dvs med högstgradskoefficient 1) irreducibla polynom i $\mathbb{Z}_3[x]$ som delar både $f(x) = x^5 + x^3 + x^2 + x + 2$ och $g(x) = x^6 + x^5 + x^3 + 1$.
- 8) (3p) Det är sant att $1234^{503} \equiv 4083 \pmod{6767}$ (det behöver du inte visa).
Finn ett $k \in \mathbb{Z}_+$ sådant att $4083^k \equiv 1234 \pmod{6767}$.
[67 och 101 är primtal.]

DEL P2

- 9) (4p) Låt $SL(2, \mathbb{Z}_2)$ vara mängden av 2×2 -matriser med element i $\mathbb{Z}_2$ och determinant 1. Visa att $SL(2, \mathbb{Z}_2)$ är en grupp och bestäm ordningen för vart och ett av dess element.

- 10a) (2p) Visa att om p är ett primtal är

$$x^{p-1} - 1 = (x-1)(x-2)\dots(x-(p-1)) \text{ i } \mathbb{Z}_p[x].$$

- b) (2p) Visa **Wilsons sats**: $(p-1)! \equiv -1 \pmod{p}$ om p är ett primtal.

Resultatet i a) får användas i b), även om a) inte lösts.

- 11) (4p) Låt G vara en grupp och $\mathcal{S}_G$ vara gruppen av permutationer av mängden G (dvs alla bijektioner $G \rightarrow G$ med sammansättning av funktioner som operation).
Finn en isomorfi mellan G och en delgrupp till $\mathcal{S}_G$ (och verifiera att den är en isomorfi).

DEL P3

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

- 12) (5p) Finn ett polynom $g(x) \in \mathbb{Z}_5[x]$ sådant att $F = \{b_1\alpha + b_0 \mid b_0, b_1 \in \mathbb{Z}_5\}$, där α uppfyller att $g(\alpha) = 0$, blir en kropp och $f(x) = x^4 + 2x^3 + x + 2 \in \mathbb{Z}_5[x]$ kan faktoriseras i förstgradsfaktorer i $F[x]$.

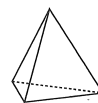
Ange också en sådan faktorisering.

($f(x)$ och $g(x)$ ses som polynom i $F(x)$ genom att element i F med $b_1 = 0$ identifieras med b_0 .)

- 13a) (1p) Låt G vara hela symmetrigruppen för en kub (dvs bestå av alla stela avbildningar som lämnar kuben invariant, inte bara rotationer). Vad är $|G|$, G :s ordning?

- b) (1p) Kubens hörn numreras 1, 2, ..., 8. Hur många element i G (från a)) svarar mot udda permutationer i S_8 (gruppen av alla permutationer av $\{1, 2, \dots, 8\}$)?

- c) (3p) En färgning av en regelbunden tetraeders sex kanter kallas **kiral** om tetraedern inte kan vridas så att färgningen blir som sin spegelbild. Hur många sådana kirala färgningar finns det, om det finns k färger att använda vid färgningen?



En tetraeder

Lycka till!

Lösningar kommer att läggas ut på kurssidan.